Haaga-Helia
ammattikorkeakoulu Oy

Tietosuoja-asetuksen muutoksen vaikutukset henkilörekistereitä hallinnoivien palveluyritysten prosesseihin

Vilhelmiina Karttunen

Opinnäytetyö
Tietojenkäsittelyn
koulutusohjelma
2018

Tiivistelmä

Haaga-Helia ammattikorkeakoulu Oy

Tekijä(t)
Vilhelmiina Karttunen

Koulutusohjelma
Tietojenkäsittelyn koulutusohjelma

Opinnäytetyön otsikko
Tietosuoja-asetuksen muutoksen vaikutukset henkilörekistereitä hallinnoivien palveluyritysten prosesseihin

Sivu- ja liitesivumäärä
23 + 1

Yleinen tietosuoja-asetus astui voimaan 24.5.2016. Sen soveltaminen alkaa kaikissa EU:n jäsenmaissa 25.5.2018. Se koskettaa kaikkea henkilötiedon käsittelyä. Siirtymäaikana EU:n tietosuojatyöryhmä WP 29 on laatinut ohjeistusta tietosuoja-asetuksen tulkinnasta. Asetus tuo mukanaan uusia velvoitteita henkilörekistereitä hallinnoiville yrityksille ja yhteisöille, vaikka pääperiaatteet säilyvätkin samoina. Uusia velvoitteita tulee mm. rekisterinpitäjälle, kun taas rekisteröidylle lisätään oikeuksia. Asetus tulee täsmentymään kansallisen lainsäädännön myötä. Lain on tarkoitus tulla voimaan samaan aikaan kun asetusta aletaan soveltaa.

Opinnäytetyössä ”Tietosuoja-asetuksen muutoksen vaikutukset henkilörekistereitä hallinnoivien palveluyritysten prosesseihin” kuvataan asetuksen säännöksiä, tehdään asetuksesta tulkintoja ja annetaan esimerkkiyrityksen kautta käytännön ohjeita, kuinka asetukseen tulee valmistautua ja miten henkilötietoja tulee käsitellä asetuksen hengenmukaisesti. Opinnäytetyön tarkoitus ei ole tehdä nimenomaista rinnakkaisvertailua jo olemassa olevan tietosuojalain ja uuden asetuksen välillä. Opinnäytetyö ei myöskään ota kantaa lopulliseen tietosuojalain uudistukseen, sillä laki ei astu voimaan opinnäytetyönteon aikana.

Opinnäytetyön aloitus ajoittui käytännössä vuoden 2017 puolelle, kun tekijä aloitti työssään tutustumaan tietosuoja-asetuksen sisältöön. Varsinaista kirjoitusosuutta alettiin työstää myöhemmässä vaiheessa. Työtä on tehty asetuksen ollessa vielä hyvin tulkinnanvarainen. Opinnäytetyö on tutkimusmenetelmällä kirjoitettu, tietoperustana yleinen tietosuoja-asetus. Työ tehtiin ilman varsinaista toimeksiantajaa ja aihe valittiin tekijän työhön liittyvän projektin johdosta. Tavoitteena opinnäytetyölle oli syventää tekijän asiantuntijuutta tietosuoja-asetuksen tuomiin muutoksiin.

Asiasanat
Tietosuoja-asetus, GDPR, tietosuoja, tietojenkäsittely, henkilötieto, henkilötietolaki

Sisällys

1 Johdanto 1
2 Tietosuoja-asetus 2
2.1 Käsitteet 3
2.1.1 Henkilötieto 3
2.1.2 Arkaluontoinen henkilötieto 4
2.1.3 Käsittely 4
2.1.4 Oikeutettu etu 4
2.1.5 Profilointi 5
2.1.6 Anonymisointi 5
2.1.7 Pseudonymisointi 5
2.1.8 Rekisteri 6
2.1.9 Rekisterinpitäjä 6
2.1.10 Henkilötietojen käsittelijä 6
2.1.11 Kolmas osapuoli 6
2.1.12 Rekisteröidyn suostumus 6
2.1.13 Henkilötietojen tietoturvaloukkaus 6
2.1.14 Edustaja 7
2.1.15 Yritys 7
2.1.16 Valvontaviranomainen 7
3 Asetuksen velvoitteiden implementointi käytäntöön 7
3.1 Tietosuojatoimet henkilötietoja käsiteltäessä 7
3.1.1 Tietojen minimointi 8
3.1.2 Henkilötietojen käsittely 8
3.2 Yrityksen johdon toimet 9
3.3 Yrityksen omat tietosuojaperiaatteet 10
3.4 Henkilöstön henkilötietojen käsittely 10
3.4.1 Rekisteröidylle toimitettavat tiedot 11
3.4.2 Seloste käsittelytoimista 12
3.5 Yrityksen markkinointi 12
3.5.1 Suostumus tiedon keräämiseen ja käyttämiseen 13
3.6 Yrityksen asiakkuudet ja toimeksiannot 14
3.7 Kolmansien osapuolten kanssa tehdyt sopimukset 14
3.8 Tietoturvaloukkauksien ilmoitusvelvollisuus 15
3.9 Järjestelmät ja sovellukset 15
3.10 Tietosuojariskiarvio 16
3.11 Rekisteröidyn oikeudet 16
3.11.1 Rekisteröidyn oikeus saada pääsy tietoihin 16

3.11.2 Oikeus tietojen oikaisemiseen tai poistamiseen 17
3.11.3 Oikeus käsittelyn rajoittamiseen 17
3.11.4 Oikeus siirtää tiedot järjestelmästä toiseen 17
3.11.5 Vastustamisoikeus 18
3.12 Henkilötietojen säilyttäminen ja käyttörajoitukset 18
3.13 Viranomaistahot 19
3.14 Henkilöstön kouluttaminen 19
4 Pohdinta 20
Lähteet 22
Liite 1 1

1 Johdanto

Työympäristömme muuttuu jatkuvasti; teknologia edistyy, lainsäädännöt muuttuvat ja asiakkaiden ja yksilöiden vaatimukset lisääntyvät jatkuvasti. Se merkitsee meille jokaiselle, joka on tekemisissä henkilötietojen kanssa sitä, että on yhä tärkeämpää kiinnittää tietojen suojeluun huomiota.

Tietosuojavaltuutettu Reijo Aarnion mukaan (2017/01) ”Digitaalisuuden, talouden uusien muotojen, sijaintitietojen kiinnostavuuden, tekoälyn, koneoppimisen ja robotiikan myötä on huomattu, että kaikki digitaalisuuden hyödyntäminen perustuu luottamukselle. Tietosuoja on ajankohtaisempi asia kuin koskaan aikaisemmin”.

Tällä hetkellä Suomen ja Euroopan unionin tietosuojalakeja ollaan uudistamassa. Toukokuun 25. päivä alkaen EU:n yleistä tietosuoja-asetusta (General Data Protection Regulation, GDPR) aletaan soveltaa EU:n kaikissa jäsenmaissa. Lähtökohtaisesti asetusta tullaan soveltamaan kaikkeen henkilötietojen käsittelyyn ja sen laiminlyönnistä voi seurata yrityksille merkittäviä sakkoja. Tietosuoja-asetusta tullaan täydentämään kansallisella lainsäädännöllä ja uuden lain on tarkoitus tulla voimaan samaan aikaan asetuksen kanssa. (Tietosuojavaltuutetun toimisto 2017.)

Tietosuojavaltuutetun mukaan (Tietosuojavaltuutetun toimisto 2017) riskiperusteinen lähestymistapa sekä henkilötiedon rekisterinpitäjän osoitusvelvollisuus ovat uusia, keskeisiä asioita, joita tietosuoja-asetus tuo mukanaan. Rekisterinpitäjän velvollisuudet kasvavat sitä mukaa, mitä korkeampia riskejä henkilötietojen käsittelyyn liittyy. Rekisterinpitäjän on myös tässä asiassa pystyttävä osoittamaan, että se noudattaa tietosuoja-asetusta muun muassa tekemällä riskien vaikutustenarviointeja. Suomessa on ollut tietosuojalaki voimassa jo lähes toistakymmentä vuotta, ja uusi asetus onkin pitkälti samankaltainen, mutta tuo mukanaan joitakin lisävelvoitteita. Lainsäädäntöä uusitaan, jotta henkilötietojen suojaa ja rekisteröityjen oikeuksia saadaan parannettua ja tietosuojasääntelyä kaikissa EU-maissa saataisiin yhtenäistettyä.

Syy käynnistää tämä projekti oli ensiksi selkeyttää opinnäytetyöntekijälle, mitä asetuksen tuomat lisävelvoitteet ovat. Tietosuoja-asetukseen liittyvää työtä on opinnäytetyön tekijä tehnyt viime vuoden kesäkuusta alkaen. Opinnäytetyön tekijän työtehtäviin nykyisessä työpaikassa kuuluu tälläkin hetkellä perehtyä asetuksen määräämien lisävelvoitteiden tuomiin muutoksiin. Toinen syy projektille oli tuottaa ohjeistusta, kuinka esimerkkiyrityksen käytännön arjen toimia tulee muuttaa, jotta yrityksen toimintaperiaatteet ja käytänteet vastaavat asetuksen hengenmukaisuutta sekä sen asettamia velvoitteita. Tavoiteltu hyöty

projektista syntyi, kun tekijän ymmärrys asetuksesta syveni ja esimerkkiyritykselle saatiin projektista tuloksena ohjeistus siitä, että minkälaisiin prosessimuutoksiin yrityksen tulee varautua niiltä osin kuin se hallinnoi ja käsittelee henkilötietoja sisältäviä rekistereitä. Projektin tehtävänä oli siis tutustua uuteen tietosuoja-asetukseen, mutta projekti ei ottanut lopullista kantaa lain muutoksiin, sillä asetus astuu voimaan toukokuussa ja laista oli projektin edetessä vasta tehty hallitukselle ehdotus. Osin asetus oli myös hyvin tulkinnanvarainen.

