EU:N TIETOSUOJA-ASETUS JA SEN VAATIMAT KÄYTÄNNÖN MUUTOKSET TILITOIMISTOSSA

LAHDEN AMMATTIKORKEAKOULU
Tradenomi (AMK)
Liiketalous
Syksy 2018
Annika Lamminen
Eija Rantanen

Tiivistelmä

Tekijät	Julkaisun laji	Valmistumisaika
Lamminen, Annika Rantanen, Eija	Opinnäytetyö, AMK	Syksy 2018
	Sivumäärä 84 sivua	

Työn nimi

EU:n tietosuoja-asetus ja sen vaatimat käytännön muutokset tilitoimistossa

Tutkinto

Tradenomi (AMK)

Tiivistelmä

Työn aiheena oli EU:n tietosuoja-asetus ja sen vaatimat käytännön muutokset tilitoimistossa. Tavoitteena oli selvittää mitä muutoksia asetus aiheuttaa tilitoimistossa sekä helpottaa pienten tilitoimistojen selviytymistä asetuksen vaatimista toimenpiteistä. Saatujen tutkimustulosten perusteella pystyttiin arvioimaan tilitoimistojen halua ja resursseja asetuksen edellyttämien selosteiden laatimiseksi ja tietosuojan tason turvaamiseksi.

Opinnäytetyö koostui teoreettisesta ja empiirisestä osasta. Teoriaosuuden sisältö oli koottu aiheeseen liittyvistä luennoista ja kirjallisista sekä sähköisistä teoksista ja julkaisuista. Teoriaosuus jakautui kolmeen osaan. Ensimmäinen teorialuku käsitteli EU:n tietosuoja-asetusta yleisesti ja toisessa luvussa syvennyttiin tarkemmin asetuksen seitsemään yleiseen periaatteeseen. Kolmannessa teorialuvussa käytiin läpi keskeisiä muutoksia, joita asetuksen myötä on tilitoimistoille aiheutunut sekä muutoksien vaatimia käytännön toimia.

Opinnäytetyön tuloksena selvisi, että monella tutkimukseen haastatelluista suomalaisista yrityksistä oli henkilötietojen käsittely ollut hyvin hoidettu jo ennen uutta tietosuoja-asetusta, siksi sitä ei ole pidetty niin tarpeellisena. Suurimmat muutokset olivat tämän tutkimuksen mukaan tilitoimistoissa olleet tietojärjestelmien ja tietoturvan parantaminen sekä erilaisten dokumenttien laadinta. Tilitoimistot olivat saaneet asetuksesta hyvin tietoa, mutta valmistautuminen asetuksen aiheuttamiin muutoksiin oli heikkoa ja se oli vaatinut paljon lisätyötä.

Asiasanat

GDPR, tietosuoja-asetus, tietosuojalaki, henkilötietojen käsittely, osoitusvelvollisuus, tilitoimisto

Abstract

Authors	Type of publication	Published
Lamminen, Annika	Bachelor's thesis	Spring 2018
Rantanen, Eija	Number of pages	
	84 pages	

Title of publication

EU's data privacy regulation and practical changes it requires in accounting firm

Name of Degree

Bachelor of Financial Management

Abstract

This thesis focused on the General Data Protection Regulation, GDPR. The subject of this thesis was EU's data privacy regulation and the practical changes it requires in an accounting firm. The objective was to find out which changes are needed to meet the regulation and to make it easier for small accounting firms to manage the actions required. From the research results, it was possible to analyze the firms' motivation and resources for preparing the needed specifications and to secure a sufficient level of data privacy.

This thesis consisted of two parts; theoretical and empirical. The theoretical part included lectures as well as printed and electronic works and publications. This part was divided into three chapters. The first chapter dealt with the EU's data privacy regulation in general. The second chapter is focused on the seven common principles of the regulation. The third chapter describes the key changes the data privacy regulation has brought for accounting firms and the actions it requires.

The results of this thesis show many of the interviewed firms had managed personal data well even before this new data privacy regulation and therefore it was not considered very useful. According to this research, the biggest changes in accounting firms were the updating of data systems and protection, as well as the preparation of various new documents. The firms were satisfied with the information received about the regulation but the preparation for the required changes had been poor and it had caused a lot of extra work.

Keywords

GDPR, General Data Protection Regulation, Data Protection Act, processing of personal data, accountability, accounting firm

SISÄLLYS

1 JOHDANTO 1
1.1 Työn taustaa 1
1.2 Tavoitteet, tutkimuskysymykset ja aiheen rajaus 1
1.3 Tutkimusmenetelmät ja aineiston hankinta 3
1.4 Opinnäytetyön rakenne 3
2 GDPR – EU:N TIETOSUOJA-ASETUS 5
2.1 Tietosuoja-asetuksen tausta 5
2.2 Asetuksen oikeusperusta ja tarve 8
2.3 Tietosuojatutkimus 9
2.3.1 Suomalaisten vastaajien tulokset 10
2.3.2 Yhteenveto tietosuojatutkimuksen vastauksista 11
2.4 Tietosuoja-asetuksen tavoitteet 11
2.4.1 Tarkoituksena luoda parempi henkilötietojen suoja 12
2.4.2 Digitaalitalouden kehityksen tukeminen ja sääntöjen yhtenäistäminen 13
2.4.3 Avoimuus 14
2.4.4 Tehokas valvonta 14
2.5 Asetuksen soveltamisala 16
2.6 Ennakkovalmistautuminen 19
2.7 Tietosuoja-asetuksen soveltaminen käytännössä 21
3 HENKILÖTIETOJEN KÄSITTELYÄ KOSKEVAT PERIAATTEET 23
3.1 Seitsemän yleistä periaatetta 23
3.2 Lainmukaisuus, kohtuullisuus ja läpinäkyvyys 24
3.3 Käyttötarkoitussidonnaisuus 27
3.4 Tietojen minimointi 29
3.5 Täsmällisyys 29
3.6 Säilytyksen rajoittaminen 30
3.7 Eheys ja luottamuksellisuus 30
3.8 Erityiset henkilötietoryhmät 31
4 KESKEISET MUUTOKSET TILITOIMISTOALALLA 34
4.1 Keskeisimmät käsitteet 34
4.1.1 Rekisteröity ja henkilötieto 34
4.1.2 Henkilötietojen käsittely ja rekisteri 35
4.1.3 Rekisterinpitäjä ja henkilötietojen käsittelijä 35

4.2 Keskeisimmät muutokset 36
4.3 Käytännön toimenpiteet 37
4.3.1 Tietoanalyysi 37
4.3.2 Prosessit 41
4.3.3 Tarvittavat dokumentit 45
4.3.4 Sopimusuudistukset 47
4.4 Tulkintaongelmia 49
5 TUTKIMUKSEN TOTEUTUS JA TULOKSET 51
5.1 Tutkimuksen toteutus 51
5.1.1 Kevään 2018 haastattelujen tulokset 52
5.1.2 Syksyn 2018 haastattelujen tulokset 58
5.2 Johtopäätökset 71
6 YHTEENVETO 74
LÄHTEET 77
LIITTEET 84

1 JOHDANTO

1.1 Työn taustaa

Henkilötietoja on käsitelty jo kauan, mutta verrattain myöhään on alettu pohtia sitä, mitä haittaa näiden tietojen joutumisesta vääriin käsiin voi seurata (Nyyssölä 2018, 23). Koko ajan kehittyvässä tietoyhteiskunnassamme, jossa tiedot liikkuvat yhä enemmän sähköisesti, tarvitaan ajantasaista lainsäädäntöä säätelemää sitä, miten sähköisesti liikkuvia tietoja saa käsitellä.

Uutta tietosuoja-asetusta on alettu soveltamaan 25.5.2018. Asetus on suurin uudistus EU:ssa 20 vuoteen ja siten myös Suomessakin. Asetuksella pyritään parantamaan kansalaisten asemaa, kun heidän henkilötietojaan käsitellään. Lisäksi pyritään edistämään elinkeinoelämää ja luomaan kustannussäästöjä viranomaistoiminnan tehostamisella. (Oikeus.fi 2017.)

Tietosuoja-asetusta täydentäväksi laiksi Suomeen on tulossa tietosuojalaki. Täytäntöönpanotyöryhmän mietintö tietosuojalaista on julkaistu 21. kesäkuuta 2017 ja mietinnöstä hallitus on antanut esityksen maaliskuussa 2018, HE 9/2018. Tällä hetkellä tietosuojalakia ei ole vielä hyväksytty, vaan toistaiseksi sovelletaan vielä henkilötietolakia rinnakkain tietosuoja-asetuksen kanssa. Samaan aikaan tietosuoja-asetuksen kanssa tuli voimaan myös tietosuojadirektiivi, jota käsitellään tässä opinnäytetyössä vain pintapuolisesti ja pääpaino on tietosuoja-asetuksessa.

1.2 Tavoitteet, tutkimuskysymykset ja aiheen rajaus

Tässä opinnäytetyössä tutkitaan uudesta EU:n tietosuoja-asetuksesta aiheutuvia käytännön muutoksia tilitoimistossa. Miten nykyistä sopimuskäytäntöä ja toimintatapoja tulee muuttaa, jotta EU:n uuden tietosuoja-asetuksen vaatimukset täyttyvät. Työ toteutetaan tilitoimiston toimeksiannon pohjalta, mutta sen tavoitteena on myös toimia apuna muille tilitoimistoille, jotka vielä kamppailevat asetuksen vaatimusten täyttämisessä. Työn tarkoituksena on luoda selkeä näkemys siitä, miten EU:n uutta tietosuoja-asetusta tulisi käytännössä soveltaa, ja mitä muutoksia sen eteen yritysten, erityisesti tilitoimistojen, tulee tehdä. Tutkimuksen tavoitteena on selvittää pienien tilitoimistojen valmistautumista asetuksen muutoksiin, sekä sitä, onko asetuksen vaatimiin toimenpiteisiin saatu riittävästi ohjeistusta ja onko ohjeistus ollut helposti ymmärrettävää. Lisäksi työssä selvitetään, koetaanko asetus alalla tarpeelliseksi. Työhön halutaan mukaan myös asunto-osakeyhtiöiden näkökulmaa henkilötietojen käsittelystä, koska tilitoimistossa, josta toimeksianto on tullut, hoidetaan myös asunto-osakeyhtiöiden kirjanpitoja.

Opinnäytetyön tekeminen aloitettiin tammikuussa 2018 jolloin asetuksen siirtymäaikaa oli enää neljä kuukautta jäljellä. Tavoitteena oli saada työ valmiiksi ennen kuin siirtymäaika on päättynyt, mutta alkuhaastatteluja tehdessä selvisi, että pienten yritysten valmistautuminen asetuksen vaatimiin muutoksiin oli heikkoa, jolloin tutkimusosio olisi jäänyt liian suppeaksi. Tämän takia työn valmistumista ei kiirehditty keväällä, vaan tekemistä jatkettiin syksyyn 2018 asti, jolloin asetuksesta ja sen vaatimista toimenpiteistä oli enemmän käytännön kokemuksia. Teoriaosuutta rajatessa huomioidaan, että työssä on tarkoitus käsitellä tietosuoja-asetusta tilitoimiston näkökulmasta. Sen vuoksi teoriaosuudessa käydään läpi tilitoimiston kannalta olennaisimpia asioita eikä asetusta kokonaisuudessaan.

Tutkimuksen pääongelma on seuraava:

- Miten uusi tietosuoja-asetus vaikuttaa tilitoimistojen toimintaan?

Tutkimukseen haetaan vastauksia myös seuraavilla alatutkimuskysymyksillä:

- Miten yritykset ovat kokeneet saaneensa tietoa asetuksesta?
- Miten valmistautuminen tietosuoja-asetukseen on sujunut?

Tietosuoja-asetuksesta on tehty opinnäytetöitä jo jonkin verran, mutta tilitoimistojen näkökulmasta, ei tätä työtä suunniteltaessa ollut vielä aiemmin tehty yhtään, vaikkakin myöhemmin myös sellainen on tullut. Samoin vastaavia töitä löytyy myös pk-yritysten näkökulmasta. Tämä opinnäytetyö eroaa samankaltaisista töistä laajuutensa puolesta ja siinä, että henkilötietojen käsittelyssä on sivuttu tilitoimiston näkökulman lisäksi myös asuntoosakeyhtiöiden näkökulmaa, mitä ei ole otettu aiemmissa opinnäytetöissä huomioon. Jari Öljymäen (2017) työ EU:n Tietosuojauudistus vuodelta 2017 vertaa tulevaa tietosuojauudistusta edeltäneisiin lainsäädäntöihin sekä Suomen henkilötietolakiin. Tutkimusongelmana Öljymäen työssä on se, millä tasolla Suomen valmistautuminen tietosuoja-asetuksen soveltamiseen kansallisessa lainsäädännössään on. Lopputulokseksi on saatu, että Suomessa valmius on hyvällä tasolla ja valmistelut parhaillaan käynnissä. Vastaavasti hieman ennen asetuksen siirtymäajan päättymistä valmistuneessa Hanna Niemen (2018a) työssä EU:n tietosuoja-asetuksen muutosten vaikutukset tilitoimistossa on aihe täysin sama ja tehty myös toimeksiannosta tilitoimistolle. Aihetta on kuitenkin käsitelty suppeammin verrattuna tähän työhön, koska Niemen työssä on käsitelty ainoastaan valmistautumista asetukseen ennen siirtymäajan päättymistä. Niemen työssä on päädytty siihen lopputulokseen, että asetukseen valmistautuminen on ollut arvioitua hitaampaa.