2 Tietosuoja-asetus

Tietosuojan tärkeys ja henkilötietojen käytön turvaaminen kasvattavat merkitystään koko ajan. Toukokuussa voimaan tulevalla EU:n yleisellä tietosuoja-asetuksella tiukennetaan henkilötietojen tietosuojaa koskevia vaatimuksia Euroopan talousalueella (ETA), lisätään sääntelyviranomaisia, luodaan merkittäviä seuraamuksia asetuksen noudattamatta jättämiselle ja pyritään laajentamaan EU:n sääntelyviranomaisten auktoriteettia ympäri maailmaa. Alla olevassa kuvassa on kuvattuna asetuksen tavoitteet.

Kuva 1 Parempi luottamus online-palveluihin edistää EU:n digitaalista sisämarkkinoiden kehittämistä.(OpiTietosuojaa.fi, 2018.)

Nyt uuden asetuksen myötä, tietosuojaan liittyvät haasteet kasvavat entisestään. Tästä johtuen monissa organisaatioissa edellytetään, että harkitaan uudelleen, kuinka henkilötietoja käsitellään ja pidetään huolta siitä, että on tarkistettu niiden käyttötarkoitus. Pyrki-

mys on samalla lieventää tietojen käyttöön liittyviä riskejä. Muita syitä asetukselle ovat tarkoitus vahvistaa sääntöjä luonnollisten henkilöiden suojelulle henkilötietojen käsittelyssä sekä säännöt, jotka koskevat henkilötietojen vapaata liikkuvuutta.

Tietosuoja-asetus tullee tiukentamaan tietosuojaan liittyviä vaatimuksia Euroopan talousalueelle sekä liittyen Euroopan talousalueella kerättyihin henkilötietoihin, jotka on siirretty muihin maihin. Asetus vaatii, että Euroopan talousalueella olevien henkilöiden henkilötietoja suojataan kaikkialla, minne tietoja saatetaan siirtää. Poikkeuksena on, jos tietoja ei kerätä Euroopan talousalueella tai jos sopimusvelvoitteilla on vaihtoehtoiset suojeluvaatimukset.

2.1 Käsitteet

Alla olevassa luvussa selvennetään ja kerrotaan yksityiskohtaisemmin asetuksessa ilmenevistä käsitteistä. Oleellista on ymmärtää henkilötiedon määre ja kuinka tunnistaa mitä on henkilötieto.

2.1.1 Henkilötieto

Yleisen tietosuoja-asetuksen mukaan henkilötietoa on mikä tahansa tieto, jonka perusteella tietty henkilö, jäljempänä tekstissä ’rekisteröity’, voidaan tunnistaa. Esimerkiksi käyntikortissa olevat tiedot lasketaan henkilötiedoksi. Koska henkilön nimi on ilmoitettu käyntikortissa, se tekee kaikesta muusta informaatiosta kortilla myöskin henkilötietoa. Jos nämä tiedot otettaisiin erilleen toisistaan, niistä ei välttämättä saisi tunnistettua tiettyä henkilöä, sillä esimerkiksi yrityksen puhelinnumero, yrityksen nimi tai toimipaikan osoite eivät ole yksinään riittäviä tietoja, joiden avulla voitaisiin tunnistaa henkilö. Tiedot eivät ole henkilötietoja, jos niitä ei voida yhdistää yksittäiseen henkilöön tai niitä ei voida yhdistää muihin tietoihin ja käyttää niitä yhdessä yksilöiden tunnistamiseen. Alla olevat esimerkit riittävät tietyn yksilön tunnistamiseksi:

- matti.m.mattinen@anttila.fi (yksittäiselle henkilölle osoitettu sähköpostiosoite)
- 12.202.222.12 (IP-osoite, kun se liittyy tiettyyn laitteeseen, yksilöllinen internetin käyttö)

Muita esimerkkejä tiedoista, jotka ovat henkilötietoa:

- Sosiaaliturvatunnus
- Passin numero
- ID-numero
- IP-osoite (verkkotunniste)

- Sijaintitieto

Asiayhteydestä on myös mahdollista päätellä henkilö, jolloin tieto, jota muutoin ei mieltäisi henkilötiedoksi, saattaakin muuttua siksi. Jos sukupuoli, tehtävänimike, osoite tai muu tieto on ilmaistu yhdessä henkilön nimen kanssa, nämä ovat myös henkilötietoja. On siis erityisesti kiinnitettävä huomiota missä kontekstissa tiedot ilmenevät, jotta ymmärtää poistaa henkilötiedon sekä sen kontekstin välisen yhteyden ja näin vähentää väärinkäytön riskiä liittyen henkilötietojen käsittelyyn. (PricewaterhouseCoopers 2017.)

2.1.2 Arkaluontoinen henkilötieto

Osa henkilötiedoista voi olla niin arkaluontoista, että tiedon tahattomasta paljastumisesta saattaisi aiheutua suuri riski tiedoissa ilmenneelle henkilölle. Arkaluontoisista henkilötiedoista voidaan puhua omana erityisryhmänään ja tällaisia tietoja käsiteltäessä onkin oltava erityisen huolellinen.

Esimerkiksi työskenneltäessä henkilöstöhallinnon puolella tai terveydenhuollon alalla, usein käsitellään hyvin arkaluontoisia tietoja henkilöistä. Muun muassa palkkatiedot, terveystiedot, luottokorttinumerot, pankkitilitiedot ja sosiaaliturvatunnukset ovat konkreettisia esimerkkejä arkaluonteisista tiedoista, joiden paljastuminen on riskialtista.

2.1.3 Käsittely

Asetuksessa tarkoitetaan käsittelyllä toimintoa tai toimintoja, joita kohdistetaan henkilötietoja sisältäviin tietojoukkoihin joko automaattista tietojenkäsittelyä käyttäen tai manuaalisesti, kuten tietojen keräämistä, tallentamista, järjestämistä, jäsentämistä, säilyttämistä, muokkaamista tai muuttamista, hakua, kyselyä, käyttöä, tietojen luovuttamista siirtämällä, levittämällä tai asettamalla ne muutoin saataville, tietojen yhteensovittamista tai yhdistämistä, rajoittamista, poistamista tai tuhoamista. (Asetus yleisestä tietosuojasta 679/2016/EU.)

2.1.4 Oikeutettu etu

Jotta yritys voi toteuttaa liiketoimintaansa, tähän usein liittyy henkilötietojen käsittelyä. Sitä ei voida välttämättä tässä yhteydessä perustella lakisääteisellä velvoitteella tai rekisteröidyn kanssa tehdyn sopimuksen perusteella. Henkilötietojen käsittely voi tuolloin olla perusteltua 'oikeutetun edun' perusteella. Yrityksen tulee kuitenkin tarkastaa, ettei tämän oikeutetun edun mukaisesta toiminnasta aiheudu vakavaa haittaa rekisteröityjen oikeuksil-

le ja vapauksille. Jos näin käy, yritys ei voi käyttää tietojenkäsittelyn perusteena oikeutettua etua, vaan sen on löydettävä toinen oikeusperuste. (Euroopan komissio.)

2.1.5 Profilointi

Profiloinnilla tarkoitetaan mitä tahansa henkilötietojen automaattista käsittelyä, jossa henkilötietoja käyttämällä arvioidaan henkilön tiettyjä henkilökohtaisia ominaisuuksia, erityisesti analysoidaan tai ennakoidaan piirteitä, jotka liittyvät henkilön työsuoritukseen, taloudelliseen tilanteeseen, terveyteen, henkilökohtaisiin mieltymyksiin, kiinnostuksen kohteisiin, luotettavuuteen, käyttäytymiseen, sijaintiin tai liikkeisiin. (Asetus yleisestä tietosuojasta 679/2016/EU.)

Käsittelyperusteen ollessa olemassa profilointi on sallittua, eikä asetus aseta yleistä profiloinnin kielto-oikeutta.

2.1.6 Anonymisointi

Anonymisoitu tieto tarkoittaa, että henkilöä ei tiedon perusteella ole lainkaan yksilöitävissä. Jos esimerkiksi luettelossa on nimiä ja syntymäpäiviä, ne yhdessä edustavat henkilötietoa. Nimien poistaminen jättää luettelon päivämääristä, jotka eivät enää liity tiettyihin henkilöihin, joten ne pelkältään eivät ole enää henkilötietoja. Päivämääräluetteloa voidaan käyttää anonymisoituna tietolähteenä, koska se ei enää ole henkilörekisteri. Anonymisointi on suositeltavaa aina kun se on mahdollista ja helposti toteutettavissa.

2.1.7 Pseudonymisointi

Pseudonymisoimisella tarkoitetaan henkilötietojen käsittelemistä siten, ettei niitä voida enää käsittelyn jälkeen yhdistää tiettyyn rekisteröityyn käyttämättä lisätietoja, edellyttäen että tällaiset lisätiedot säilytetään erillään ja niihin sovelletaan teknisiä ja organisatorisia toimenpiteitä, joilla varmistetaan, ettei henkilötietojen yhdistämistä tunnistettuun henkilöön tapahdu. (Asetus yleisestä tietosuojasta 679/2016/EU.)

Jos anonymisointia ei voi toteuttaa täydellisesti, voi käyttää pseudonymisointia sen sijaan. Käytännössä se tarkoittaa sitä, että alkuperäisten tietojen sijaan käytetään pseudonyymia, esimerkiksi fiktiivistä nimeä tai viitettä, todellisen tiedon sijaan. Pseudonyymi korvaa tiedon, jolla henkilö on tunnistettavissa. Nimet, syntymäajat, henkilöllisyystunnukset ja muut tunnisteet voidaan kaikki korvata pseodonyymeillä. Esimerkiksi henkilöiden nimet listassa voi korvata numerolla ja käyttää numeroiden ja syntymäpäivien yhdistelmää, jolloin syn-

tymäpäiviä ei suoraan voi yhdistää henkilöön. Pseudonyymit tulee suojata tarkasti, jotta niitä ei tahattomasti voi jälleen yhdistää alkuperäiseen tietoon.

2.1.8 Rekisteri

Asetuksen mukaan rekisteri voi sisältää minkä tahansa tietojoukon jäsennellyistä henkilötiedoista, josta tiedot ovat saatavilla tietyin perustein. (Asetus yleisestä tietosuojasta 679/2016/EU).

2.1.9 Rekisterinpitäjä

Rekisterinpitäjä voi olla asetuksen neljännen artiklan mukaan joko luonnollinen henkilö, viranomainen, virasto tai muu elin, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot. (Asetus yleisestä tietosuojasta 679/2016/EU.)

2.1.10 Henkilötietojen käsittelijä

Asetuksen mukaan henkilötietojen käsittelijä on luonnollinen henkilö, viranomainen, virasto tai muu, joka käsittelee henkilötietoja rekisterinpitäjän lukuun. (Asetus yleisestä tietosuojasta 679/2016/EU.)

2.1.11 Kolmas osapuoli

Asetuksen mukaan kolmas osapuoli voi tarkoittaa joko luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta toimielintä, jolla on oikeus käsitellä henkilötietoja rekisterinpitäjän tai henkilötietojen käsittelijän välittömän vastuun alaisena. (Asetus yleisestä tietosuojasta 679/2016/EU.)

2.1.12 Rekisteröidyn suostumus

Rekisteröidyn suostumuksella tarkoitetaan mitä tahansa vapaaehtoista, yksilöityä, tietoista ja yksiselitteistä tahdonilmaisua, jolla rekisteröity hyväksyy henkilötietojensa käsittelyn antamalla suostumusta ilmaisevan lausuman tai toteuttamalla selkeästi suostumusta ilmaisevan toimen. (Asetus yleisestä tietosuojasta 679/2016/EU.)

2.1.13 Henkilötietojen tietoturvaloukkaus

Tietoturvaloukkauksen seurauksena on siirrettyjen, tallennettujen tai muuten käsiteltyjen henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muutta-

minen, luvaton luovuttaminen tai pääsy tietoihin. (Asetus yleisestä tietosuojasta 679/2016/EU.)

2.1.14 Edustaja

Edustajasta puhutaan asetuksessa, kun tarkoitetaan unioniin sijoittautunutta luonnollista henkilöä tai oikeushenkilöä, jonka rekisterinpitäjä tai henkilötietojen käsittelijä on nimennyt kirjallisesti toimimaan lukuunsa 27 artiklan nojalla ja joka edustaa rekisterinpitäjää tai henkilötietojen käsittelijää, kun on kyse tähän asetukseen perustuvista rekisterinpitäjän tai henkilötietojen käsittelijän velvollisuuksista. (Asetus yleisestä tietosuojasta 679/2016/EU.)

2.1.15 Yritys

Yritys on asetuksen sanastossa kuvattu seuraavasti; ”taloudellista toimintaa harjoittavaa luonnollista henkilöä tai oikeushenkilöä sen oikeudellisesta muodosta riippumatta, mukaan lukien kumppanuudet tai yhdistykset, jotka säännöllisesti harjoittavat taloudellista toimintaa”. (Asetus yleisestä tietosuojasta 679/2016/EU.)

2.1.16 Valvontaviranomainen

Valvontaviranomainen tarkoittaa jäsenvaltion perustamaa riippumatonta viranomaista. (Asetus yleisestä tietosuojasta 679/2016/EU.)

3 Asetuksen velvoitteiden implementointi käytäntöön

Tässä luvussa käsitellään aihekohtaisesti asetuksen asettamia velvoitteita ja annetaan käytännön ohjeistusta arkeen esimerkkiyritykselle, joka hallinnoi henkilörekistereitä. Ohjeistus sisältää toimia, joita tulee suorittaa, jotta ne johtavat esimerkkiyrityksen käytänteiden yhdenmukaisuuteen asetukseen nähden.

3.1 Tietosuojatoimet henkilötietoja käsiteltäessä

Työskenneltäessä esimerkkiyrityksen joko sisäisten- tai ulkoisten asiakkaiden kanssa, on hyvä ottaa huomioon muutamia asioita, jotka voivat huomattavasti parantaa käsiteltävien henkilötietojen tietosuojaa sekä myös rajoittaa käsittelyn määrää, eli asetuksen hengenmukaisesti pitää käsittely minimissään.

Oikeusministeriön julkaisun mukaan rekisterinpitäjän tulee huomioida henkilötietojen käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat, todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit. Tä-

mä siksi, jotta rekisterinpitäjä pystyy toteuttamaan tarvittavat tekniset ja organisatoriset toimenpiteet, joilla voidaan varmistaa ja osoittaa, että käsittelyssä noudatetaan tietosuoja-asetusta.

Näillä toimenpiteillä tarkoitetaan suojatoimenpiteitä, kuten esimerkiksi henkilöstön koulutusta, henkilöstölle annettuja ohjeita ja määräyksiä, salassapitositoumuksia, tilavalvontaa, tietojärjestelmien tietoturvaa, tietojen salausta, auditointeja, etäkäyttöyhteyksiä ja teknisiä rajoituksia. (Tietosuojavaltuutetun toimisto & Oikeusministeriö 2017, 13.)

3.1.1 Tietojen minimointi

Esimerkkiyrityksen harkitessa henkilötietojen keräystä, tulisi aluksi pohtia, kuinka paljon henkilötietoja todella tarvitsee mihinkin tarkoitukseen ja näin ollen pitää kerätty tieto mahdollisimman tarkoituksenmukaisena, olennaisena ja minimoituna. Tämä velvollisuus koskee kerättyjen henkilötietojen määriä, käsittelyn laajuutta, säilytysaikaa ja saatavilla oloa, eikä tämä käytäntö juuri poikkea siitä, mitä jo nykyisessä henkilötietolaissa säädetään. Tietojen minimoinnin toteuttamiseksi tulee tehdä tarvittavat toimenpiteet. Myös tietojen pseudonymisointi ja muut suojatoimet olisi hyvä saada sisällytettyä käsittelyn rutiinitoimenpiteisiin. Esimerkkiyrityksen tulee myös muistaa, että sillä on oltava valmiudet varmistua ja osoittaa, että käsittelyssä noudatetaan asetusta. (Asetus yleisestä tietosuojasta 679/2016/EU.)

3.1.2 Henkilötietojen käsittely

Asetuksessa puhutaan henkilötiedon käsittelystä hyvin laajasti, mutta erityisesti tulee huomioida, että käsittelylle on aina oltava oikeusperuste. Oikeusperusteet kuvataan yksityiskohtaisesti ja näistä säädetään 6 artiklassa. Huomiota on myös erityisesti kiinnitettävä arkaluontoisten tietojen käsittelyyn. Asetuksen 9 artiklan mukaan erityisiä henkilötietoryhmiä koskevasta käsittelystä todetaan muun muassa seuraava:

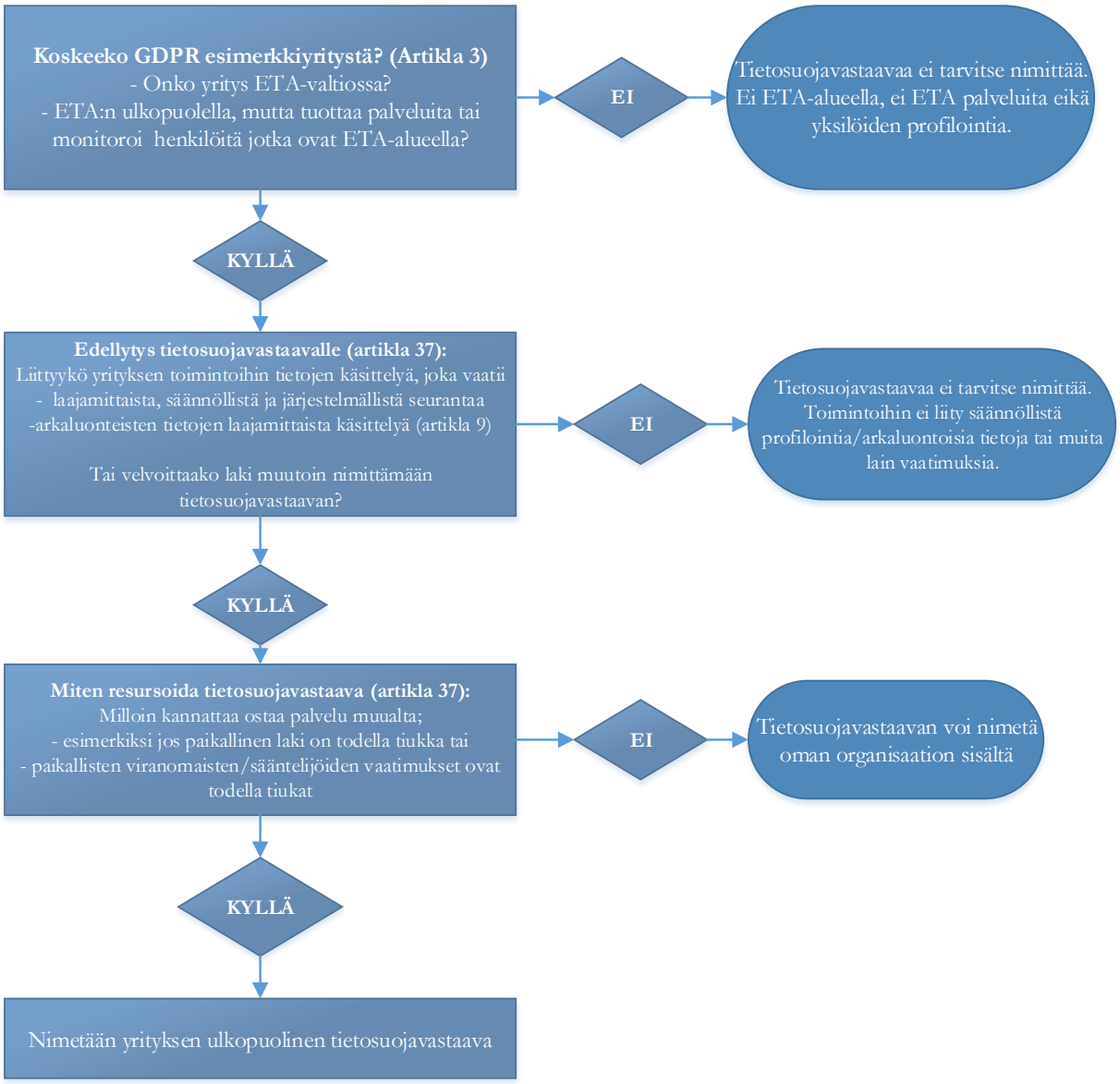
> ”Sellaisten henkilötietojen käsittely, joista ilmenee rotu tai etninen alkuperä, poliittisia mielipiteitä, uskonnollinen tai filosofinen vakaumus tai ammattiliiton jäsenyys sekä geneettisten tai biometristen tietojen käsittely henkilön yksiselitteistä tunnistamista varten tai terveyttä koskevien tietojen taikka luonnollisen henkilön seksuaalista käyttäytymistä ja suuntautumista koskevien tietojen käsittely on kiellettyä.” (Asetus yleisestä tietosuojasta 679/2016/EU.)

Esimerkkiyrityksen tulee selvittää, mikä on se peruste tai oikeutettu etu, jonka mukaan yrityksessä käsitellään henkilötietoja, joka on laissa säädetty. Nämä tulee myös dokumen-

toida osoitusvelvollisuuden täyttämiseksi. Henkilötietolain mukaiset oikeusperusteet eroavat hieman nyt asetuksessa säädetyistä perusteista. (Tietosuojavaltuutetun toimisto & Oikeusministeriö 2017, 19.)

3.2 Yrityksen johdon toimet

Esimerkkiyrityksen olisi ensiksi varmistuttava, onko yrityksen asetuksen määrittämällä tavalla nimettävä tietosuojavastaava. Tietosuojavastaava voi olla joko oman henkilöstön jäsen ja hoitaa tehtäviään palvelusopimuksen perusteella tai tietosuojavastaavaksi voi myös palkata ulkopuolisen tahon.



Kuva 2. Yllä kuvattu yksinkertaisella päätöspuulla, kuinka voi ratkaista tietosuojavastaavan tarpeen. (PricewaterhouseCoopers 2017.)

Oikeusministeriön julkaisu selventää, että tietosuojavastaavan tehtäviin kuuluu seurata henkilötietojen käsittelyn lainmukaisuutta ja toimia valvontaviranomaisen sekä rekisteröityjen yhteyspisteenä henkilötietojen käsittelyyn liittyvissä kysymyksissä. Johdolle kuuluu kuitenkin edelleen vastuu siitä, että yrityksessä käsitellään henkilötietoja lainmukaisesti, ei tietosuojavastaavalle.

Riippuen yrityksen toiminnasta, tietosuoja-asetus ei pakota nimittämään tietosuojavastaavaa, mutta esimerkkiyrityksessä on kuitenkin syytä määritellä henkilö, jonka tehtävänä on tietosuojaa koskevien asioiden huomioon ottaminen ja joka toimii yhteyshenkilönä rekisteröidyn oikeuksiin ja viranomaisvalvontaan liittyvissä kysymyksissä. (Tietosuojavaltuutetun toimisto & Oikeusministeriö 2017, 35.)

3.3 Yrityksen omat tietosuojaperiaatteet

Esimerkkiyrityksen kannattaa konsultoida asianmukaisia sidosryhmiä ja tehdä analyysi siitä, millaiset ovat yrityksen tämän hetken tietosuojaperiaatteet, noudattavatko ne nykyistä henkilötietolakia ja pohtia, tulisiko niitä muuttaa uuden asetuksen myötä. Eli olemassa olevia käytänteitä kannattaa verrata tietosuojalakiin ja uuteen asetukseen ja selvittää ovatko ne yhdenmukaisia. Sen jälkeen tulee päättää tavat, joilla asetuksen mukanaan tuoma kulttuurimuutos tulee tutuksi henkilöstölle; kuinka heidät koulutetaan ja ohjeistetaan niin, jotta periaatteet ovat kunnossa ja tietojen suojaaminen näkyy arjen töissä.

3.4 Henkilöstön henkilötietojen käsittely

Jos esimerkkiyrityksessä kerätään ja käsitellään työntekijöiden henkilötietoja, niin tällöin tulee pitää mielessä läpinäkyvyys informoinnissa eli henkilöstölle tulee kertoa, kuinka heidän tietojaan käsitellään, mihin niitä käytetään ja kuinka niitä suojataan. Läpinäkyvyydellä tarkoitetaan asetuksessa täydellistä ja tarkkaa tiedonantoa. Avoimet tiedonannot eivät saa olla harhaanjohtavia.

Asetuksen mukaan henkilötietojen käsittelyn suhteen on noudatettava seuraavia vaatimuksia:

a) ”niitä on käsiteltävä lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi (”lainmukaisuus, kohtuullisuus ja läpinäkyvyys”);
b) ne on kerättävä tiettyä, nimenomaista ja laillista tarkoitusta varten, eikä niitä saa käsitellä myöhemmin näiden tarkoitusten kanssa yhteen sopimattomalla tavalla; myöhempää käsittelyä yleisen edun mukaisia arkistointitarkoituksia taikka tieteellisiä tai historiallisia tutkimustarkoituksia tai tilastollisia tarkoituksia varten ei katsota 89 artiklan 1 kohdan mukaisesti yhteensopimattomaksi alkuperäisten tarkoitusten kanssa (”käyttötarkoitussidonnaisuus”);

c) henkilötietojen on oltava asianmukaisia ja olennaisia ja rajoitettuja siihen, mikä on tarpeellista suhteessa niihin tarkoituksiin, joita varten niitä käsitellään (”tietojen minimointi”);
d) henkilötietojen on oltava täsmällisiä ja tarvittaessa päivitettyjä; on toteutettava kaikki mahdolliset kohtuulliset toimenpiteet sen varmistamiseksi, että käsittelyn tarkoituksiin nähden epätarkat ja virheelliset henkilötiedot poistetaan tai oikaistaan viipymättä (”täsmällisyys”);
e) ne on säilytettävä muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan kuin on tarpeen tietojenkäsittelyn tarkoitusten toteuttamista varten; henkilötietoja voidaan säilyttää pidempiä aikoja, jos henkilötietoja käsitellään ainoastaan yleisen edun mukaisia arkistointitarkoituksia taikka tieteellisiä tai historiallisia tutkimustarkoituksia tai tilastollisia tarkoituksia varten 89 artiklan 1 kohdan mukaisesti edellyttäen, että tässä asetuksessa vaaditut asianmukaiset tekniset ja organisatoriset toimenpiteet on pantu täytäntöön rekisteröidyn oikeuksien ja vapauksien turvaamiseksi (”säilytyksen rajoittaminen”);
f) niitä on käsiteltävä tavalla, jolla varmistetaan henkilötietojen asianmukainen turvallisuus, mukaan lukien suojaaminen luvattomalta ja lainvastaiselta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta käyttäen asianmukaisia teknisiä tai organisatorisia toimia (”eheys ja luottamuksellisuus”).
g) Lisäksi on pystyttävä näyttämään, että vaatimuksia on noudatettu (”osoitusvelvollisuus”).” (Asetus yleisestä tietosuojasta 679/2016/EU.)

Esimerkkiyrityksessä tulisi siis olla henkilöstöhallinnon puolella täysi ymmärrys siitä, mitä henkilötietoja kerätään henkilöstöltä sekä miten ja mihin tarkoituksiin tietoja käytetään ja käsitellään. Jos käsittelyyn kuuluu arkaluonteisia tietoja henkilöstöstä, tulee arvioida, onko käsittely laajaa ja säännöllistä ja jos on, yrityksen tulisi tehdä riskien vaikutusten arviointi. Jos yrityksessä on eri liiketoimintayksikköjä, samat toimenpiteet tulee tehdä jokaisessa erikseen. Oikeusperusteen kannattaa sisältyä arvioinnin jälkeiseen dokumentointiin, esimerkiksi tulisi mainita oikeutetut edut. Henkilöstöhallinnon tietojenkäsittely- ja käytänteet kannattaa päivittää yhdenmukaisiksi tietosuoja-asetuksen kanssa.