1.3 Tutkimusmenetelmät ja aineiston hankinta

Tämä opinnäytetyö on kvalitatiivinen eli laadullinen tutkimus, jossa tutkittavaa aineistoa on kerätty pääasiassa haastatteluilla. Kvalitatiivisessa tutkimuksessa pyritään tutkimaan asiaa mahdollisimman kokonaisvaltaisesti ja halutaan tehdä uusia löydöksiä tutkittavasta aiheesta sen sijaan, että pyrittäisiin vain todentamaan jo aiheesta aiemmin havaittuja tosiasioita (Hirsjärvi, Remes & Sajavaara 2007, 157). Menetelmäksi valikoitui puolistrukturoitu haastattelu, jossa kaikille haastateltaville on esitetty lähes samat kysymykset lähes samassa järjestyksessä. Kysymykset ovat olleet etukäteen mietittyjä, mutta niitä ei ole esitetty tietyssä järjestyksessä niin kuin pelkästään strukturoidussa haastattelussa tehdään, vaan keskustelu on ollut vapaamuotoisempaa. Lisäksi puolistrukturoitu haastattelu sopii menetelmänä hyvin käytettäväksi tutkimuksiin, joissa aihetta on tutkittu vielä suhteellisen vähän. (Näpärä 2017.)

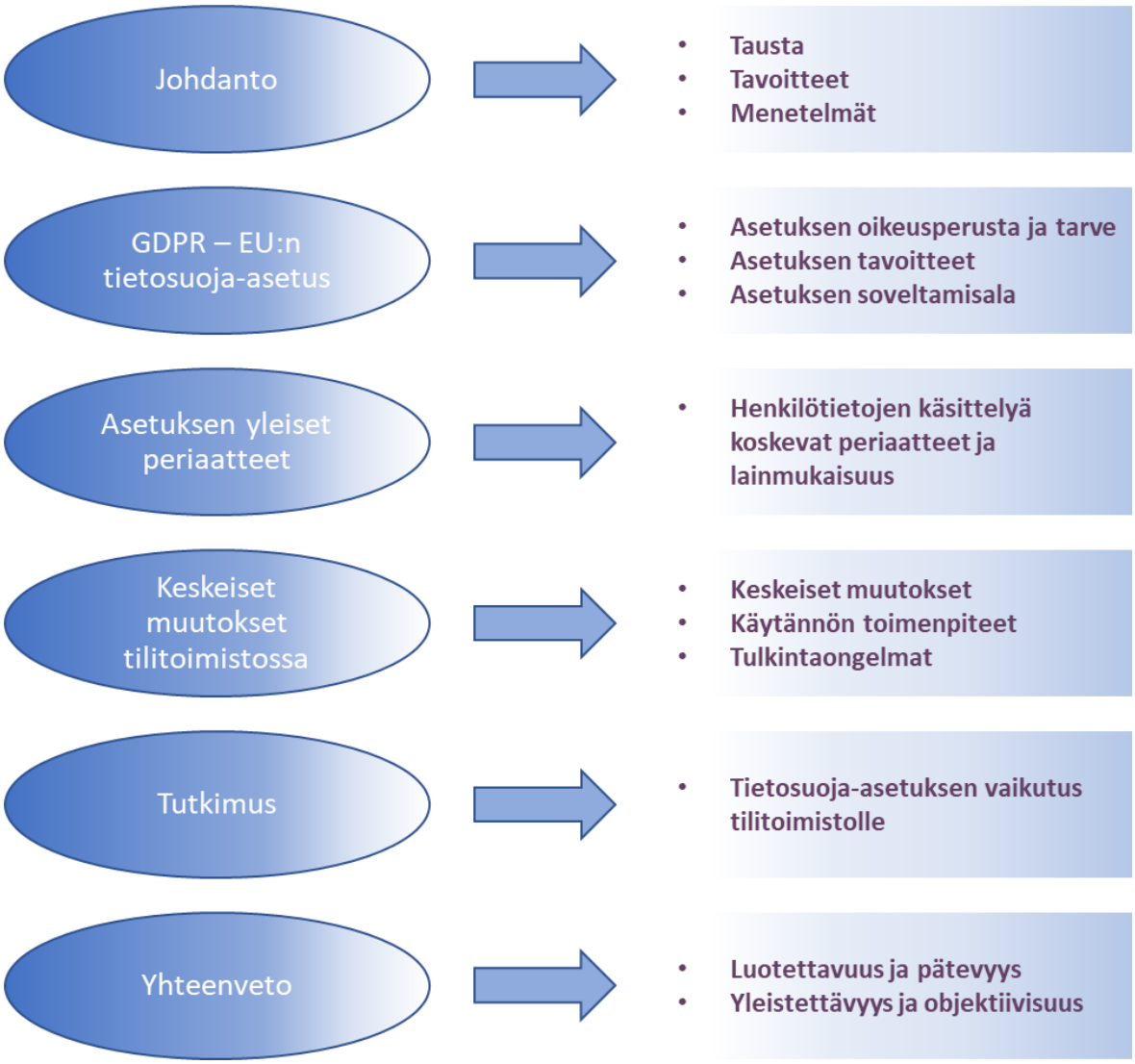
1.4 Opinnäytetyön rakenne

Opinnäytetyön rakenne koostuu johdannosta, teoriasta, empiriasta sekä yhteenvedosta. Johdannossa esitellään työn taustaa, tavoitteita, perusteet aiheen rajaukselle sekä käytetyt tutkimusmenetelmät, aineiston hankinta ja opinnäytetyön rakenne.

Teoriaosuutta käsitellään työn toisessa ja kolmannessa luvussa, joissa on tarkasteltu EU:n tietosuoja-asetusta, asetuksen oikeusperustaa ja tarvetta asetukselle sekä asetuksen mukaisia henkilötietojen käsittelyn pääpiirteitä. Teoriaosuutta on jatkettu myös luvussa neljä, jossa käsitellään asetuksen aiheuttamia muutoksia ja käytännön toimenpiteitä tilitoimistoissa.

Viides luku keskittyy empiiriseen tutkimukseen ja sitä saatuihin tutkimustuloksiin. Luvussa on kuvattu tutkimuksen suunnittelu ja toteutus sekä tehty johtopäätökset tutkimustulosten perusteella. Tutkimus on ollut kaksiosainen ja nämä tutkimusosat on jaettu omiksi alaluvuikseen tutkimuksen toteutuksen alle.

Viimeisessä, kuudennessa luvussa on yhteenveto, joka päättää opinnäytetyön. Yhteenvedossa kootaan yhteen koko työ ja pohditaan mitä vastauksista on saatu tutkimuskysymykseen sekä alatutkimuskysymyksiin. Yhteenvedossa arvioidaan tutkimuksen luotettavuutta, pätevyyttä, yleistettävyyttä ja objektiivisuutta. Yhteenvedon jälkeen on esitetty työssä käytetty lähteet ja lähteitä seuraa työn liitteet. Opinnäytetyön rakennetta on kuvattu kuviossa 1 (Kuvio 1, sivu 4).



Kuvio 1. Työn rakenne

2 GDPR – EU:N TIETOSUOJA-ASETUS

2.1 Tietosuoja-asetuksen tausta

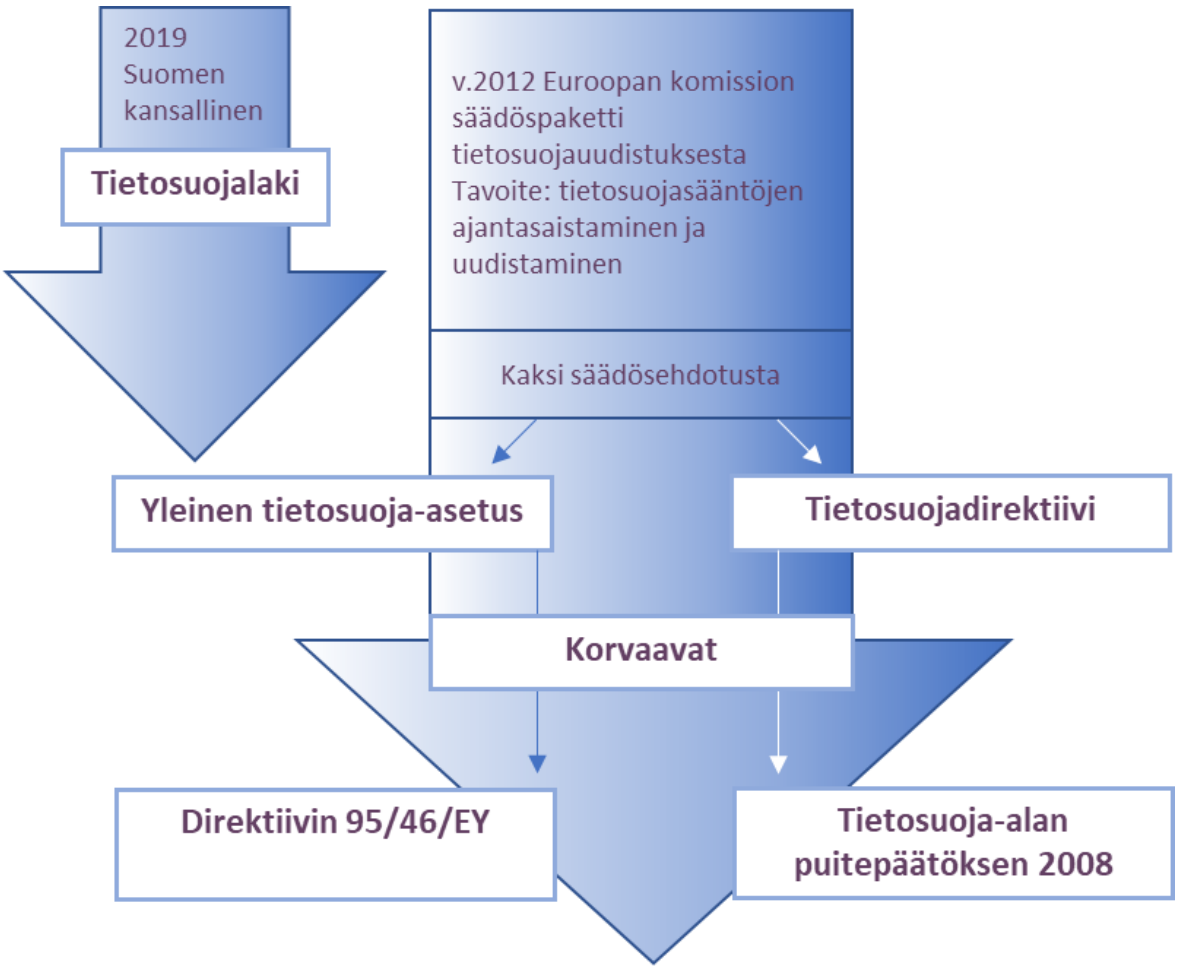
GDPR tulee sanoista General Data Protection Regulation, suomennettuna yleinen tietosuoja-asetus, joka tarkoittaa EU:n uutta tietosuoja-asetusta (Hanninen, Laine, Rantala, Rusi & Varhela 2017,13; European Data Protection Supervisor 2018). Koska kyseessä on asetus, se on suoraan sovellettavaa lainsäädäntöä kaikissa EU:n jäsenmaissa. Asetus jättää kuitenkin jäsenvaltioille jonkin verran direktiivin omaista liikkumavaraa, jonka kunkin jäsenvaltion lainsäätäjä saa täydentää ja täsmentää itse, huomioiden oman kansallisen näkökulman. (Oikeusministeriö 2017; Eduskunta 2018a.) Suomessa tätä liikkumavaraa täydentää ja täsmentää tulossa oleva tietosuojalaki. Henkilötietojen käsittelyn tulee olla asetuksen mukaista 25.5.2018 alkaen (Oikeusministeriö, Tietosuojavaltuutetun toimisto 2017).

Asetus vastaa teknologisen kehityksen ja globalisaation tuomiin uusiin haasteisiin henkilötietojen käsittelyssä (Oikeusministeriö, Tietosuojavaltuutetun toimisto 2017). Lisäksi tavoite on vahvistaa sääntöjä koskien henkilötietojen vapaata liikkuvuutta unionin sisällä (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 1.luku 1 artikla). Ennen tietosuojalainsäädäntö perustui pitkälti rekistereihin, nyt pääpaino on henkilötietojen käyttötarkoituksessa (Hanninen ym. 2017, 22).

Tietosuojan lainsäädännön muuttaminen alkoi jo tammikuussa 2012, kun Euroopan komissio julkaisi ehdotuksen lain uudistamisesta (Valtiovarainministeriö 2016). Vuonna 2010 Eurooppa-neuvosto antoi luvan komissiolle neuvotella Yhdysvaltojen kanssa tietosuojasopimuksen, puitesopimuksen. Sopimuksella pyritään takaamaan Euroopan kansalaisten henkilötietojen suojaaminen, kun tietoja siirretään EU:sta Yhdysvaltoihin lainvalvontaan liittyvissä asioissa. (Eurooppa-neuvosto 2016.) Lisäksi puitesopimuksen allekirjoittamisen ehtona oli, että Yhdysvallat hyväksyy myös lain, jolla EU:n kansalainen voi hakea muutosta Yhdysvaltain oikeudessa. Tämän Privacy Shield-järjestelmän Yhdysvallat hyväksyi vuonna 2016. (Eurooppa-neuvosto 2016; Nyyssölä 2018, 294.)

Kaikista uudistuksen sisällöstä ei päästy heti sopuun, siksi itse tuotokset; yleinen tietosuoja-asetus Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 ja tietosuojadirektiivi (EU) 2016/680 julkaistiin vasta toukokuussa 2016 (Valtiovarainministeriö 2016; Bergström, Karhula & Kipinoinen 2018). Säädökset astuvat voimaan kahden vuoden siirtymäajan jälkeen 25.5.2018 (Valtiovarainministeriö 2016).

Tietosuojauudistuksen vaiheita on vielä tarkemmin havainnollistettu kuviossa 2.



Kuvio 2.Tietosuoja-asetuksen uudistuksen vaiheet

Yleinen tietosuoja-asetus GDPR, korvaa direktiivin 95/46/EY sekä lainvalvonta-alan tietosuojadirektiivi tietosuoja-alan puitepäätöksen 2008/977/YOS (Valtiovarainministeriö 2016; Eurooppa-neuvosto 2015). Molemmat korvatut asetukset koskevat henkilötietojen suojaamista ja ovat osa suurempaa säädöskokonaisuutta, tietosuojapakettia. Euroopan komission tietosuojapaketin vaiheita ja sen aiheuttamia muutoksia säädöksiin on havainnollistettu kuviossa 2.