3.4.1 Rekisteröidylle toimitettavat tiedot

Rekisterinpitäjän velvollisuutena on toteuttaa rekisteröidyn oikeuksia. Rekisteröidyn oikeuksia on parannettu ja ne ovat kuvattuna asetuksessa yksityiskohtaisemmin kuin tämän hetken laissa ja uusia oikeuksia on tullut jonkin verran lisää. Esimerkiksi kun henkilötietoja kerätään rekisteröidyltä, hänelle tulee Tietosuojavaltuutetun toimiston ja oikeusministeriön mukaan, samassa yhteydessä toimittaa muun muassa seuraavia tietoja:

- rekisterinpitäjän ja tapauskohtaisesti tämän mahdollisen edustajan identiteetti ja yhteystiedot;
- yrityksen tietosuojavastaavan yhteystiedot (jos on nimitetty)
- henkilötietojen käsittelyn tarkoitukset sekä käsittelyn oikeusperuste;

- rekisterinpitäjän tai kolmannen osapuolen oikeutetut edut
- henkilötietojen vastaanottajat tai vastaanottajaryhmät;
- tapauksen mukaan tieto siitä, että rekisterinpitäjä aikoo siirtää henkilötietoja kolmanteen maahan tai kansainväliselle järjestölle. (Tietosuojavaltuutetun toimisto & Oikeusministeriö 2017, 24.)

3.4.2 Seloste käsittelytoimista

Asetuksen 30 artikla säätää, että jokaisen rekisterinpitäjän on ylläpidettävä selostetta vastuullaan olevista käsittelytoimista. Asetuksen 30 artiklan mukaan:

> ”Selosteen on käsitettävä kaikki seuraavat tiedot:
> a) rekisterinpitäjän ja mahdollisen yhteisrekisterinpitäjän, rekisterinpitäjän edustajan ja tietosuojavastaavan nimi ja yhteystiedot;
> b) käsittelyn tarkoitukset;
> c) kuvaus rekisteröityjen ryhmistä ja henkilötietoryhmistä;
> d) henkilötietojen vastaanottajien ryhmät, joille henkilötietoja on luovutettu tai luovutetaan, mukaan lukien kolmansissa maissa tai kansainvälisissä järjestöissä olevat vastaanottajat;
> e) tarvittaessa tiedot henkilötietojen siirtämisestä kolmanteen maahan tai kansainväliselle järjestölle, mukaan lukien tieto siitä, mikä kolmas maa tai kansainvälinen järjestö on kyseessä, sekä asianmukaisia suojatoimia koskevat asiakirjat, jos kyseessä on 49 artiklan 1 kohdan toisessa alakohdassa tarkoitettu siirto;
> f) mahdollisuuksien mukaan eri tietoryhmien poistamisen suunnitellut määräajat;
> g) mahdollisuuksien mukaan yleinen kuvaus 32 artiklan 1 kohdassa tarkoitetuista teknisistä ja organisatorisista turvatoimista.” (Asetus yleisestä tietosuojasta 679/2016/EU.)

Samoin kunkin henkilötietojen käsittelijän ja tarvittaessa henkilötietojen käsittelijän edustajan on ylläpidettävä selostetta kaikista rekisterinpitäjän lukuun suoritettavista käsittelytoimista. Selosteiden on oltava kirjallisia ja sähköisessä muodossa. Selosteet on annettava valvontaviranomaisille pyydettäessä. Nämä velvollisuudet eivät kuitenkaan koske yritystä tai järjestöä, jossa on alle 250 työntekijää. (Tietosuojavaltuutetun toimisto & Oikeusministeriö 2017, 18.)

3.5 Yrityksen markkinointi

Markkinoinnilla on laaja merkitys ja se sisältää toimintaa, jonka tarkoituksena on edistää organisaation tuotteita ja palveluita. Suoramarkkinointi edellyttää sitä, että henkilöihin otetaan suoraan yhteyttä esimerkiksi postitse, puhelimitse tai sähköpostitse, kun taas epä-

suora markkinointi usein liittyy kolmannen osapuolen välityksellä tapahtuvaan kommunikointiin.

Markkinointiin saattaa joskus kuulua analyysien tekoa tai henkilön profilointia, jotta pystytään luokittelemaan heitä, joille markkinointi on suunnattu. Analyysien oikeellisuuden määrittäminen on haastavaa ja siinä tulee ottaa myös muu lainsäädäntö kuin tietosuojalaki huomioon. Jotkut suoramarkkinointilait sovelletaan henkilön kansalaisuuden perusteella, jolle markkinointi on suunnattu. Tästä johtuen on tärkeää ymmärtää millaisia lakeja - paikallisia ja mahdollisesti ulkomaisia - liittyy tietosuojaan, markkinointiin, kilpailuun, sähköiseen viestintään jne. Henkilötietojen käsittelyyn markkinoinnissa on oltava laillinen edellytys. EU:ssa on tavallisesti mahdollista markkinoida perustuen "oikeutettuun etuun". Markkinoinnissa tulee myös huomioida 7 artiklan maininta siitä, että jos tietojenkäsittely perustuu suostumukseen, rekisterinpitäjän on pystyttävä osoittamaan, että rekisteröity on antanut suostumuksen henkilötietojensa käsittelyyn. Markkinointia hoitavien tulisi esimerkkiyrityksessä tehdä analyysi ja dokumentointi markkinointitoiminnan tyypeistä (suora tai epäsuora markkinointi), käytetyistä viestintäkanavista ja pohtia mihin markkinointitoiminta on kohdistunut ja käyttää tätä dokumentaatiota jatkossa apuvälineenä varmistamaan lain mukaiset toimet.

3.5.1 Suostumus tiedon keräämiseen ja käyttämiseen

Pynnä kertoo blogissaan (Pynnä,16.01.2018.), että tämän hetken laki ja asetuksen jälkeinen tilanne on melko samanlainen. Erojakin löytyy kuten se, että yrityksen on pyydettävä suostumus selkokielisenä tiedon keräämiseen ja käyttämiseen sekä sillä tapaa, että sen selkeästi erottaa muusta sisällöstä. Yrityksen on myös pystyttävä osoittamaan, että suostumus on annettu. Suostumuksen dokumentoinnista on hyvä käydä ilmi, kuka on antanut suostumuksen, mihin on suostuttu, milloin ja millä tapaa suostumus on annettu. Lisäksi pitää ilmoittaa rekisteröidylle hänen mahdollisuudestaan peruuttaa suostumus milloin tahansa. Palvelun tarjoamisen ehdoksi ei voi asettaa suostumusta sellaisten henkilötietojen käsittelyyn, jotka eivät ole tarpeen kyseisen palvelusopimuksen täytäntöönpanoa varten. Suostumuksen peruuttaminen ei vaikuta aiemmin suoritetun käsittelyn lainmukaisuuteen, joka on tehty rekisteröidyn suostumuksella.

Suostumuksen dokumentointiin ja peruuttamiseen ovat hyviä vaihtoehtoja esimerkiksi kirjallisen dokumentin allekirjoittaminen, “opt-in” näppäin, kyllä/ei-valinta, valinnat asetuspaneelissa, sähköpostivastaus, jossa pyydetään suostumusta, myöntävä vastaus suulliseen luvan kysymiseen tai vapaaehtoisten tietojen antaminen tiettyyn tarkoitukseen. (Pynnä,16.01.2018.)

3.6 Yrityksen asiakkuudet ja toimeksiannot

Esimerkkiyrityksen tulisi tarkastaa ja päivittää tietosuojaehdot asiakkaiden toimeksiantosopimuksissa, mukaan lukien sovitut palveluehdot. Yrityksen tulisi myöskin päättää kuinka toimia tilanteissa, joissa vain asiakkaalla on suora yhteys henkilöihin, joista kerätään henkilötietoja. Lisäksi tulisi tehdä päätös henkilötietojen hallinnoijan / käsittelijän erottelusta. Tämä on monimutkaista, sillä asetus on tämän osalta vielä hyvin tulkinnanvarainen. Yrityksen olisi suositeltavaa kehittää strategia tietosuojaan liittyvien sopimusehtojen muutoksista ja kuinka pyynnöt niistä hoidetaan ja käsitellään.

3.7 Kolmansien osapuolten kanssa tehdyt sopimukset

Esimerkkiyrityksen tulee pohtia mitä palveluita käytetään ja minkälaisia sopimuksia heillä on olemassa kolmansien osapuolten kanssa. Sen jälkeen näistä tulee tunnistaa missä liikkuu henkilötietoa tai onko yrityksen ulkopuolisilla pääsyä niihin. Näitä voi olla esimerkiksi:

- Vuokratyöntekijöiden välitysfirmat
- Teknologiatoimittajat (SaaS, pilvi, datakeskuspalvelut jne.)
- Yrityspalvelut (esim. matkailupalvelut ja hotellit)
- Konsultit ja muut palveluntarjoajat
- Alihankkijat, joita käytetään toimeksiannoissa

Rekisterinpitäjälle tulee myös uusi velvoite käyttää vain sellaisia henkilötietojen käsittelijöitä, jotka toteuttavat suojatoimet asianmukaisten teknisten ja organisatoristen toimien täytäntöön panemiseksi niin, että käsittely täyttää tietosuoja-asetuksen vaatimukset. (Asetus yleisestä tietosuojasta 679/2016/EU.)

Rekisterinpitäjän lukuun henkilötietoja käsittelevistä tahoista kannattaa tehdä erillinen listaus, jossa näkyy vähintään kummankin osapuolen nimi, kuka sopimuksia hallinnoi jne. Tarvittaessa tulee päivittää sopimuksia näiden kolmansien osapuolten kanssa, jotka sitovat henkilötietojen käsittelijää suhteessa rekisterinpitäjään ja jossa vahvistetaan käsittelyn kohde ja kesto, käsittelyn luonne ja tarkoitus, henkilötietojen tyyppi ja rekisteröityjen ryhmät, rekisterinpitäjän velvollisuudet ja oikeudet. Pitää myös olla selvää, että henkilötietojen käsittelijä ei saa käyttää toisen henkilötietojen käsittelijän palveluksia ilman rekisterinpitäjän erityistä ennakkolupaa ja lisäksi asetuksen 28 artikla säätää tarkat ehdot mitä henkilötiedon käsittelijän velvollisuuksiin kuuluu. (Asetus yleisestä tietosuojasta 679/2016/EU.)

3.8 Tietoturvaloukkauksien ilmoitusvelvollisuus

Tietosuoja-asetuksessa säädetään, että rekisterinpitäjällä on velvollisuus ilmoittaa tietosuojaviranomaiselle ja rekisteröidylle henkilötietojen tietoturvaloukkauksista. Mahdollisissa korkean riskin tapauksissa on ilmoitettava myös rekisteröidylle loukkauksesta. Viranomaisilmoitukseen on annettu vain kolmen vuorokauden eli tarkemmin 72 tunnin aikaraja, jolloin ilmoitus on tehtävä. Aika lähtee juoksemaan suoraan tietoturvaloukkauksen havaitsemisesta, eikä se katso viikonpäivää eikä pyhiä. Ilmoituksen voi olla tekemättä, mikäli loukkauksesta ei todennäköisesti aiheudu luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvaa riskiä. Henkilötietojen käsittelijän on puolestaan ilmoitettava viipymättä rekisterinpitäjälle tietoturvaloukkauksesta. Rekisterinpitäjän velvollisuus on taas dokumentoida kaikki henkilötietojen tietoturvaloukkaukset, loukkauksen vaikutukset ja toteutetut korjaavat toimet. Valvontaviranomaisen pitää pystyä dokumentoinnin avulla tarkistamaan, että rekisterinpitäjä on noudattanut ilmoitusvelvollisuuttaan.
(Tietosuojavaltuutetun toimisto & Oikeusministeriö 2017, 32.)

Tietoturvaloukkausten varalle tulisi kehittää prosessi, jotta tietoturvaloukkaukseen liittyvien ilmoitusvelvollisuuksien täyttäminen olisi mahdollisimman tehokasta ja ylipäätään mahdollista. Esimerkkiyrityksen kannattaa tehdä prosessikuvaus siitä, miten ohjeistetaan henkilöstöä tunnistamaan tietoturvaloukkaus, valita ne kanavat joissa siitä ilmoitetaan, kuinka tapaukset dokumentoidaan ja selvitetään ja miten koko prosessi toimii tehokkaasti vahinkojen minimoimiseksi. (Tietosuojavaltuutetun toimisto & Oikeusministeriö 2017, 32.)

3.9 Järjestelmät ja sovellukset

Esimerkkiyrityksen tulee ottaa huomioon henkilötietojen käsittelyyn liittyvien prosessien ja tietojärjestelmien suunnittelussa rekisteröidyn oikeudet. Käytetyistä järjestelmistä ja sovelluksista kannattaa kirjata järjestelmärekisteri, jossa käy ilmi minkälaista dataa ne sisältävät. Mikäli sovelluksissa tai järjestelmissä havaitaan henkilötietoihin liittyviä tietoturvariskejä, niiden käyttöä tulee arvioida uudelleen ja tehdä kehityssuunnitelma datan tietoturvan ja tietosuojan parantamiseksi. Tulevaisuudessa uusien järjestelmien hankinnassa tulee myös tehdä tietosuojavaikutusten arvioinnit ja varmistaa ohjelmistojen turvallisuus ennen hankintoja.

Oikeusministeriön julkaisu (Tietosuojavaltuutetun toimisto & Oikeusministeriö 2017, 31.) kannustaa tietojen suojaamiseen kaikissa käsittelyn vaiheissa alkaen tietojen keräämisestä ja päättyen tietojen tuhoamiseen. Käsittelyn turvallisuus edellyttää esimerkiksi kykyä taata järjestelmien ja palveluiden luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus sekä varmuuskopioiden palautuskyky ja pääsy tietoihin fyysisen tai teknisen vian sattues-

sa. Tietojen suojaaminen edellyttää myös henkilötietojen käsittelyn seuraamista ja valvontaa.

3.10 Tietosuojariskiarvio

Tietosuojariskiarviointi on arviointi riskeistä, jotka liittyvät henkilötietojen käsittelyyn asiakassitoumuksissa, sisäisissä prosesseissa / projekteissa sekä tietoteknisten sovellusten käyttöönotossa tai päivityksissä. Koska esimerkkiyritys sijaitsee ETA:n alueella ja kerää, käsittelee ja käyttää henkilötietoja henkilöistä, tietosuojariskiarvioinnin teko kirjallisena on asetuksen edellytysten hengenmukaista. Tietosuojariskiarvioinnin tuloksista selviää, onko käsittelyssä henkilötietoja, jotka saattavat aiheuttaa riskin yksilöille. Jos näin on, tulee suorittaa tietosuojaa koskeva vaikutusten arviointi ennen projektin aloittamista.

3.11 Rekisteröidyn oikeudet

Henkilötietolain mukaiseen tarkastusoikeuteen nähden asetus on jälleen hieman yksityiskohtaisempi, kun puhutaan rekisteröidyn oikeudesta omiin henkilötietoihinsa. Alla kuvataan tarkemmin näitä oikeuksia.

3.11.1 Rekisteröidyn oikeus saada pääsy tietoihin

Toisin kuin henkilötietolaissa, tietosuoja-asetuksessa ei määrätä muotoa rekisteröidyn pyynnölle päästä käsiksi häntä koskeviin henkilötietoihin. Jos hän lähettää pyynnön sähköisesti, rekisterinpitäjän on toimitettava tiedot yleisesti käytetyssä sähköisessä muodossa, ellei rekisteröity toisin pyydä. (Tietosuojavaltuutetun toimisto & Oikeusministeriö 2017, 24.)

> ”Tietosuoja-asetuksessa aikaraja rekisteröidyn esittämään pyyntöön reagoimiselle on yksi kuukausi. Määräaikaa voidaan tarvittaessa jatkaa enintään kahdella kuukaudella ottaen huomioon pyyntöjen monimutkaisuus ja määrä. Rekisterinpitäjän on ilmoitettava rekisteröidylle mahdollisesta määräajan jatkamisesta kuukauden kuluessa pyynnön vastaanottamisesta sekä kerrottava viivästymisen syyt.” (Tietosuojavaltuutetun toimisto & Oikeusministeriö 2017, 25.)

Asetuksessa mainitaan myös, että rekisteröidyn tulee lisäksi saada tieto käsittelyn tarkoituksesta, henkilötietoryhmästä, henkilötiedon vastaanottajasta ja erityisesti kolmansissa maissa olevista vastaanottajista tai kansainvälisistä järjestöistä, joille henkilötietoja on luovutettu tai on tarkoitus luovuttaa, mahdollisuuksien mukaan henkilötietojen suunnitellusta säilytysajasta. Rekisteröidyllä on oikeus pyytää rekisterinpitäjältä häntä itseään koskevien henkilötietojen oikaisemista tai poistamista.

3.11.2 Oikeus tietojen oikaisemiseen tai poistamiseen

Tietosuoja-asetus takaa 17 artiklan mukaan rekisteröidylle oikeuden tietojen oikaisemiseen sekä oikeuden tietojen poistamiseen ja tätä kutsutaan oikeudeksi tulla unohdetuksi. Henkilötietolaki sisältää myös vastaavat oikeudet, joten tässä ei sinänsä ole mitään uutta. Lisäksi kuitenkin asetus määrää velvollisuudesta ilmoittaa tiedon korjaamisesta sille, jolle rekisterinpitäjä on luovuttanut tai jolta rekisterinpitäjä on saanut henkilötiedon.

Jos henkilö haluaa poistaa tietonsa, tulee ne poistaa tietyin poikkeuksin, esimerkiksi jos niitä ei enää tarvita laillisiin tarkoituksiin, joita varten ne kerättiin tai rekisteröity peruuttaa suostumuksen, johon käsittely on perustunut eikä käsittelyyn ole muuta laillista perustetta. (Asetus yleisestä tietosuojasta 679/2016/EU.)

3.11.3 Oikeus käsittelyn rajoittamiseen

Rekisteröidyllä on oikeus saada häntä koskevien henkilötietojen aktiivinen käsittely rajoitetuksi. Oikeus on olemassa muun muassa silloin, kun rekisteröity kiistää henkilötietojen paikkaansa pitävyyden esittämällä henkilötietojen oikaisua tai poistoa koskevan pyynnön. Henkilötietojen käsittelyn rajoittamista koskevia menetelmiä voivat olla esimerkiksi valittujen tietojen siirtäminen toiseen käsittelyjärjestelmään tai käyttöoikeuksien rajoittaminen valittuihin henkilötietoihin. Käsittelyn rajoittaminen on varmistettava teknisesti niin, etteivät henkilötiedot joudu käsittelytoimenpiteiden kohteeksi. Rekisterinpitäjä saa edelleen säilyttää tietoja, muttei muutoin käsitellä niitä ilman rekisteröidyn suostumusta. Rekisterinpitäjä saa käsitellä rekisteröidyn henkilötietoja myös esimerkiksi oikeudellisen vaateen laatimiseksi, esittämiseksi tai puolustamiseksi tai tärkeää jäsenvaltion etua koskevista syistä. (Tietosuojavaltuutetun toimisto & Oikeusministeriö 2017, 26.)