> *Kokonaisuudistuksen tavoitteena on ollut luoda Euroopan unionille ajanmukainen, vahva, yhtenäinen ja kattava tietosuojakehys. Uudistus on ollut tarpeellinen informaatioteknologian nopea kehityksen ja jäsenvaltioiden hajanaisten henkilötietojen suojaa koskevien säädösten ja niiden epäyhtenäisen soveltamisen vuoksi.* (HE 9/2018.)

Direktiivi 95/46/EY

Vuonna 1995 annettu tietosuojadirektiivi 95/46/EY koskee henkilötietojen vapaata liikkuvuutta sekä henkilöiden suojelua, kun heidän henkilötietojaan käsitellään (Henkilötietodirektiivi 95/46 EY). Direktiivi hyväksyttiin ajankohtana, jolloin internet oli vasta alkuvaiheessa, mutta sen aavisteltiin helpottavan ja lisäävän henkilötietojen kansainvälistä liikkuvuutta (EDPS 2018; Henkilötietodirektiivi 95/46). Direktiivi kumottiin toukokuussa 2018, kun uusi tietosuoja-asetus astui voimaan (Milt 2018). Tietosuojadirektiivi pantiin Suomessa voimaan henkilötietolailla 523/1999 (Oikeusministeriö 2017). Henkilötietolaki korvautuu kansallisella tietosuojalailla, mutta uusi laki on tällä hetkellä vielä valiokunnilla käsittelyssä, joten henkilötietolaki on vielä voimassa.

Puitepäätös 2008/977/YOS

Puitepäätös käsittelee henkilötietojen suojaamista rikosasioissa, joissa tietoja siirretään esimerkiksi poliisin ja oikeuden välillä (Neuvoston puitepäätös 2008/977/YOS). Puitepäätös kumottiin toukokuussa 2018, kun uusi Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/680 astui voimaan (Milt 2018). Direktiivi koskee henkilötietojen suojelua, kun viranomaiset käsittelevät niitä esimerkiksi rikoksien selvittelyn, tutkimisen tai ennaltaehkäisemisen takia. Lisäksi direktiivi koskee näiden tietojen vapaata liikkuvuutta Euroopan unionin sisällä viranomaisten välillä. (Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/680.)

Tietosuojalaki

Oikeusministeriön asettama työryhmä ehdotti kesäkuussa 2017, että Suomeen säädettäisiin uusi tietosuojalaki. Tietosuojalaista tulisi Suomessa uusi yleislaki, joka koskisi henkilötietojen käsittelyä ja täydentäisi Euroopan parlamentin ja neuvoston antamaa yleistä tietosuoja-asetusta. (Oikeusministeriö, 2017; HE 9/2018.)

Tietosuoja-asetuksessa on kohtia, jotka jäsenvaltion lainsäätäjä saa itse päättää. Työryhmän ehdotuksen mukaan näistä päätöksistä säädettäisiin tietosuojalailla. Näitä olisivat muun muassa oikeusturva, seuraamukset sekä tietojenkäsittelyn erityistilanteet. Tietojenkäsittelyn erityistilanteilla tarkoitetaan esimerkiksi henkilötunnuksen käsittelyä, tilastointia ja sananvapauden turvaamista. (Oikeusministeriö, 2017.) Tietosuojalakia olisi tarkoitus soveltaa rinnakkain tietosuoja-asetuksen kanssa eikä muodostaa siitä itsenäistä sääntelykokonaisuutta (HE 9/2018).

Työryhmä on ehdottanut, että uudella lailla korvattaisiin nykyinen henkilötietolaki sekä laki tietosuojalautakunnasta ja tietosuojavaltuutetusta (Oikeusministeriö 2017). EU:n yleistä tietosuoja-asetusta alettiin soveltamaan jäsenvaltioissa 25.5.2018. Työryhmän

alkuperäinen ehdotus oli, että tietosuojalaki olisi astunut voimaan samaan aikaan tietosuoja-asetuksen kanssa. (Oikeusministeriö 2017.) Laki on parhaillaan käsittelyssä ja sen on tarkoitus astua voimaan 1.1.2019, mutta Suvanto (2018) epäilee, ettei laki ole välttämättä vielä silloinkaan valmis (Eduskunta 2018b; Suvanto 2018).

2.2 Asetuksen oikeusperusta ja tarve

Tietosuoja-asetuksen perusteet tulevat jo Euroopan unionin perusoikeuskirjasta (2000). Euroopan unionin perusoikeuskirjan (2000, 7 artikla) mukaan, jokaisella on oikeus siihen, että hänen yksityisyyttään kunnioitetaan. Lisäksi 8:nnen artiklan mukaan:

> *Jokaisella on oikeus henkilötietojensa suojaan.*

Tietojen käsittelyn on oltava tarkoituksenmukaista ja siihen pitää olla henkilön suostumus tai laillinen oikeusperuste. Lisäksi jokaisella on oikeus tietää, mitä tietoja hänestä on kerätty ja mahdollisuus oikaista väärät tiedot. Perusoikeuskirjan mukaan näitä henkilötietojen suojan sääntöjä valvoo viranomainen. (Euroopan unionin perusoikeuskirja artikla 8, 2000.) Eli pohja henkilötietojen suojaamiselle ja siten uudelle tietosuoja-asetukselle tulee jo Euroopan unionin perusoikeuskirjasta.

Yrityksillä, seuroilla ja yhdistyksillä on hallussaan paljon henkilötietoja. Niitä kertyy niin asiakkaista kuin omista työntekijöistä ja yhteistyökumppaneista. Tietoja voidaan säilyttää, hyödyntää tai jopa luovuttaa ulkopuolisille käytettäväksi. (Nyyssölä 2018, 23.) Esimerkiksi yritys voi olla ulkoistanut palkanmaksun tilitoimistolle, jolloin yritys luovuttaa palkanmaksua varten työntekijöidensä henkilötietoja ulkopuoliselle yritykselle.

Yritykset keräävät henkilötietoja pääasiassa omien intressien takia, mutta myös lainsäädäntö ja asetukset vaativat yrityksiä keräämään ja säilyttämään henkilötietoja (Nyyssölä 2018, 23; Koivuniemi 2018). Yrityksissä henkilötietojen kerääminen voi olla tarpeen myös rekisteröidyn edun kannalta. Palkanlaskentaa ei pysty toteuttamaan tietämättä henkilötunnusta ja verkkokaupan tilausta ei voida toimittaa asiakkaalle tietämättä osoitetta.

Henkilötietoja on edellä mainittuihin tarpeisiin kerätty jo kauan, mutta tietojenkäsittelyn turvallisuuteen ja henkilön yksityisyyden suojaan ei ole ollut aiemmin selkeitä säännöksiä laissa (Nyyssölä 2018, 23). Lisäksi maailma on muuttunut paljon vuodesta 1995, jolloin henkilötietodirektiivi 95/46/EY on annettu (Jourová 2016). Henkilötietoja käsitellään nykyään automaattisesti ja sähköisesti (Nyyssölä 2018, 23). Esimerkiksi henkilökohtaisia tietoja jaetaan nykyään internetin sosiaalisten verkostojen kautta tai tietoja tallennetaan etäpalvelinfarmeille, niin sanottuihin “pilvipalveluihin” omien henkilökohtaisten tietokoneiden sijaan (Jourová 2016). Asetuksen tarkoitus on puuttua näihin automaattisiin

päätöksentekoihin, joilla tarkoitetaan tilanteita, joissa ihminen ei ole ollenkaan mukana päättämässä vaan kone tekee asetettujen kriteerien avulla päätöksen (Nyyssölä 2018, 194).

Rikollisuus on myös tietojen käsittelyn automatisaation seurauksena muuttunut. Nykyään henkilötiedot ovat haluttua valuuttaa (Haarma & Leppänen 2018, 8). Varkaita ei enää kiinnosta parkkialueiden autot vaan entistä enemmän netin välityksellä tapahtuvat petokset. Petoksiin liittyvät identiteettivarkaudet ovat lisääntyneet huimasti ja tämä trendi näyttäisi olevan edelleen kasvussa. Identiteettivarkaudella tarkoitetaan sitä, että joku toinen käyttää luvatta toisen henkilötietoja ja petokseksi tämä muuttuu, kun esimerkiksi tilataan tietokone netistä ja lasku menee toiselle henkilölle. Näitä edellä kuvattuja tilauspetoksia tulee poliisin tutkintaan viikoittain. Yleensä tilatut tuotteet on tarkoitus myydä eteenpäin. (Koivisto 2018, A2.) Tilauksiin käytettäviä henkilötietoja kalastellaan ihmisiltä esimerkiksi erilaisten huijaussähköpostien avulla. Esimerkiksi verohallinnon nimissä on lähetetty ihmisille huijaussähköposteja, joiden avulla on tarkoitus kalastella ihmisiltä pankkitunnuksia ja luottokorttitietoja (Hienola 2018).

Myös Kriminologian ja oikeuspolitiikan instituutin rikollisuuskatsauksen tulokset olivat samanlaiset, katsauksen mukaan varkausrikokset ovat vähentyneet, mutta vastaavasti petosrikokset ja erityisesti maksukorttipetokset ovat lisääntyneet. Katsauksen mukaan rikostilaisuudet ovat lisääntyneet ja muuttuneet, koska tietotekniikka on kehittynyt niin paljon. (Niemi 2018b.) Ennen maksukorttirikoksia on ollut eniten pääkaupunkiseudulla, mutta nyt alueelliset rajat eivät enää ole niin selkeät, koska verkkoasiointi on lisääntynyt kautta maan (Ellonen, Danielsson & Virtanen 2018, 128).

Vuonna 2016 korttien väärinkäyttökertoja oli 17 915 ja toisaalta vuonna 2017 käyttökertoja oli 6 372, tämä selittyy katsauksen mukaan valvontajärjestelmien kehittymisellä. Toisaalta hyvin moni petosrikos jää piiloon tilastosta, koska niitä ei ilmoiteta poliisille, luku saattaa siis olla hyvin paljon suurempikin. Vuonna 2017 maksuvälinepetoksista selvitettiin 10 % ja törkeistä maksuvälinepetoksista 23 %. Verrattuna vuoteen 2016 maksuvälinepetoksia selvitettiin kahdeksan kertaa enemmän. (Ellonen ym. 128-129.)

2.3 Tietosuojatutkimus

Erityiseurobarometri 431 on kyselytutkimus tietosuojasta, joka toteutettiin Euroopan unionin 28 jäsenvaltiossa helmi-maaliskuussa 2015 Euroopan komission oikeus- ja kuluttajaasioiden pääosaston pyynnöstä. Kyselyn tarkoitus oli selvittää unionin jäsenten asenteita tietosuojaa kohtaan ja verrata niitä vuoden 2010 tuloksiin. (European Comission 2015b.)

Kyselyyn vastasi kaikkiaan 27 980 vastaajaa erilaisista sosiaalisista ja demografisista lähtökohdista. Suomalaisia kyselyyn vastasi 1016. Kyselyt tehtiin kasvokkain jokaisen vastaajan omalla äidinkielellään heidän kotonaan. (European Comission 2015a; European Comission 2015b.) Kaikkiaan kyselyssä tutkittiin neljää osa-aluetta liittyen vastaajan mielipiteisiin: henkilötietojen hallinnasta, henkilötietojen luovuttamiseen liittyvistä asenteista, henkilötietoja koskevista oikeuksista sekä muiden osapuolten suorittamasta henkilötietojen käsittelystä (European Comission 2015b).

2.3.1 Suomalaisten vastaajien tulokset

Käsitys henkilötietojen hallinnasta

Suomalaisista 64 % kokivat, että he pystyvät vaikuttamaan verkossa antamiinsa tietoihin osittain, vastaava luku kaikissa EU-maissa oli 50 %. Toisaalta suomalaisista 16 % oli sitä mieltä, että heillä on antamiinsa tietoihin täysi vaikutusvalta, tai ei ollenkaan valtaa. 60 % suomalaisista oli huolissaan siitä, että tahot, jotka keräävät heidän tietojaan, käyttävät niitä eri tarkoitukseen kuin alkuperäinen tarkoitus oli, esimerkiksi suoramarkkinointiin. (Euroopan komissio 2015.)

Henkilötietojen luovuttamista koskevat asenteet

Yli kaksi kolmesta suomalaisesta on sitä mieltä, että henkilötietojen antaminen tuotteiden ja palveluiden saamiseksi on osa nykyaikaa. Ilman henkilötietojen luovuttamista palvelua tai tuotetta ei välttämättä saa. Toisaalta suurin osa suomalaisista vastaajista kokee, että henkilötietojen luovuttaminen ei ole yhdentekevää, eivätkä suomalaiset mielellään luovuta henkilötietojaan edes silloin, kun sillä saa vastineeksi verkon ilmaispalveluja, kuten sähköpostin käyttöönsä. Asenteissa suurin ero oli maakohtaisten tietojen keräämisessä; yli puolet koko kyselyyn vastanneista oli sitä mieltä, että maan hallitus kerää enemmän henkilökohtaisia tietoja, kun suomalaisista tätä mieltä oli kolmasosa. (Euroopan komissio 2015.)

Henkilötietoja koskevat oikeudet ja suojakeinot

Suomalaisista 94 % pitää hyvin tärkeänä sitä, että henkilötietoja koskisi samat oikeudet ja sama suoja riippumatta siitä, missä paikassa palvelua tarjoava yritys toimii tai sijaitsee. Yli puolet suomalaisista on sitä mieltä, että viranomaisen, jonka tehtävä olisi valvoa henkilötietojen suojaa koskevaa lakia, tulisi toimia kansallisella tasolla. Vastaavasti unionin tasolla vastaajista 45 % on sitä mieltä, että lakia pitäisi valvoa Euroopan unionin tasolla. (Euroopan komissio 2015.)