3.11.4 Oikeus siirtää tiedot järjestelmästä toiseen

Asetuksen 21 artikla määrittää seuraavaa rekisteröityjen oikeudesta siirtää henkilötietojaan;

> ”Rekisteröidyllä on oikeus saada häntä koskevat henkilötiedot, jotka hän on toimittanut rekisterinpitäjälle, jäsennellyssä, yleisesti käytetyssä ja koneellisesti luettavassa muodossa, ja oikeus siirtää kyseiset tiedot toiselle rekisterinpitäjälle sen rekisterinpitäjän estämättä, jolle henkilötiedot on toimitettu”. (Asetus yleisestä tietosuojasta 679/2016/EU.)

Esimerkkiyrityksen tulisi siis varmentua siitä, että pystyy toimittamaan kyseiset tiedot juuri sillä tavalla kuten rekisteröity pyytää ja että järjestelmistä pystytään tuottamaan ulos valitut tiedot ja että ne saadaan mainitussa muodossa.

3.11.5 Vastustamisoikeus

Asetus takaa, että rekisteröidyllä on oikeus erityiseen tilanteeseensa liittyvällä perusteella, milloin tahansa vastustaa häntä koskevien henkilötietojen käsittelyä ja näin ollen kieltää niiden käytön. Rekisterinpitäjä ei saa enää käsitellä henkilötietoja, jos näin tapahtuu. Ainoastaan jos rekisterinpitäjä kykenee osoittamaan, että käsittelyyn on olemassa tärkeä, oikeutettu ja perusteltu syy, joka syrjäyttää rekisteröidyn edut, oikeudet ja vapaudet. (Asetus yleisestä tietosuojasta 679/2016/EU.) Tietosuojavaltuutetun toimiston ja oikeusministeriön mukaan;

> ”Vastustamisoikeus liittyy vain osaan käsittelyperusteista. Se kattaa käsittelyn, joka perustuu yleistä etua koskevan tehtävän suorittamiseen tai rekisterinpitäjälle kuuluvan julkisen vallan käyttöön sekä rekisterinpitäjän tai kolmannen oikeutetun edun toteuttamiseen. Lisäksi vastustamisoikeus koskee käsittelyä suoramarkkinointia varten sekä tietyin edellytyksin myös käsittelyä tieteellistä, historiallista tai tilastollista tutkimusta varten, tästä oikeudesta voidaan kuitenkin säätää poikkeuksia kansallisella lailla. ” (Tietosuojavaltuutetun toimisto & Oikeusministeriö 2017, 26.)

3.12 Henkilötietojen säilyttäminen ja käyttörajoitukset

Esimerkkiyrityksen tulee tarkastella tiedon säilytys- ja hävittämiskäytäntöjään varmistaakseen, että henkilötietoja ei säilytetä pidempään kuin on tarpeen tai jos niitä on säilytettävä, on dokumentoitava syyt siihen ja varmistaa, että asianmukaiset käyttöoikeustarkastukset tehdään säännöllisesti. Kannattaa myös harkita rekisteritietojen säilyttämisaikataulua, joka määrittelee tallennetut tiedot (tietueet), joita olisi säilytettävä ja kuinka kauan ne pitäisi säilyttää. Lisäksi on hyvä suunnitella tietojen hävittämiskäytäntö ja sen dokumentointi, jossa kuvataan yksityiskohtaisesti tiedon käsittelyä.

Asetus toteaa, että henkilötiedot;

> ”on säilytettävä muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan kuin on tarpeen tietojenkäsittelyn tarkoitusten toteuttamista varten; henkilötietoja voidaan säilyttää pidempiä aikoja, jos henkilötietoja käsitellään ainoastaan yleisen edun mukaisia arkistointitarkoituksia taikka tieteellisiä tai historiallisia tutkimustarkoituksia tai tilastollisia tarkoituksia varten 89 artiklan 1 kohdan mukaisesti edellyttäen, että tässä asetuksessa vaaditut asianmukaiset tekniset ja organisatoriset toimenpiteet on pantu täytäntöön rekisteröidyn oikeuksien ja vapauksien turvaamiseksi (”säilytyksen rajoittaminen”)” (Asetus yleisestä tietosuojasta 679/2016/EU.)

Henkilötietojen käyttö tulee siis rajata kerättyihin tarkoituksiin. Jos henkilötietojen käsittelylle ilmenee uusia tarkoituksia, tulisi ottaa yhteyttä tietosuojasta vastuussa oleviin ja varmistaa ovatko kyseiset uudet tarkoitukset asiaankuuluvia ja sopimusten mukaisia.

3.13 Viranomaistahot

Tietosuoja-asetuksen myötä rekisterinpitäjän tarvitsee asioida vain yhden jäsenvaltion valvontaviranomaisen kanssa. Toimivaltainen valvontaviranomainen määräytyy rekisterinpitäjän tai henkilötietojen käsittelijän toimipaikan tai päätoimipaikan mukaan. Toimivaltaista valvontaviranomaista kutsutaan johtavaksi valvontaviranomaiseksi ja se toimii rekisterinpitäjän tai henkilötietojen käsittelijän ainoana yhteyspisteenä kaikissa henkilötietojen käsittelyyn liittyvissä kysymyksissä. Yrityksen tulee huomioida, että asetuksessa annettu päätoimipaikan määritelmä eroaa rekisterinpitäjän ja henkilötietojen käsittelijän välillä. (Tietosuojavaltuutetun toimisto & Oikeusministeriö 2017, 29.)

Asetuksessa lukee yhteistyöstä valvontaviranomaisen kanssa seuraavaa:

> ”Rekisterinpitäjän ja henkilötietojen käsittelijän sekä tarvittaessa rekisterinpitäjän tai henkilötietojen käsittelijän edustajan on pyynnöstä tehtävä yhteistyötä valvontaviranomaisen kanssa sen tehtävien suorittamiseksi.” (Asetus yleisestä tietosuojasta 679/2016/EU.)

3.14 Henkilöstön kouluttaminen

Asetus ei määrää henkilöstön kouluttamisesta nimenomaisesti, mutta henkilötiedon suojaus ja henkilöstön sitoutuminen toimenpiteisiin niitä suojatakseen, tulisi näkyä käytännön arjessa. Jokaisen tulisi huolehtia omalta osaltaan henkilötiedoista, joita säilytetään esimerkiksi omilla työkoneilla. Jokainen on itse vastuussa näistä. Näin ollen koulutusta tulisi tarjota vähintään henkilöstölle, jotka käsittelevät henkilötietoja työssään, kolmansien osapuolten ja asiakkaiden kanssa asioiville ja myös antaa ohjeistusta tietosuojaa ja tietoturvaa koskevissa kysymyksissä. Tietoturvaloukkauksissa eri tilanteita varten tulisi laatia toimintaohjeet, minkä lisäksi tulisi huolehtia henkilöstön osaamisesta kriisitilanteessa. Esimerkkiyrityksen olisi hyvä järjestää ainakin pienimuotoinen pakollinen koulutus omalle henkilöstölleen ja pitää mahdollisesti tietoiskuja aiheesta.

Esimerkkiyrityksen kannattaa täten miettiä oikeita tapoja ja väyliä, miten ja kenen suunnasta kannattaa viestiä omalle henkilöstölle. Viestejä voidaan kommunikoida monella eri tavalla. Kannattaa siis valita oikeanlaiset toimenpiteet, jotka perustuvat haluttuun sitoutumistasoon, ei tule myöskään luottaa vain yhteen viestintäkanavaan, jotta haluttu lopputulos varmasti saavutetaan. Liitteessä 1 on kuvattuna eri kanavat, joita voi hyödyntää. (PricewaterhouseCoopers 2017.)

4 Pohdinta

Henkilötietojen suojaaminen on kaiken tekemisen ydin. Meillä kaikilla on vastuu rajoittaa, suojella ja kunnioittaa henkilökohtaisia tietoja, joiden parissa työskentelemme päivittäin. On monia tekijöitä, jotka on otettava huomioon, jotta voi käsitellä henkilötietoja oikein. Henkilötietojen käsittelyssä tulee ensisijaisesti muistaa rajoittaa, suojata ja kunnioittaa niitä. Näin toimimalla vähennämme riskejä, jotka voivat liittyä yrityksen maineen menettämiseen tai ovat taloudellisia tai juridisia. Tietosuojaperiaatteita tulee tarkastella säännöllisesti sekä varmistua siitä, että henkilöstö kykenee tunnistamaan ja raportoimaan tietoturvaloukkaukset vaaditulla tavalla. Henkilötietojen käsittelyn riskiarvioinnit on toteutettava hankkeissa ja prosesseissa, joihin sisältyy henkilötietojen käsittelyä. Tässä opinnäytetyössä yritettiin käyttää paljon konkreettisia esimerkkejä, mitä oikeassa arjessa voi tulla eteen.

Tietosuoja-asetuksen ollessa valmisteilla ja tarkentuessa opinnäytetyön edetessä, jotkin asetuksen artiklat ovat olleet hyvin tulkinnanvaraisia ja ymmärrys on ollut vaihteleva eri sisällöntuottajilla. Opinnäytetyön aihe on tällä hetkellä niin ajankohtainen, että aiheesta löytyy tuhansittain artikkeleita ja erilaisia julkaisuja. Tekijällä oli myös mahdollisuus osallistua muutamaan tietosuoja-asetusta käsittelevään luentoon työnsä puolesta, mutta luennot eivät vastanneet aivan opinnäytetyönkuvaa. Lähteiden valinnassa onkin tehty ratkaisu, että päätelmät tehtiin lähes yksinomaan asetukseen ja viranomaislähteisiin perustuen materiaalin paljouden vuoksi.

Tähän aiheeseen tutustuessa ja siitä kirjoittaessa, on ollut tärkeää seurata virallista tiedottamista, koska asiat ovat vasta täsmentyneet ajan kuluessa. Koska opinnäytetyöllä ei ollut varsinaista toimeksiantajaa, haasteita ilmeni etenkin työn rajaamisessa. Tämän hetken tietosuojalaki ja uusi tietosuoja-asetus ovat itsessään jo niin laajoja, että aihe-aluetta olisi pitänyt rajata tarkemmin ja ottaa aikataulu paremmin huomioon. Lisäksi olisi ollut ajallisesti mahdotonta tutustua uuteen lakiehdotukseen ja sisällyttää siitä asioita työhön, vaikka tämä olisikin ollut oleellista aiheeseen liittyen. Opinnäytetyön tekstityyliin oli osaltaan hankala vaikuttaa, sillä lakiteksti on tyyliltään melko uniikkia ja tekijä koki sen muotoilun lähes mahdottomaksi.

Työn valmistuessa oppimistavoitteeseen on päästy ja opinnäytetyöntekijällä on todella kattava kuva ja osaamista tietosuoja-asetuksesta. Osaaminen edesauttaa tekijän toimintatapoja työelämässä ja tätä osaamista pystyy hyödyntämään projekteissa, joissa vaaditaan tietosuojaan perehtynyttä henkilöä. Kaikenkaikkiaan voi todeta, että selvityksestä saatu

osaaminen on myös yleistiedon kannalta tärkeää, sillä asetus koskee niin montaa yritystä ja yhteisöä, ettei asian tuntemuksesta voi olla kuin hyötyä. Asetus ei toki koske yksityishenkilöiden kirjanpitoa tai muuta, joissa saattaa olla henkilötietoja eli oppia ei sentään tarvitse hyödyntää työn ulkopuolella. Tulevaisuudessa on jännittävää nähdä, miten lopullinen tietosuojalaki muotoutuu. Toukokuun jälkeen tullaan varmasti kuulemaan ennakkotapauksista ja näkemään mitä käy muun muassa koskien rekisteröityjen lähettämiä tietopyyntöjä, julkisuuteen nousseita tietoturvaloukkauksia ja asetuksen laiminlyönnistä aiheutuneita seuraamuksia.

Lähteet

Euroopan komissio. Mitä tarkoittaa 'oikeutettu etu'? Luettu 16.3.3018. https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/what-does-grounds-legitimate-interest-mean_fi

Euroopan parlamentin ja neuvoston asetus luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (EU) 2016/679. Luettavissa: http://eur-lex.europa.eu/legal-content/FI/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.FIN&toc=OJ:L:2016:119:FULL

Oikeusministeriö ja tietosuojavaltuutetun toimisto 2017. Miten valmistautua EU:n tietosuoja-asetukseen? Selvityksiä ja ohjeita. Helsinki. Luettavissa: http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/1Em8rT7IF/Miten_valmistautua_EUn_tietosuoja-asetukseen.pdf

OpiTietosuojaa.fi 2018. Luettu 16.3.3018. https://opitietosuojaa.fi/index.php/fi/56-lainsaeaedaentoe/lait/eun-tietosuoja-asetus/23-tuleva-eu-n-tietosuoja-asetus

Perko J. 07.06.2016. 5 väärää luuloa EU:n tietosuoja-asetuksesta. Luettavissa: https://www.asml.fi/blogi/eu-tietosuoja-5-luuloa/

PricewaterhouseCoopers 2017. Intranet. NDPP Implementation Toolkit. Luettu: 25.11.2017.

PricewaterhouseCoopers 2017. Intranet. Change Management Guidance and Tools. Luettu: 26.11.2017.

PricewaterhouseCoopers 2017. Intranet. Guidance on how to use the DPO Decision Tree. Luettu: 26.11.2017.

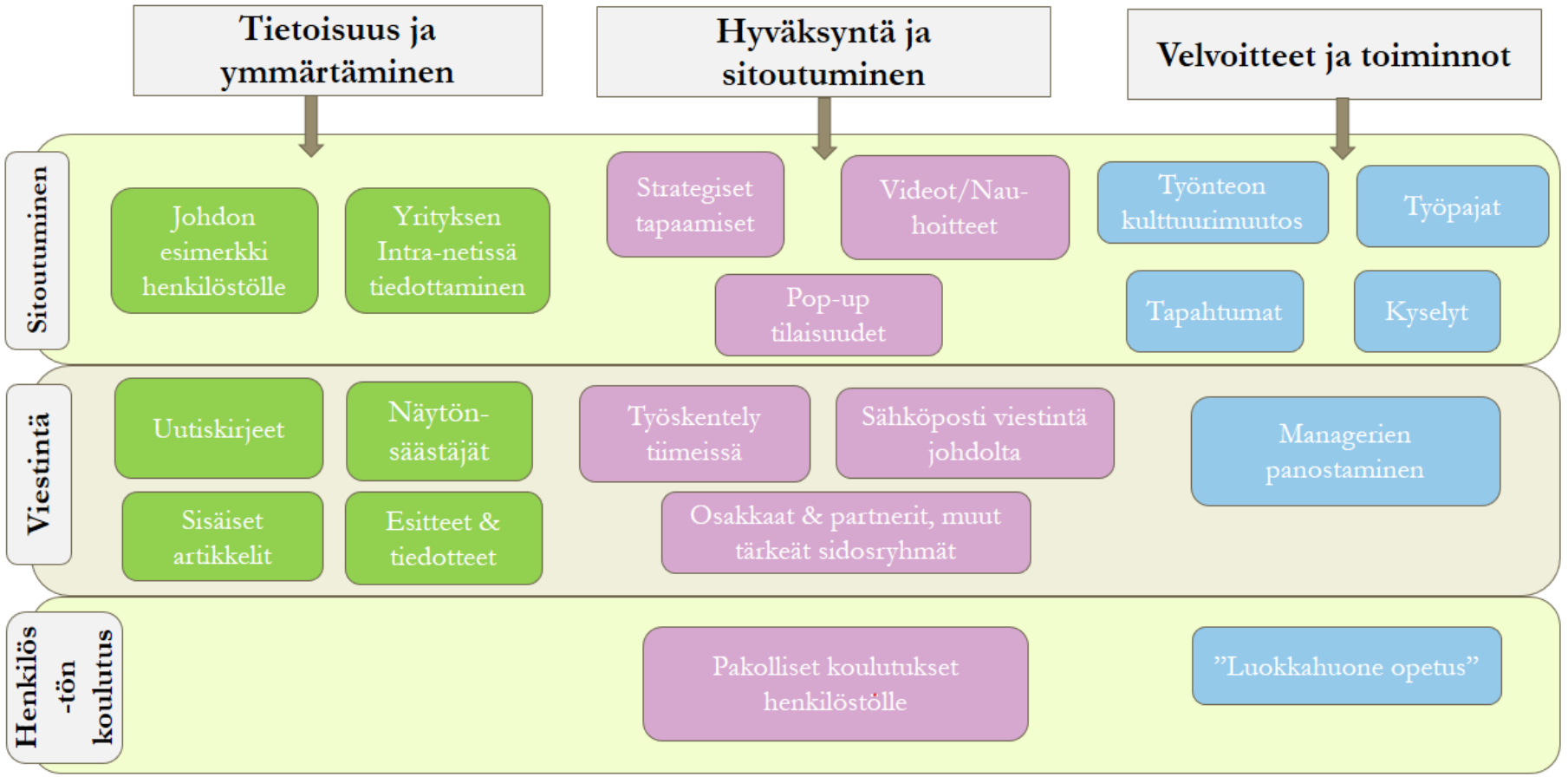
Pynnä P. 16.01.2018. Puretaan myyttejä – GDPR ja suostumus. Luettavissa: https://www.asml.fi/blogi/gdpr-eu-tietoosuoja-asetus-suostumus/

Tietosuojavaltuutetun toimisto 2017. Tietosuojapäivän teemoina tietosuoja-asetus ja kansalaisten tiedolliset oikeudet. Luettu: 13.2.2018. http://www.tietosuoja.fi/fi/index/ajankohtaista/tiedotteet/2017/01/tietosuojapaivanteemoinatietosuoja-asetusjakansalaistentiedollisetoikeudet_0.html

Tietosuojavaltuutetun toimisto 2017. EU:n tietosuojauudistus. Luettavissa: http://www.tietosuoja.fi/fi/index/euntietosuojauudistus.html#mitenvalmistautuatietosuoja-asetukseen

Valiokunnan lausunto PeVL142018 vp – HE 9/2018 vp. Luettavissa: https://www.eduskunta.fi/FI/vaski/Lausunto/Sivut/PeVL_14+2018.aspx

Liite 1


Tietoisuus ja ymmärtäminen
Hyväksyntä ja sitoutuminen
Velvoitteet ja toiminnot
Sitoutuminen
Johdon esimerkki henkilöstölle
Yrityksen Intra-netissä tiedottaminen
Strategiset tapaamiset
Videot/Nau-hoitteet
Pop-up tilaisuudet
Työnteon kulttuurimuutos
Työpajat
Tapahtumat
Kyselyt
Viestintä
Uutiskirjeet
Näytön-säästäjät
Sisäiset artikkelit
Esitteet & tiedotteet
Työskentely tiimeissä
Sähköposti viestintä johdolta
Osakkaat & partnerit, muut tärkeät sidosryhmät
Managerien panostaminen
Henkilös-tön koulutus
Pakolliset koulutukset henkilöstölle
”Luokkahuone opetus”