Muiden osapuolten suorittama henkilötietojen käsittely

Suomalaisista yli 89 % luottaa, että heidän henkilötietonsa ovat turvassa, kun niitä käsittelee terveydenhoitoon liittyvä taho, kansallinen viranomainen, esimerkiksi verottaja, tai pankit ja rahalaitokset. Yli 50 % vastaajista myös luottaa, että Euroopan komissio, kaupat ja tavaratalot, puhelinyhtiöt sekä internet-palveluiden tarjoajat suojaavat henkilötietoja. Nämä prosentit ovat unionin kaikkiin vastaajiin nähden huomattavasti korkeammat. Esimerkiksi puhelinyhtiöihin ja internet-palvelujen tarjoajiin kaikista vastaajista luottaa vain 33 %. Yli puolet niin suomalaisista, kuin kaikista vastaajista, ei luota verkossa toimiviin yrityksiin, esimerkiksi hakukoneisiin. (Euroopan komissio 2015.)

2.3.2 Yhteenveto tietosuojatutkimuksen vastauksista

Tutkimuksessa havaittiin, että suuri osa eurooppalaisista käyttää säännöllisesti verkkopalveluja. Kuitenkin verkkopalveluiden käytössä on tutkimuksen mukaan selkeitä maakohtaisia eroja. Esimerkiksi yli 80 % suomalaisista käyttää verkkopankkipalveluita joka viikko, kun taas kreikkalaisista verkkopankkia käyttää viikoittain alle 10 %. (European Comission 2015a.)

Vuonna 2015 luottamus verkkoyrityksiin oli edelleen vähäistä, sillä alle 25 % vastaajista luotti siihen, että verkossa toimivat yritykset käsittelisivät luottamuksellisesti heidän henkilötietojaan. Tämä korostaa tarvetta uudistaa tietosuojamalleja Euroopassa. Tämä toteutettaisiin määräämällä yrityksille selkeät standardit, joihin pyrkiä ja joita noudattamalla voidaan taata kansalaisille, että heidän henkilötietonsa ovat turvassa. (European Comission 2015a.) Hyvän tietoturvan uskotaan myös lisäävän luottamusta yritysten tarjoamiin palveluihin (Haarma & Leppänen 2018, 8).

Suurin osa tutkimukseen vastaajista hyväksyy, että digitaaliaikana tiedonkeruu on osa tätä päivää, kunhan se pysyy asianmukaisissa rajoissa. Kuitenkin yli 70 % vastaajista katsoo, että heidän nimenomaista hyväksyntää olisi vaadittava kaikissa tapauksissa ennen kuin mitään heidän henkilökohtaisia tietoja kerätään tai käsitellään. Lisäksi vastaajista vain 15 % kokee, että he pystyvät täysin hallitsemaan tietoja, jotka he luovuttavat verkkoon. Vastaajista 67 % on sitä mieltä, että henkilötietoja käsittelevän yrityksen vastuulla on ilmoittaa rekisteröidylle, jos hänen tietojaan katoaa tai varastetaan. (European Comission 2015a.)

2.4 Tietosuoja-asetuksen tavoitteet

Asetuksella on kaksi tavoitetta: vahvistaa säännöt, kun käsitellään luonnollisten henkilöiden henkilötietoja sekä turvata näiden tietojen vapaa liikkuvuus Euroopan unionin sisällä (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 1.luku 1 artikla).

Alla olevassa taulukossa 1 on vielä koottu asetuksen tavoitteet tiivistäen ja huomioitu miten näiden tavoitteiden toteutuminen mahdollistetaan. Seuraavissa alaluvussa kerrotaan näistä aiheista tarkemmin.

Taulukko 1. Asetuksen tavoitteet (Oikeusministeriö, Tietosuojavaltuutetun toimisto 2017; Hassinen 2018)

Tavoite		Miten toteutetaan
2.4.1	Parantaa henkilötietojen suojaa	Tiukentamalla sääntöjä, miten henkilötieoja voidaan kerätä → osoitusvelvollisuus
2.4.2	Tukea digitaalitalouden kehitystä sisämarkkinoiden alueella	Yhdenmukaistamalla jäsenvaltioiden tietosuojaa koskevat säännökset → Lisätä luottamusta
2.4.3	Lisätä henkilötietojen käsittelyn avoimuutta ja läpinäkyvyyttä	Rekisteröity voi entistä paremmin valvoa henkilötietojensa käsittelyä ja hallinnoida paremmin tietoja, joita hänestä kerätään
2.4.4	Velvoitteiden noudattamista tuetaan tehokkaalla täytäntöönpanolla ja seuraamuksilla	Valvontaviranomainen voi määrätä korjaavia toimenpiteitä tai hallinnollisia sakkoja

2.4.1 Tarkoituksena luoda parempi henkilötietojen suoja

Taulukossa 1 on ensimmäisellä rivillä asetuksen ensisijainen tavoite, henkilötietojen suojan parantaminen. Tavoite on parantaa luonnollisten henkilöiden suojelua tilanteissa, joissa heidän henkilötietojaan käsitellään (Oikeusministeriö, Tietosuojavaltuutetun toimisto 2017). Tämä toteutetaan määrittelemällä oikeusperusteiset ja tiukemmat säännöt, jonka puitteissa henkilötietoja voidaan kerätä. Yrityksen pitää myös pystyä näyttämään toteen, että käytännössä toimitaan asetuksen mukaan. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 2.luku 5 artikla kohta 1-2.)

Osoitusvelvollisuus

Osoitusvelvollisuudella tarkoitetaan asetuksessa sitä, että rekisterinpitäjän pitää pystyä näyttämään, että hän toimii noudattaen asetuksen 2. luvun artikla 5:nnessä määriteltyjen henkilötietojen käsittelyn periaatteiden mukaan. Periaatteet käydään läpi tarkemmin tämän työn luvussa 3.4. sivulla 29.

> *Rekisterinpitäjän on huolehdittava siitä, että tietosuojaperiaatteita noudatetaan kaikissa henkilötietojen käsittelyvaiheissa. Rekisterinpitäjää koskevan osoitusvelvollisuuden johdosta rekisterinpitäjän on pystyttävä myös osoittamaan, että periaatteita noudatetaan. Rekisterinpitäjän on siis arvioita, mitä periaatteet käytännössä*

> *tarkoittavat ja miten ne toteutuvat omassa toiminnassa. Periaatteiden noudattamisen osoittaminen edellyttää rekisterinpitäjältä muun muassa henkilötietojen käsittelyn aiempaa tarkempaa suunnittelua ja dokumentointia.* (Oikeusministeriö, Tietosuojavaltuutetun toimisto 2017.*)*

Koska valvontaviranomaiselle pitää pystyä osoittamaan, että henkilötietojen kerääjä toimii asetuksen mukaisesti. Ei siis riitä, että rekisterinpitäjä vain noudattaa periaatteita, jos ei ole näyttää tätä myös konkreettisesti. (Nevasalo & Parviainen 2017, 30.) Rekisterinpitäjän sekä henkilötietojenkäsittelijän tulee siis tietää mitä henkilötietoja, miten ja milloin niitä käsitellään sekä miten toimia, jos käsittelyprosessi pettää (Haarma & Leppänen 2018, 8). Käytännössä tämä tarkoittaa sitä, että rekisterinpitäjän tulee dokumentoida niin organisaatio- kuin järjestelmätasolla: käytännöt, menettelyt ja toimenpiteet siitä, miten henkilötietoja käsitellään (Nevasalo & Parviainen 2017, 30). Vaiheet voi taulukoida esimerkiksi Exceliin. Nyyssölän (2018, 84) mukaan osoitusvelvollisuudesta on käytetty myös termiä käännetty todistustaakka. Tällä tarkoitetaan sitä, että rekisterinpitäjä olisi syyllinen tietosuoja-asetuksen rikkomukseen, jos hän ei pysty toisin todistamaan.

2.4.2 Digitaalitalouden kehityksen tukeminen ja sääntöjen yhtenäistäminen

Toisella rivillä taulukossa 1 (Taulukko 1, sivu 12) on tavoitteena digitaalitalouden kehitys EU:n alueella. Tähän pyritään lisäämällä kansalaisten luottamusta ja takaamalla, että asetuksen noudattamisen myötä EU-maiden sisällä henkilötietojen luovuttaminen on turvallista. Kun tämä toteutuu, uskotaan sen vaikuttavan sisämarkkinoiden kehitykseen positiivisesti ja tukevan samalla digitaalitalouden kehitystä. Eli asetuksen ei ole tarkoitus rajoittaa henkilötietojen liikkuvuutta Euroopan unionin jäsenvaltioiden välillä vaan ennemminkin lisätä sitä. (Oikeusministeriö, Tietosuojavaltuutetun toimisto 2017.)

Tietosuoja-asetuksen mukaan henkilötietodirektiivin tavoitteet ja periaatteet ovat edelleen pätevät, mutta päivittämiselle on tarvetta. Direktiivin avulla ei ole muun muassa pystytty yhdentämään tietosuojakäytäntöjä niin, että ne olisivat koko EU:n alueella samanlaiset. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 johdanto-osan kohta 9.) Esimerkiksi Suomessa jokin voi olla kiellettyä, kun se on Saksassa sallittua (Lehtola 2016).

Erot johtuvat pääosin siitä, että tietosuojadirektiiviä 95/46/EY on pantu täytäntöön ja sovellettu jäsenvaltioissa eri lailla. Näistä eroista johtuva kansalaisten epävarmuus erityisesti heidän luovuttaessaan tietoja verkkoympäristössä voi heikentää unionin taloudellista toimintaa, vääristää kilpailua ja haitata viranomaisten toimintaa heidän suorittaessaan unionin määräysten mukaisia velvollisuuksiaan. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 johdanto-osan kohta 9.) Asetuksen avulla kaikissa jäsenvaltiossa tulee

voimaan samanlaiset sanktiot rikkomuksista ja yhdenmukainen valvonta, myös eri jäsenvaltioiden viranomaisten välillä (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 johdanto-osan kohta 13).

Sääntöjen yhdenmukaistaminen hyödyttää myös yrityksiä, sillä yhtenäistämisen myötä myös yritysten on aiempaa helpompaa laajentaa toimintaansa muihin EU-maihin. Tietosuojavaltuutettu Aarnio arvioi asetuksen myötä myös Suomeen tulevan entistä enemmän kilpailua. (Hassinen 2018, A10.)

2.4.3 Avoimuus

Kolmantena tavoitteena taulukossa 1 (Taulukko 1, sivu 12) on henkilötietojen käsittelyn avoimuuden ja läpinäkyvyyden lisääminen. Tällä halutaan taata, että rekisteröidyllä olisi aiempaa enemmän oikeuksia hallita tietojansa. Siksi rekisteröidyn tulisi muun muassa saada tietää mitä, missä määrin ja miten hänen henkilötietojaan kerätään, käsitellään tai aiotaan mahdollisesti muokata. Näiden seikkojen tulee olla rekisteröidylle helposti saatavilla sekä helposti ymmärrettävissä. Tästä johtuen rekisterinpitäjän, tulee aina arvioida, miten henkilötietoja käsitellään tai tullaan käsittelemään. Tähän liittyen rekisteröidylle pitää kertoa tarkasti kuka rekisterinpitäjä on ja mihin käyttötarkoitukseen hän tietoja kerää. Lisäksi rekisteröidylle tulee ilmoittaa henkilötietojen käsittelyn riskeistä, suojatoimista sekä rekisteröidyn oikeuksista. (Hanninen ym. 2017, 48.) Läpinäkyvyyttä on käyty vielä tarkemmin läpi luvussa 3.2 Lainmukaisuus, kohtuullisuus ja läpinäkyvyys sivulla 24.

2.4.4 Tehokas valvonta

Taulukon 1 (Taulukko 1, sivu 12) neljännellä rivillä on mainittu tavoitteeksi asetuksen velvoitteiden noudattamisen seuraaminen ja mahdollisesta asetuksen noudattamatta jättämisestä määrättävät seuraamukset. Suomessa asetuksen valvontaviranomaisena toimii tietosuojavaltuutettu, joka valvoo asetuksen soveltamista (Nyyssölä 2018, 300). Tietosuojavaltuutetulla on oikeus saada maksutta tehtäviensä hoidon kannalta tarpeelliset tiedot salassapitosäännöksistä huolimatta ja hänellä on apunaan lainsäädännön tulkintaan liittyvissä kysymyksissä asiantuntijalautakunta. Lisäksi tietosuojavaltuutettu voi pyytää lausuntoja ulkopuolisilta asiantuntijoilta sekä saada poliisilta virka-apua tehtäviensä suorittamiseksi (HE 9/2018 17-20 §). Nyyssölä (2018,302) toteaakin, että tutkintaa suorittaessa tietosuojavaltuutetulla on käytännössä lähes rajattomat oikeudet. Kuitenkin asetuksen johdanto-osassa (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 johdanto-osan kohta 129) otetaan kantaa siihen, että valvontaviranomaisen tekemien toimenpiteiden pitäisi olla tarkoituksenmukaisia ja oikeasuhteisia eikä niistä saisi koitua asianomaisille

turhia kustannuksia tai haittoja. Lisäksi kaikki oikeudelliset toimenpiteet pitäisi perustella kirjallisesti, selkeästi ja yksiselitteisesti sekä kertoa myös niiden syyt.

Sanktiot

Sanktiot voivat olla yrityksille jopa 20 miljoonaa euroa tai 4 % edellisen tilikauden maailmanlaajuisesta kokonaisliikevaihdosta (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 8.luku 83 artikla, kohta 6-7). Asetuksen pääasiallinen tarkoitus ei kuitenkaan ole suuret sanktiot, vaan ohjata sekä neuvoa rekisterinpitäjiä toimimaan oikein (Haarma & Leppänen 2018, 10, 52). Hallinnollisia sakkoja ei voida myöskään määrätä ilman selkeää näyttöä siitä, että rekisterinpitäjä olisi rikkonut asetuksen määräyksiä, ja kaikissa rikkomuksissa arvioidaan rikkomusta aina tapauskohtaisesti sekä kokonaisvaltaisesti (Nyyssölä 2018, 66; Haarma & Leppänen 2018, 52).

Käytössä on myös paljon lievempiä seuraamuksia kuin hallinnollinen sakko, kuten varoitus, huomautus tai määräys muuttaa henkilötietojen käsittelyn käytäntöjä asetuksen mukaiseksi (Haarma & Leppänen 2018,52; Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 8.luku 58 artikla, kohta 2). Määräyksen tueksi voidaan asettaa uhkasakko (Nyyssölä 2018, 67). Uhkasakkoa voidaan käyttää myös tehosteena, jos rekisterinpitäjällä ei ole aikomusta antaa tietosuojavaltuutetulle tämän tarvitsemia tietoja. Kaikissa tapauksissa uhkasakko määräytyy tapauskohtaisesti ja siihen sovelletaan uhkasakkolakia 1113/1990. (HE 9/2018 22 §.) Toisaalta, jos rekisteröidylle on aiheutunut rahallista tai aineetonta haittaa asetuksen vastaisesta toiminnasta, voi rekisterinpitäjä joutua myös vahingonkorvausvastuuseen (Haarma & Leppänen 2018, 52-53). Seuraamukset asetuksen rikkomisesta voivat olla myös yritykselle taloudellisesti merkittävät, mutta ehkä rahaakin tärkeämpää on se mitä tapahtuu yrityksen maineelle, brändille ja imagolle sen jälkeen, kun yritys on jäänyt kiinni siitä, että se on käsitellyt henkilötietoja väärin (ID BBN 2017).

Kukin jäsenvaltio saa itse määritellä sen, voiko viranomaisille tai julkishallinnon elimille määrätä hallinnollisia sakkoja ja missä määrin (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 8.luku 83 artikla, kohta 6-7). Hallituksen esityksen mukaan Suomessa seuraamusmaksua ei voida määrätä.

> *Seuraamusmaksua ei voida määrätä valtion viranomaisille, valtion liikelaitoksille, kunnallisille viranomaisille, itsenäisille julkisoikeudellisille laitoksille, eduskunnan virastoille eikä tasavallan presidentin kanslialle* (HE 9/2018 25 §).

Tätä on perusteltu esityksen yksityiskohtaisten perustelujen neljännessä luvussa sillä, että hallinnollinen seuraamusmaksu on vieras menettelytapa suomalaisessa oikeusjärjestyksessä. Lisäksi julkishallintoon kohdistuu muita erityisvaatimuksia. (HE 9/2018 25 §.)

Viranomaisiin kohdistuu myös laajempi vastuu työssä tehdyistä virheistä. Lisäksi viranomaisten on pystyttävä hoitamaan lakisääteiset tehtävänsä ja heidän toimintansa on hyvin budjettisidonnaista. (HE 9/2018.) Esimerkiksi jos poliisia rangaistaisiin suurilla hallinnollisilla sakoilla vaikutus voisi näkyä siinä, että kansalaiset jäisivät vaille poliisin apua tai poliisin tuleminen tapahtumapaikalle kestäisi pitkän aikaa. Eli sakon vaikutus ei toimi toivotulla tavalla budjettisidottuun viranomaiseen kuin yksityisellä puolella toimivaan yritykseen. Toisaalta myös viranomaiselle tai julkishallinnon elimelle voidaan määrätä uhkasakkoja (HE 9/2018).

2.5 Asetuksen soveltamisala

Asetus koskee niin yksityisiä kuin julkisia yrityksiä, yhteisöjä, seuroja ja kaikkia, jotka käsittelevät henkilötietoja, käytetystä teknologiasta, henkilötietojen luonteesta tai laajuudesta riippumatta (Oikeusministeriö, Tietosuojavaltuutetun toimisto 2017).

Aineellinen ja alueellinen soveltamisala

Asetuksen soveltaminen jaetaan kahteen osaan: aineelliseen ja alueelliseen. Aineellinen soveltamisala määrittää sen, minkälaista henkilötietojen käsittelyä asetus koskee ja alueellinen soveltamisala määrittää nimensä mukaisesti millä alueella asetusta sovelletaan (Nyyssölä 2018, 39-40).

Aineellinen soveltamisala määritellään seuraavasti:

> *Tätä asetusta sovelletaan henkilötietojen käsittelyyn, joka on osittain tai kokonaan automaattista, sekä sellaisten henkilötietojen käsittelyyn muussa kuin automaattisessa muodossa, jotka muodostavat rekisterin osan tai joiden on tarkoitus muodostaa rekisterin osa* (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 1.luvun 2. artiklan kohta 1).

Tästä voidaan päätellä, että kun henkilötietoja käsitellään automaattisesti, sovelletaan aina tietosuoja-asetusta, mutta manuaalisesti käsiteltäessä asetus ei tulekaan aina sovellettavaksi (Nyyssölä 2018, 40). Toisaalta asetusta on noudatettava käytettävästä tekniikasta riippumatta, jos käsiteltävät henkilötiedot muodostavat rekisterin tai ovat osa sitä (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 johdanto-osan kohta 15). Jos käsitellään henkilötietoja ja ne eivät muodosta rekisterin osaa tai niiden ei ole tarkoituskaan muodostaa sitä, niihin ei sovelleta asetusta (Nyyssölä 2018, 40). Esimerkiksi asiakirjat, joita ei ole järjestetty tiettyjen perusteiden mukaisesti eivät kuuluu asetuksen soveltamisalaan (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 johdanto-osan kohta 15). Esimerkiksi jos yrityksellä on mappi, jossa on asiakastietoja täysin epämääräisessä

järjestyksessä siihen ei välttämättä sovelleta tietosuoja-asetusta, tärkeää on pohtia tulkinnan kannalta sitä, ovatko ne osa jotakin rekisteriä. Lisäksi henkilötiedot, jotka ovat vain puheen varassa, eivät kuulu tietosuoja-asetuksen piiriin, mutta jos toinen henkilö kertoo tiedot suoraan esimerkiksi rekisterin asiakastiedoista, asetus tulee sovellettavaksi. (Nyyssölä 2018, 40.) Lisäksi toiminta, jossa asiakastietoja pidetään vain muistissa mielessä, ei ole asetuksen näkökulmasta rekisteri, johon asetusta sovellettaisiin. Esimerkiksi pienempi kampaamoalan yrittäjä voi muistaa asiakkaansa kasvoista ja tunnistaa heidät, mutta ei pidä mitään paperista kortistoa tai sähköistä listaa asiakkaistaan, silloin hänen mielessään oleva rekisteri ei ole asetuksen kannalta tällainen asiakasrekisteri. (Koivuniemi 2018.) Voidaan siis ajatella, että yrittäjän puhelimen muistissa olevat numerot, joista osa on hänen asiakkaidensa ja osa hänen ystäviensä ja sukulaistensa, olisi myös asiakasrekisteri tai osa sitä.

> *Tätä asetusta sovelletaan henkilötietojen käsittelyyn, jota suoritetaan unionin alueella sijaitsevassa rekisterinpitäjän tai henkilötietojen käsittelijän toimipaikassa toiminnan yhteydessä, riippumatta siitä, suoritetaanko käsittely unionin alueella vai ei* (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 1.luvun 3. artiklan kohta 1).

Asetus tulee sovellettavaksi tietyissä tilanteissa, vaikka organisaatio ei olisi sijoittautunut unionin alueelle (Oikeusministeriö, Tietosuojavaltuutetun toimisto 2017). Esimerkiksi tilitoimiston käsittelemät henkilötiedot voivat olla Kanadassa asuvien, mutta koska tilitoimisto toimii EU:n alueella, tulee henkilötietojen käsittelyssä soveltaa tietosuoja-asetusta. Asetusta on myös sovellettava tilanteissa, jossa tilanne on päinvastainen. Esimerkiksi kanadalainen tilitoimisto voi toimia yhteistyössä suomalaisen tytäryhtiön kanssa ja itse toiminta tapahtua pilvipalvelussa, silloin sovelletaan myös tietosuoja-asetusta. (Nyyssölä 2018, 41-42.)

Lisäksi asetusta tulee soveltaa, jos suomalainen henkilö tilaa esimerkiksi tuotteita kiinalaiselta verkkosivustolta, johon hänen tulee tallentaa henkilötietoja tilauksen onnistumiseksi. Eli myös palveluissa ja tuotteissa ei ole väliä sillä onko niiden tarjoaja unionin alueella, vaan riittää, että rekisteröity on Euroopan kansalainen. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 1.luvun 3. artiklan kohta 2.)

Asetusta ei sovelleta seuraaviin tapauksiin

Koska asetus koskee vain luonnollisia henkilöitä sitä ei vastaavasti sovelleta esimerkiksi yrityksiin, valtioihin tai kuntiin (Nyyssölä 2018, 38).

> *Tämä asetus ei koske oikeushenkilöiden ja erityisesti oikeushenkilöiden muodossa perustettujen yritysten henkilötietojen käsittelyä, kuten oikeushenkilön nimeä, oikeudellista muotoa ja yhteystietoja* (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 johdanto-osan kohta 14).

Lisäksi asetusta ei sovelleta tilanteisiin, joissa viranomaiset käsittelevät henkilötietoja tiettyä tarkoitusta varten. Tällaisia tarkoituksia ovat muun muassa rikoksien selvittelyyn, ennaltaehkäisemiseen ja syytteisiin liittyvä henkilötietojen käsittely tai tilanteet, joissa tarkoituksena on suojella yleistä turvallisuutta. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 1.luvun 2.artikla.) Näihin tilanteisiin sovelletaan erillistä unionin antamaa säädöstä Euroopan parlamentin ja neuvoston direktiiviä (EU) 2016/680. Vastaavasti jos viranomainen käsittelee henkilötietoja muuta tarkoitusta varten, sovelletaan tietosuoja-asetusta. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 johdanto-osan kohta 19.)

Anonyymi

Asetuksen johdanto-osan kohdassa 26 kerrotaan, että asetus ei koske anonyymien tietojen käsittelyä (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 johdanto-osan kohta 26). Anonyymejä tietoja voi olla kahdenlaisia, kuten on havainnollistettu taulukossa 2. Anonyymit tiedot ovat tietoja, jotka eivät liity tunnistettuun henkilöön tai tunnistettavissa olevaan henkilöön (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 johdanto-osan kohta 26). Taulukossa 2 henkilö A on tiedossa, mutta hänen henkilötietoja ei ole tiedossa, siksi hän on anonyymi. Henkilö X on myös anonyymi, vaikka hänestä tiedetään muutama henkilötieto, henkilötietoja on kuitenkin vielä niin vähän, että häntä ei voida niiden perusteella tunnistaa.

Taulukko 2. Anonyymi ja Pseudonyymi

Anonyymi		
	Henkilö A	Henkilö X
Henkilötieto	x	Ikä
Henkilötieto	x	Sukupuoli
Pseudonyymi		
Henkilötieto		Ammattiryhmä
Henkilötieto		Kotipaikka

Anonyymien tietojen perusteella luonnollista henkilöä ei voida enää tunnistaa. Tai jos luonnollinen henkilö on tunnistettavissa, tietoja ei pystytä yhdistämään häneen. Tämä tarkoittaa sitä, että tiedot on esimerkiksi eroteltu niin, ettei näitä tietoja voi enää yhdistää

luonnolliseen henkilöön kohtuullisella vaivalla. Kohtuulliseen vaivaan tulee huomioida niin siitä koituvat kustannukset kuin käytettävissä oleva teknologia, unohtamatta tähän tarvittavaa aikaa. Tämän takia asetus ei estä henkilötietojen keräämistä tutkimus- tai tilastotarkoitusta varten. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 johdanto-osan kohta 26.)

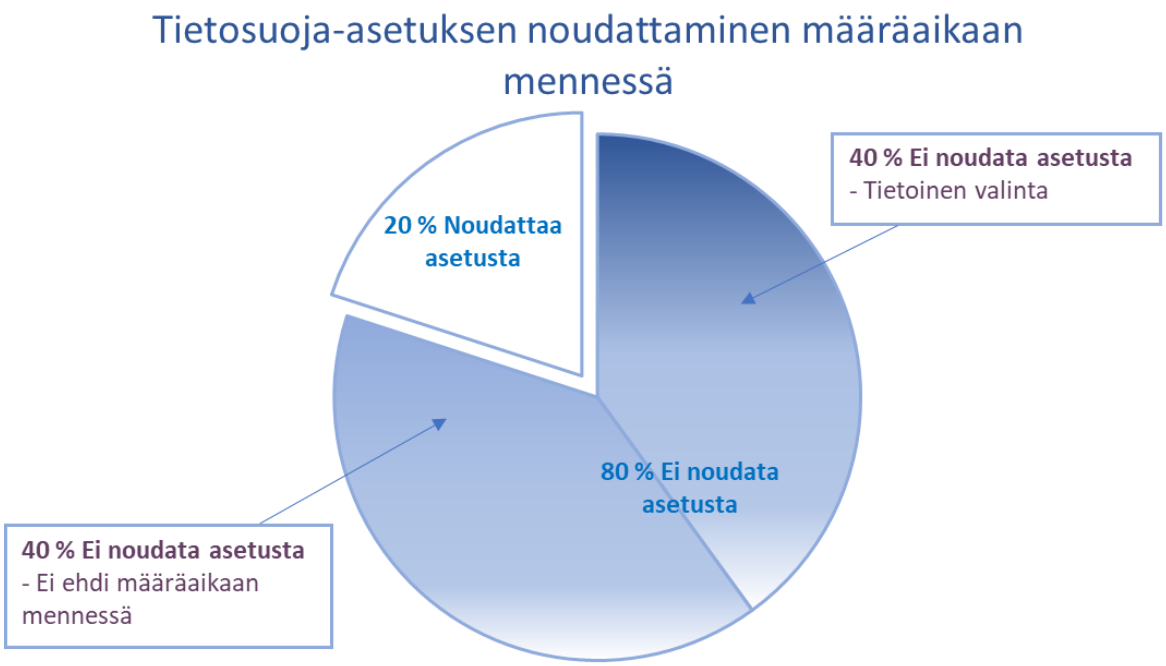
Pseudonyymi

Anonyymi käsitteeseen liittyy läheisesti käsite pseudonyymi, joka tarkoittaa henkilötietoa, joka voidaan yhdistää luonnolliseen henkilöön lisätietoja käyttämällä (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 johdanto-osan kohta 26). Tätä on havainnollistettu taulukossa 2 (Taulukko 2, sivu 18), henkilö on aluksi ollut tunnistamaton, anonyymi, mutta kun häneen voidaan liittää tarpeeksi paljon henkilötietoja, hänet voidaan niiden perusteella tunnistaa. Tällöin tiedoista tulee asetuksen kannalta henkilötietoja, joihin asetusta tulee soveltaa. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 johdanto-osan kohta 26).

Lisäksi asetusta ei sovelleta kuolleisiin henkilöihin vaan jokainen jäsenvaltio saa itse päättää säännöt, miten näiden tietojen kohdalla toimitaan (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 johdanto-osan kohta 27). Ainakaan vielä ei Suomessa ole tällaista lainsäädäntöä, joka kertoisi esimerkiksi miten kuolleen työntekijän henkilötietoja tulisi käsitellä (Nyyssölä 2018, 38-39).

2.6 Ennakkovalmistautuminen

Asetuksen noudattaminen vaatii monissa yrityksissä paljon käytännönjärjestelyitä. Osassa yrityksissä on nimettävä tietosuojavastaava, muutettava sopimuksia erityisesti vastuukysymysten takia ja muutettava mahdollisesti myös toimintatapoja. Ohjelmistot on päivitettävä sellaisiksi, että kuluttaja voi tarvittaessa vaihtaa tietonsa yrityksestä toiseen ja tarkistaa tietonsa suoraan sähköisesti tietokannasta. (Lehto 2017.)



Kuvio 3. Tietosuoja-asetuksen noudattaminen Forresterin tutkimuksen (2018b) mukaan

Kuviossa 3 esitetään Forresterin (2018a) tutkimuksessa esitetyt arviot asetusta määräaikaan mennessä noudattavista yrityksistä sekä syistä, miksi asetusta ei noudatettaisi. Amerikkalainen tutkimus- ja neuvonantajayritys Forrester (2018b) ennustaa, että alle 80 % yrityksistä noudattaa asetusta määräaikaan mennessä (Forrester 2018a; Forrester 2018b). Tätä on havainnollistettu kuviossa 3. Forrester (2018b) ennakoi, että näistä 80 % puolet jättää asetuksen vaatimukset täyttämättä tahallaan. Syynä on se, että yritykset arvioivat muutoksista koituvat kustannukset suuremmiksi kuin asetuksen täyttämättä jättämisestä koituvat sanktiot. (Forrester 2018b.) Toisaalta Toivosen (2017) mukaan sanktiot voivat olla jopa niin kovat, että ne voivat kaataa yrityksen. Vastaavasti toinen puoli yrityksistä, jotka eivät noudata asetusta määräaikaan mennessä, pyrkivät muuttamaan toimintansa asetuksen mukaiseksi, mutta epäonnistuvat aikataulun takia tai onnistuvat vain osittain. (ID BBN 2017.)

Toisaalta hyvällä valmistautumisellakin uskotaan olevan puolensa. Jos yritys on valmistautunut hyvin asetuksen vaatimiin muutoksiin ja hoitanut muutokset asianmukaisesti ja huolellisesti, asiakkaat voivat nähdä tämän myönteisenä osana asiakaspalvelua ja se voi mahdollisesti tuoda yritykselle myös kilpailuetua. (Hanninen ym. 2017, 14.)

Forresterin (2018b) ennusteeseen verrattuna Suomessa luvut eivät ole sen paremmat. Vuonna 2017 arvioitiin että, vain alle 2 % suomalaisista yrityksistä on tehnyt tarvittavat muutokset tai selvitykset tietosuoja-asetusta varten (Forrester 2018b). Toisaalta valmistautumisessa arvellaan olevan suuria alakohtaisia eroja. Tämän arvellaan johtuvan siitä,

että pienemmät yritykset voivat ajatella asetuksen koskevan vain suurimpia yrityksiä tai vain tiettyjä aloja. (Lehto 2017.)

Valmistautumisen arvellaan olevan pisimmällä tietotekniikka-alan yrityksissä. Toisaalta Roihan mukaan kyseiselle toimialalle asetus on erityisen haastava, sillä asetus koskee niitä sekä rekisterinpitäjän että tietojenkäsittelijän roolissa. (Lehto 2017.) Sama pätee myös tilitoimistoihin, jotka ovat usein sekä tiedonkäsittelijöitä että rekisterinpitäjiä.

2.7 Tietosuoja-asetuksen soveltaminen käytännössä

Kantelisen (2018) mukaan asetuksen soveltaminen on lähtenyt hyvin liikkeelle. Hän kuvaakin asetuksen voimaantuloa toukokuussa eräänlaiseksi yritysten välietapiksi ja toteaa, että monet organisaatiot ovat jatkaneet projektin viimeistelyä ja toimenpiteiden loppuun saattamista tämän jälkeen. Lisäksi Kantelisen mielestä asetuksesta liikkui paljon uhkakuvia ennen kuin se astui voimaan, mutta ne ovat osoittautuneet harhaanjohtaviksi.

Toisaalta Ruotsissa datavalvontaviranomainen Datainspektionen on aloittanut tutkinnan yli 60 yrityksestä. Tarkoituksena on selvittää, täyttävätkö yhtiöt EU:n tietosuoja-asetuksen velvoitteet. (Kantelinen 2018; Lehmusvirta 2018.) Jos velvoitteita ei ole noudatettu, sanktioina ovat varoitus, sekä pahimmillaan kymmenen miljoonan euron sakot tai yhtiöiden maailmanlaajuisesta liikevaihdosta 2 %, jotka vastaavat asetuksen 8:nnen luvun artiklan 83 kohdan 4 hallinnollisten sakkojen määrää (2016/679 8.luku artikla 83 kohta 4; Lehmusvirta 2018). Tutkittavia yrityksiä on monelta toimialalta; muun muassa pankkeja, viranomaisia, liittojärjestöjä ja teleoperaattoreita. Tutkinta yrityksistä aloitettiin kesäkuussa, vain muutama päivä sen jälkeen, kun asetus astui voimaan. Tuloksien oli tarkoitus ilmestyä elokuussa, mutta tutkinta on vieläkin kesken. (Kantelinen 2018; Lehmusvirta 2018.)

Ensimmäinen GDPR rikkomus tuli julki Saksassa heinäkuussa (Virtanen 2018). Saksan tuomioistuin totesi, että tapauksessa rikottiin asetuksen 5:nnen artiklan periaatteita, koska henkilötietoja oli kerätty tarpeettomasti. Asiassa voittoa tavoittelematon amerikkalainen ICANN-yhtiö ja sen saksalainen yhteistyökumppani EPAG olivat vastakkain. (Millar & Marshall 2018.) ICANN oli vaatinut yhteistyökumppaniaan keräämään henkilökohtaisia tietoja ihmisistä, jotka ostavat verkkotunnuksia. Lisäksi ICANN halusi tietää verkkotunnuksia tehneiden tahojen teknisien ja hallinnollisten henkilöiden nimet sekä yhteystiedot. EPAG ei suostunut keräämään jälkimmäisiä henkilötietoja, koska niille ei ollut asetuksen mukaista oikeudellista perustetta, eikä niiden kerääminen ollut ICANN:in liiketoiminnan kannalta välttämätöntä. (Millar & Marshall 2018; Virtanen 2018.) ICANN teki tästä kanteen paikalliselle oikeusistuimelle Saksassa, ja väitti että kyseisiä henkilötietoja tarvittiin mahdollisten ongelmien ratkaisemiseksi, joita voi syntyä, kun verkkotunnuksia luodaan. Kanne

kuitenkin hylättiin, koska oikeusistuin totesi näiden tietojen keräämisen rikkovan tietojen minimoinnin periaatetta. Lisäksi oikeusistuin totesi, ettei kyseisiä tietoja ole kerätty aiemminkaan eikä ICANN:lla ollut riittäviä perusteita miksi niiden keruu nyt olisi välttämätöntä. ICANN on valittanut päätöksestä korkeimpaan alueellisen tuomioistuimeen, eikä sieltä ole vielä tullut päätöstä. (Millar & Marshall 2018.) Tapausta voidaan kuitenkin pitää tärkeänä ennakkotapauksena (Virtanen 2018).

ICANN on ollut muutenkin julkisuudessa tietosuoja-asetukseen liittyen, koska yhtiö valvoo maailmanlaajuista WHOIS-tietokantaa, joka sisältää rekisteröityjen verkkotunnuksia, WHOIS-palvelu on kuin internetin puhelinluettelo. WHOIS:sta on voinut kuka tahansa löytää verkkotunnuksella rekisteröityneen tahon yhteystiedot. (MTV Uutiset 2018; Millar & Marshall 2018.) Tietosuoja-asetuksen myötä ICANN teki tietokantaan rajoituksia, ettei kuka vaan voi enää päästä käsiksi kaikkiin tietoihin. Palvelusta löytyviä verkkotunnuksia on aiemmin hyödynnetty rikostutkinnassa, koska tietokanta on ollut poliisin merkittävä apu kyberrikoksia selvitettäessä. Tietokannan poistuminen kokonaan tietosuoja-asetuksen takia heikentäisi Poliisihallituksen mukaan nettirikosten torjuntamahdollisuutta. (MTV Uutiset 2018.)

3 HENKILÖTIETOJEN KÄSITTELYÄ KOSKEVAT PERIAATTEET

3.1 Seitsemän yleistä periaatetta

Rekisterinpitäjää ohjaavat tietosuoja-asetuksessa säädetyt seitsemän yleistä periaatetta, näistä kerrotaan asetuksen 2. luvun artikloissa 5-11. Nämä on esitetty taulukossa 3. Henkilötietojen käsittelyn periaatteita noudattamalla rekisterinpitäjä käsittelee henkilötietoja rekisteröidyn oikeuksia ja vapauksia kunnioittaen (Oikeusministeriö, Tietosuojavaltuutetun toimisto 2017). Nyyssölän (2018, 65) mukaan nämä ovat koko asetuksen kannalta keskeisimmät, koska niissä tiivistyy lähes koko asetus ja muut artiklat konkretisoivat näitä periaatteita.

Taulukko 3. Tietosuoja-asetuksen periaatteet (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 2.luku)

Artiklan sisältö		Olennaisuus tilitoimistoissa
Artikla 5	Henkilötietojen käsittelyä koskevat periaatteet	Kaikessa henkilötietojen keruussa noudatettavat ohjeistukset
Artikla 6	Käsittelyn lainmukaisuus	Määrittää millä perusteilla henkilötietoja saa kerätä
Artikla 7	Suostumuksen edellytykset	Ei yleinen tilitoimistoalalla
Artikla 8	Lapsen suostumukseen sovellettavat ehdot	Ei yleinen tilitoimistoalalla
Artikla 9	Erityiset henkilötietoryhmät	Esim. ammattiliiton jäsenyys
Artikla 10	Rikostuomiot ja rikkomukset	Ei yleinen tilitoimistoalalla
Artikla 11	Käsittely, joka ei edellytä tunnistamista	Asetus ei itsessään edellytä tunnistamista, jos joku muu syy ei sitä vaadi

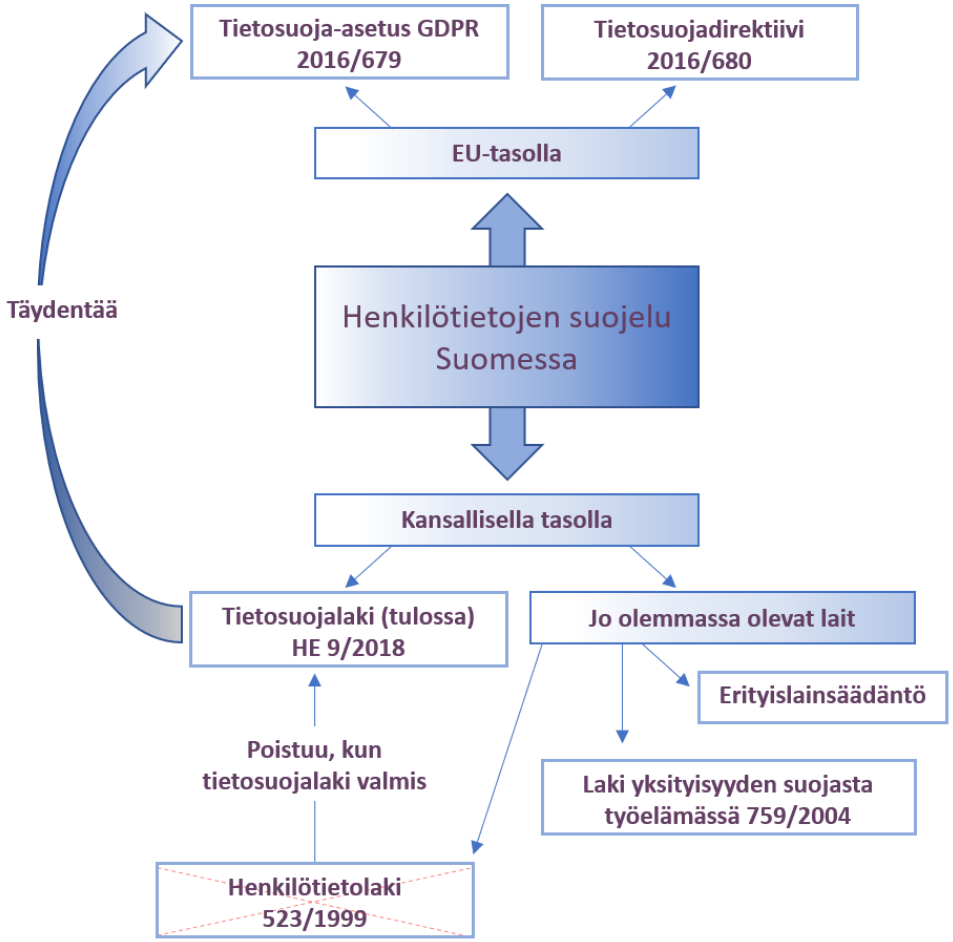
Taulukossa 3 on listattuna tietosuoja-asetuksen kaikki periaatteet. Taulukossa on huomioitu, kuinka suuri merkitys kyseisellä periaatteella on erityisesti tilitoimistoihin. Tässä työssä käydään tarkemmin läpi artiklat 5-6, joissa käydään läpi henkilötietojen käsittelyyn liittyvät periaatteet ja käsittelyn lainmukaisuus sekä erityiset henkilötietoryhmät, koska nämä periaatteet koskevat erityisesti tilitoimistoja. Artiklat 5-6 käsitellään yhdessä, koska ne liittyvät niin vahvasti yhteen. Voidaankin sanoa, että 5. artiklan lainmukaisuus kohtaa on täydennetty artiklalla 6.

Tietosuoja-asetuksen ydin muodostuukin Nyyssölän (2018, 90) mukaan asetuksen 5:nnessä artiklassa olevista henkilötietojenkäsittelyä koskevista periaatteista ja 6:nnessa artiklassa olevasta käsittelyn lainmukaisuudesta. Artiklat nivoutuvat tiiviisti yhteen, koska

5:s artikla käsittelee sitä millä tavoin henkilötietoja tulee käsitellä ja 6:s artikla sitä, millä perustein henkilötietoja saa käsitellä. Periaatteet tulevat suoraan asetuksen 2. luvun 5:nnestä artiklasta. Seuraavissa luvuissa 3.2-3.8 on avattu tarkemmin taulukon 3 (Taulukko 3, sivu 23) artiklojen sisältöä.

3.2 Lainmukaisuus, kohtuullisuus ja läpinäkyvyys

Henkilötietoja tulee käsitellä lain- ja asianmukaisesti sekä rekisteröidyn kannalta läpinäkyvästi (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 2.luku 5.artikla kohta 1). Lainmukaisuudella tarkoitetaan sitä, että henkilötietoja on käsiteltävä laillisesti. Käsittelyssä on huomioitava EU:n asetuksen määräysten lisäksi Suomen lainsäädäntö, kuten tuleva tietosuojalaki, laki yksityisyyden suojasta työelämässä sekä voimassa oleva erityislainsäädäntö. (Nyyssölä 2018, 71.) Tätä on havainnollistettu kuviossa 4. Kuoviosta voi huomata, miten sekä EU:sta että kansallisesta lainsäädännöstä tulee määräyksiä, miten henkilötietoja tulee käsitellä. Lisäksi vireillä olevan tietosuojalain on tarkoitus korvata henkilötietolaki ja täydentää tietosuoja-asetuksen jättämää kansallista liikkumavaraa.



Kuvio 4. Henkilötietojen suojelu Suomessa

Lainmukaisuudella ei tässä tapauksessa viitata vain lainsäädännöstä tuleviin perusteisiin, koska tämä tarkoittaisi sitä, että henkilötietojen käsittely olisi aina laitonta, jos juuri tälle käsittelylle ei olisi laissa vastinetta (Nyyssölä 2018, 89). Kuitenkin esimerkiksi rekisteröidyn suostumus on riittävä peruste hänen henkilötietojensa käsittelylle. Toisin sanoen, kun henkilötietojen käsittelylle löytyy peruste asetuksen 6:nnen artiklan ensimmäisestä kohdasta, käsittely on lainmukaista. Peruste on olemassa, kun vähintään yksi näistä kuudesta edellytyksestä täyttyy. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 2.luku artikla 6 kohta 1.) Edellytykset on esitelty taulukossa 4, Henkilötietojen käsittelyn lainmukaisuus ja näitä kohtia avataan tarkemmin luvussa 3.3 Käyttötarkoitussidonnaisuus sivulla 27.

Taulukko 4. Henkilötietojen käsittelyn lainmukaisuus

Henkilötietojen käsittelyn lainmukaiset edellytykset	
Rekisteröidyn	suostumus
	sopimuksen solmiminen
	etujen suojaaminen
Rekisterinpitäjän	lakisääteinen velvoite
	oikeutettu etu
	julkinen valta
yleisen edun suorittaminen	

Asetuksessa käytetään myös sanaa asianmukaisuus. Nyyssölän (2018, 71-73) mukaan on kuitenkin vaikea nähdä kyseisellä termillä itsenäistä juridista sisältöä. Nyyssölä toteaakin, että on hieman itsestään selvää, että henkilötietojen käsittely on asianmukaista, kun rekisterinpitäjä noudattaa asetuksen määräyksiä. Sama koskee myös kohtuullisuus termiä. Termi mainitaan 5:nnen artiklan ensimmäisessä kohdassa, termi ei tule ilmi ollenkaan asetuksen aiemmasta tekstistä. Nyyssölä arveleekin, että kohtuullisuus on epäonnistunut sanavalinta, eikä sillä ole itsenäistä sisältöä. Tällä Nyyssölä tarkoittaa sitä, että asetuksen tekstissä ei ole minkäänlaista viittausta kohtuuttomuuteen eikä kerrottu, mitä sillä tarkoitetaan. Noudattamalla asetusta ja lakeja henkilötietojen käsittelyssä on käsittelyä pidettävä kohtuullisena, vaikka se voisi jakaa mielipiteitä.

Läpinäkyvyys

Läpinäkyvyydellä tarkoitetaan muun muassa sitä, että rekisteröidyllä on oikeus saada tietää mitä tietoja hänestä on kerätty. Tiedot tulee esittää tiivistetysti, selkeästi ja helposti ymmärrettävässä muodossa. Kohdassa huomioidaan myös erityisesti se, että teksti pitää olla mahdollisimman yksinkertaisella kielellä, jotta lapsetkin voivat ymmärtää tekstin sisällön. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 3.luku 12. artikla kohta 1.) Läpinäkyvyyden käsite voi olla hieman hämäävä koska tällä tarkoitetaan nimenomaan sitä, että tietojen tulee olla läpinäkyviä vain rekisteröidylle itselleen ei kaikille muille (Nyyssölä 2018, 66).

Rekisteröidyllä on oikeus saada tiedot, jotka rekisterinpitäjä on kerännyt rekisteröidyltä itseltään, ja tiedot, jotka rekisterinpitäjä on saanut jotain toista kautta. Molemmissa tapauksissa rekisteröidyllä on oikeus lisäksi saada tietää muun muassa miksi hänen henkilötietojaan on käsitelty, kuinka kauan niitä säilytetään ja oikeus pyytää tietojensa poistamista. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 3. luku artiklat 13-14.) Rekisteröidyllä on oikeus saada nämä tiedot ilmaiseksi. Kuitenkin, jos rekisteröity käyttää asemaansa väärin ja pyytää tietojaan toistuvasti tai perusteettomasti on rekisterinpitäjällä oikeus kieltäytyä toimittamasta tietoja tai periä tietojen toimittamisesta kohtuullinen korvaus. Rekisterinpitäjällä on aina näyttövelvollisuus, että rekisteröity on pyytänyt tietoja turhaan. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 3.luku artikla 12 kohta 5.) Rekisteröidyn täytyy tarkastuspyynnössä eritellä mitkä tiedot haluaa tarkastaa, haluaako tiedot tietyltä ajanjaksolta vai kaikki hänestä kerätyt tiedot. Rekisteröidyn tulee määritellä missä muodossa haluaa tiedot; sähköisesti tai paperilla ja lisäksi tulee ilmoittaa yhteystiedot, johon rekisterinpitäjä voi toimittaa rekisteröidyn tiedot. (Tietosuojavaltuutetun toimisto 2018a.) Rekisteröity ei voi pyytää yleisesti kaikkia henkilötietojaan, joita hänestä on kerätty, vaan rekisteröidyn pitää tietää mitä kysyy. Rekisterinpitäjän vastuulla on myös tunnistaa, että henkilö, joka tietoja kysyy, on oikeutettu niihin, eli varmistaa tarvittaessa rekisteröidyn henkilöllisyys täsmentävin lisäkysymyksin. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 3.luku artikla 12 kohta 6.)

Jos jostain syystä rekisterinpitäjä ei toteuta rekisteröidyn pyyntöä esimerkiksi oikaista omia tietojaan, on rekisterinpitäjällä velvollisuus ilmoittaa mahdollisimman pian, kuitenkin viimeistään kuukauden kuluttua, syyt miksi hän ei ole toiminut pyynnön mukaan. Lisäksi hänen pitää kertoa rekisteröidylle, että hänellä on mahdollisuus tehdä asiasta valvontaviranomaiselle valitus. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 3.luku artikla 12 kohta 4.)

3.3 Käyttötarkoitussidonnaisuus

Käyttötarkoitussidonnaisuus tarkoittaa sitä, että kerättävillä henkilötiedoilla pitää olla laillinen ja nimenomainen tarkoitus (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 2.luku 5 artikla kohta 1). Kerättävillä tiedoilla pitää olla selkeä peruste; tietoja ei voi enää kerätä vain mielenkiinnosta tai varmuuden varalle (Nevasalo & Parviainen 2017, 31). Toisin sanoen, jos kyseinen toimenpide ei välttämättä vaadi henkilötietojen käsittelyä, niitä ei pitäisi käsitellä (Hanninen ym. 2017, 49). Lisäksi, kun henkilötietoja on kerätty alun perin tiettyä tarkoitusta varten, ei niitä saa myöhemmin soveltaa yhteensopimattomalla tavalla alkuperäisen tarkoituksen kanssa (Nevasalo & Parviainen 2017, 31).

Tarkemmin perusteet, joiden mukaan henkilötietojen käsittely on lainmukaista, on kerrottu tietosuoja-asetuksen 2. luvun 6:nnessa artiklassa. Tiivistetysti käsittely on lainmukaista, jos se perustuu rekisteröidyn suostumukseen, sopimuksen täytäntöön panemiseen, rekisteröidyn tai toisen henkilön etujen suojaamiseen, rekisterinpitäjän oikeutettuun etuun tai lakisääteisten velvoitteiden noudattamiseen (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 2.luku artikla 6 kohta 1). Nämä on esitetty taulukossa 5 (Taulukko 5, sivu 39).

Suostumus

Suostumuksen määritelmästä säädetään tarkemmin asetuksen 2. luvun 7:nnessä artiklassa (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679), mutta koska se ei ole kovin yleinen tilitoimistoalalla, sitä ei käydä tässä työssä sen tarkemmin läpi. Yksinkertaistettuna voidaan sanoa, että suostumus tulee pystyä osoittamaan ja sen täytyy olla kohdistettu tiettyyn tai selkeästi tiettyihin tarkoituksiin. Eli yleisesti yhdellä suostumuksella ei voi antaa lupaa kaikkeen henkilötietojen käsittelyyn kyseisessä tilitoimistossa. Tarkemmin ei ole määritelty kuinka tarkkaan jokainen erityinen tarkoitus on määriteltävä. (Nyyssölä 2018, 92.) Lisäksi asetus ei vaadi, että rekisteröidyn suostumus olisi kirjallinen, mutta osoitusvelvollisuuden kannalta on lähes mahdotonta osoittaa toteen muu kuin kirjallinen tahdon ilmaisu (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 1.luku artikla 4 kohta 11). Lisäksi käsittelylle olisi aina hyvä löytää joku muu syy kuin pelkästään suostumus, koska rekisteröidyllä on oikeus perua suostumus, milloin tahansa (Koivumäki 2017).

Oikeutettu etu

Oikeutettu etu on Suomessa uusi käsite, vaikkakin se on ollut muissa jäsenmaissa jo aiemmin käytössä (Nyyssölä 2018, 97). Kun asetus astui voimaan, monet yritykset lähettivät esimerkiksi sähköpostin työntekijöilleen, jossa pyysivät suostumusta lähettää uutiskirje työntekijälle jatkossakin. Viestintäalan konsultin Fårsgårdin (2018) mielestä turhat

sähköpostien lupakyselyt asetuksen voimaantulon yhteydessä ovat seurausta väärinkäsityksestä, jossa yritykset eivät ole ymmärtäneet oikeutetun edun periaatetta. Oikeutettu etu tarkoittaa sitä, että henkilötietoja saa käsitellä ilman erillistä lupaa, kun rekisterinpitäjän ja rekisteröidyn välillä on jokin merkityksellinen suhde (Lehto 2018.) Merkityksellisestä suhteesta on kyse, kun rekisteröity on esimerkiksi rekisterinpitäjän asiakas tai alainen (Tietosuojavaltuutetun toimisto 2018b). Henkilötietojen käsittelylle on laillinen peruste kun:

> — — *käsittely on tarpeen rekisterinpitäjän tai kolmannen osapuolen oikeutettujen etujen toteuttamiseksi, paitsi milloin henkilötietojen suojaa edellyttävät rekisteröidyn edut tai perusoikeudet ja -vapaudet syrjäyttävät tällaiset edut, erityisesti jos rekisteröity on lapsi* (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 2.luku artikla 6 kohta 1f).

Eli, jotta voitaisiin vedota oikeutettuun etuun, täytyy pohtia intressejä sekä rekisterinpitäjän, että rekisteröidyn näkökulmasta (Nyyssölä 2018, 96). Henkilötietoja ei saa käsitellä, jos rekisteröidyn oikeudet syrjäyttävät rekisterinpitäjän tai kolmannen osapuolen edun (Tietosuojavaltuutetun toimisto 2018b). Tieteellisissä ja historiallisissa tutkimuksissa henkilötietojen käsittely voi perustua oikeutettuun etuun tai kun henkilötietoja käsitellään petoksen estämiseksi (Nyyssölä 2018, 97; Tietosuojavaltuutetun toimisto 2018b; Euroopan komissio 2018).

Rekisteröidyllä on kuitenkin aina oikeus vastustaa henkilötietojensa käsittelyä, jos perusteena on vain oikeutettu etu. Tällöin, jos rekisterinpitäjä ei pysty osoittamaan henkilötietojen käsittelyyn tärkeää tai perusteltavaa syytä, on rekisterinpitäjän lopetettava henkilötietojen käsittely (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 4.jakso artikla 21 kohta 1.)

Kuitenkin käsittelyn lainmukaisuuden kohdassa neljä määritetään myös se mihin muuhun ja millä perustein jo kerättyjä tietoja saa käyttää, kuin alkuperäiseen tarkoitukseensa (Nyyssölä 2018, 74; Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 2.luku artikla 6 kohta 4). Nyyssölän (2018, 99) mukaan neljännen kohdan voi tiivistää niin, että käyttötarkoitussidonnaisuuden periaatteella ei voida perustella henkilötietojen käyttöä, jos niiden uusi käyttötarkoitus on kaukana vanhasta ja siitä koituu haittaa rekisteröidylle. Vastaavasti jos uudesta henkilötietojen käytöstä ei koidu rekisteröidylle merkittäviä haittoja tai tietojen käyttö liittyy läheisesti aiempaan käyttötarkoitukseen, ei henkilötietojen käytölle ole tällöin estettä.

3.4 Tietojen minimointi

Tietojen minimoinnista on myös käytetty termiä tarpeellisuusvaatimus, joka on mainittu suomalaisessa lainsäädännössä jo aiemminkin muun muassa laissa yksityisyyden suojasta työelämässä. Tämä tarkoittaa sitä, että henkilötietoja ei saa kerätä enempää kuin on toiminnan kannalta tarpeellista ja perusteltua. (Nyyssölä 2018, 66;75.)

> *Henkilötietojen on oltava asianmukaisia ja olennaisia ja rajoitettuja siihen, mikä on tarpeellista suhteessa niihin tarkoituksiin, joita varten niitä käsitellään* (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 2. luku artikla 5 kohta 1).

Rekisteröidyistä ei saa kerätä turhia tietoja. Toisin sanoen, kerättäviä henkilötietoja pitää olla vain sen verran, mikä on käsittelyn kannalta välttämätöntä. Tuleekin huomioida, että vaikka henkilötietojen keräämiseen olisi rekisteröidyn suostumus, tietoja ei saa kerätä, jos ne eivät ole kyseisen käyttötarkoituksen kannalta tarpeellisia. (Hanninen ym. 2017, 49.) Nyyssölä (2018, 66) ihmetteleekin, miksi tästä kohdasta ei ole asetuksen kannalta tarkempia määräyksiä, koska kohta on kuitenkin hänestä melkein koko asetuksen kannalta olennaisin.

3.5 Täsmällisyys

Täsmällisyys tarkoittaa sitä, että tietojen on oltava ajantasaisia ja voimassa olevia, eli yritysten on päivitettävä niitä aika ajoin. Yrityksen velvollisuus on toimia niin, että kohtuullisilla toimenpiteillä varmistetaan virheellisten henkilötietojen poistaminen tai korjaaminen. (Hanninen ym. 2017, 50.) Eli rekisterissä oleva virheellinen tieto ei ole asiakkaan vika tai asiakkaan vastuulla oikaista, vaan rekisterinpitäjän tehtävä on oma-aloitteisesti oikaista tiedot oikeiksi. Tiedon oikeellisuudeksi ei kuitenkaan yrityksen tarvitse käyttää kohtuuttomasti resursseja. Kuitenkin kaikki mikä kohtuuden rajoissa pystytään tekemään, on tehtävä. Mitä tämä sitten tarkoittaa käytännössä? (Nyyssölä 2018, 79-80.) Nyyssölän (2018, 80) mukaan kohtuullisuutta voisi verrata siihen, mikä merkitys tiedon oikeellisuudella on rekisteröidylle. Esimerkiksi palkanlaskennassa on rekisteröidylle hyvin olennaista, että palkkatiedon muutos päivittyy välittömästi oikeaksi, verrattuna siihen, että palkansaaja pyytää työtodistusta viiden vuoden jälkeen. Eli yrityksen tuskin on järkevää panostaa siihen, että työsuhteensa päättäneen työntekijän henkilötiedot olisivat ajan tasalla monen vuoden jälkeenkin. Yritysten kannattaa panostaa enemmän siihen, että tiedot, joilla on sillä hetkellä merkitystä, olisivat oikein.

3.6 Säilytyksen rajoittaminen

Säilytyksen rajoittamisessa säädellään sitä, miten pitkään ja minkälaisessa muodossa henkilötietoja saa säilyttää. Tällaista lainsäädäntöä ei ole aikaisemmin Suomessa ollut. (Nyyssölä 2018, 81.)

> *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.* (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 2.luku 5 artikla.)

Henkilötietoja ei saa säilyttää kauempaa kuin on tarpeen käsittelyn tarkoituksen toteuttamista varten (Hanninen ym. 2017, 50). Tämä on tulkittavissa niin, että henkilötietoja ei saa säilyttää tunnistettavassa muodossa kauemmin kuin on tarpeen (Nyyssölä 2018, 81). Esimerkiksi jos kyseessä on asiakassuhde, on usein tarpeen säilyttää tietoja koko asiakassuhteen ajan. Asiakassuhteen loputtua tietoja on tarpeen säilyttää esimerkiksi mahdollisten reklamaatioiden, perinnän, oikeudellisten toimenpiteiden tai takuun ajan. Jos yritys haluaa säilöä tietoja pidempään esimerkiksi tilastollisista syistä, se on mahdollista toteuttaa säilyttämällä tiedot ilman henkilötietoja. (Hanninen ym. 2017, 50.) Esimerkiksi tilitoimisto voi säilyttää tietoa kauanko on kulunut aikaa tietyn asiakkaan projektiin, jos he poistavat asiakastiedot niin, että asiakasta ei voi sen perusteella enää tunnistaa.

3.7 Eheys ja luottamuksellisuus

Tietojen eheyteen ja luottamuksellisuuteen liittyy läheisesti tietoturva (Hanninen ym. 2017, 51). Eheyden ja luottamuksellisuus kohdan tärkein sisältö koskee sitä, että rekisterinpitäjän on huolehdittava siitä, että rekisteröityjen henkilötietoja käsitellään turvallisesti (Nyyssölä 2018, 82). Miten tiedot on suojattu, ettei niitä käsitellä luvattomasti tai lainvastaisesti. Millä varmistetaan, että ulkopuolinen ei pääse käsiksi laitteistoihin, joilla henkilötiedot ovat. Yrityksen on varmistettava henkilötietoja käsittelyn asianmukainen turvallisuus ja luottamuksellisuus. Yrityksen vastuulla on myös se, etteivät tiedot vahingossa häviä, tuhoudu tai vahingoitu. (Hanninen ym. 2017, 51.) Tietojen häviämistä, tuhoutumista, lainvastaista muuttamista tai vahingoittumista pidetään tietosuojaloukkauksina, joista rekisterinpitäjän tulee ilmoittaa valvontaviranomaiselle (Nyyssölä 2018,83; Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 1. luku 4. artiklan kohta 12). Vastaavasti jos kyse on

rikkomuksesta, jossa on mahdollista rikkoa rekisteröidyn oikeuksia tai vapauksia, rikkomuksesta pitää ilmoittaa tietosuojavaltuutetulle (Nyyssölä 2018, 83).

Luottamuksellisuusvaatimusta täsmentää tulevan tietosuojalain 35 §, jossa säännellään vaitiolovelvollisuudesta (Nyyssölä 2018, 83).

> *Joka henkilötietojen käsittelyyn liittyviä toimenpiteitä suorittaessaan on saanut tietää jotakin toisen henkilön ominaisuuksista, henkilökohtaisista oloista, taloudellisesta asemasta taikka toisen liikesalaisuudesta, ei saa oikeudettomasti ilmaista sivulliselle näin saamiaan tietoja eikä käyttää niitä omaksi tai toisen hyödyksi tai toisen vahingoksi* (HE 9/2018 6. luvun 35 §).

Pykälän mukaan tietoja ei saa antaa sivulliselle. Tämä ei kuitenkaan estä esimerkiksi tilannetta, jossa työntekijä tarvitsee toisen henkilötietoja työtehtäviensä hoitamiseen, silloin hän ei ole sivullinen ja hänelle voi luovuttaa tietoja laillisesti. (Nyyssölä 2018, 83.)

Osoitusvelvollisuus

Rekisterinpitäjän on pystyttävä osoittamaan, että kaikkia edellä mainittuja periaatteita noudatetaan henkilötietojen käsittelyssä (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 2.luku 5. artiklan kohta 2). Osoitusvelvollisuutta on käyty läpi tämän työn Tietosuoja asetuksen tavoitteissa, osiossa 2.4. sivulla 12.

3.8 Erityiset henkilötietoryhmät

Erityisillä henkilötietoryhmillä tarkoitetaan arkaluonteisia tietoja, joiden käsittely muodostaa tavanomaista suuremman riskin henkilön yksityisyyden suojalle (Nyyssölä 2018, 104). Arkaluonteisia tietoja ovat muun muassa uskonnollinen vakaumus, terveyttä koskevat tiedot ja ammattiliitonjäsenyys (Hanninen ym. 2017, 40). Tilitoimistoja koskevat erityisesti ammattiliiton jäsenyys ja terveyttä koskevat tiedot, jos tilitoimisto suorittaa yrityksen palkanlaskentaa. Asetuksessa todetaan, että tällaisten arkaluonteisten tietojen käsittely on kiellettyä (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 2. luku 9. artiklan kohta 1). Tällaisten tietojen käsittelyyn on kuitenkin poikkeuksia, jolloin niitä saa käsitellä. Asetuksessa todetaan, että käsittely on sallittua, kun:

> *— — käsittely on tarpeen rekisterinpitäjän tai rekisteröidyn velvoitteiden ja erityisten oikeuksien noudattamiseksi työoikeuden, sosiaaliturvan ja sosiaalisen suojelun alalla, siltä osin kuin se sallitaan unionin oikeudessa tai jäsenvaltion lainsäädännössä tai jäsenvaltion lainsäädännön mukaisessa työehtosopimuksessa, jossa säädetään rekisteröidyn perusoikeuksia ja etuja koskevista asianmukaisista*

> *suojatoimista — —* (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 2. luku 9. artiklan kohta 2).

Tällöin ammattiliiton jäsenyyden käsittely on sallittua, kun se sallitaan työlainsäädännössä (Hanninen ym. 2017, 42). Esimerkiksi Suomen kansallisessa lainsäädännössä on tällä hetkellä henkilötietolaissa, että ammattiliiton jäsenyyttä saa käsitellä, jos se:

> *— — on tarpeen rekisterinpitäjän erityisten oikeuksien ja velvoitteiden noudattamiseksi työoikeuden alalla — —* (Henkilötietolaki 12 § 8 momentti).

Tämä on tulossa samanlaisena myös tulevaan tietosuojalakiin 6 § kolmanteen momenttiin (HE 9/2018 6 § 3 momentti). Lisäksi ammattiliiton jäsenyyttä saa käsitellä, jos rekisteröity itse on saattanut tiedon julkiseksi (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 2. luku 9. artiklan kohta 2). Tällä tarkoitetaan esimerkiksi tilannetta, jossa työntekijä on itse pyytänyt palkanlaskijaa pidättämään palkastaan suoraan ammattiliiton jäsenmaksun. Nyyssölän (2018, 107) mukaan Suomessa ei ole aina luokiteltu ammattiliittoon kuulumista arkaluonteiseksi henkilötiedoksi, koska Suomessa järjestäytymisaste on niin korkea. Tieto luokiteltiin arkaluonteiseksi EU:n henkilödirektiivin perusteella vuonna 1999.

Työntekijän terveydentilaa koskevien tietojen käsittely on myös sallittua tietosuoja-asetuksessa samalla perusteella kuin ammattiliiton jäsenyyden käsittely, 2.luvun 9:nnessä artiklassa kohdassa 2 (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 2. luku 9. artiklan kohta 2). Tarkennuksia terveydentilaa koskevien tietojen käsittelyyn tulee enemmän Suomen omasta lainsäädännöstä, laista yksityisyyden suojasta työelämässä (Laki yksityisyydensuojasta työelämässä 13.8.2004/759 5 §).

> *Työnantajalla on oikeus käsitellä työntekijän terveydentilaa koskevia tietoja, jos tiedot on kerätty työntekijältä itseltään tai hänen kirjallisella suostumuksellaan muualta ja tietojen käsittely on tarpeen sairausajan palkan tai siihen rinnastettavien terveydentilaan liittyvien etuuksien suorittamiseksi taikka sen selvittämiseksi, onko työstä poissaoloon perusteltu syy — —* (Laki yksityisyydensuojasta työelämässä 13.8.2004/759 5 §).

Jos palkanlaskenta on ulkoistettu tilitoimistolle, voi olla, että asiakas toimittaa suoraan työntekijän sairauspoissaolosta lääkärintodistuksen tilitoimistoon. Tällöin tietojen käsittely on tarpeen sairausajan palkan selvittämiseksi ja se on täten laillista. Monissa tapauksissa tilitoimistolle riittää vain tieto työntekijän poissaoloajasta, mutta silloin toimeksiantajan vastuulla on varmistaa, että työntekijä on oikeutettu sairaus ajan palkkaan. Sairausajan palkoista on säännöksiä työsopimuslain 11 § (26.1.2001/55), mutta säännöksiä tulee myös työehtosopimuksista, jotka menevät usein työsopimuslain edelle, koska ovat työntekijälle

edukkaampia (Nyyssölä 2018, 122). Pääsääntönä on, että arkaluonteisia tietoja ei saa käsitellä, eli niiden käsittelyä on suositeltavaa välttää aina kun se on mahdollista (Hanninen ym. 2017, 41).

Henkilötunnus

Henkilötunnuksen käsitteleminen ei kuulu asetuksen mukaisiin eritysiin henkilötietoryhmiin, mutta se kuuluu tietosuoja-asetuksen 9 luvun tietojenkäsittelyyn liittyvien erityistilanteiden sääntelyyn, artiklaan 87. Artiklan 87 mukaan (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679):

> *Jäsenvaltiot voivat määritellä tarkemmin erityiset kansallisen henkilönumeron tai muun yleisen tunnisteen käsittelyn edellytykset. Tässä tapauksessa kansallista henkilönumeroa tai muuta yleistä tunnistetta on käytettävä ainoastaan noudattaen rekisteröidyn oikeuksia ja vapauksia koskevia asianmukaisia suojatoimia tämän asetuksen mukaisesti.*

Toisin sanoen, henkilötunnuksen käsittelyn sääntely on jätetty kokonaan kansalliselle lainsäätäjälle. Henkilötunnus mielletään arkaluonteisiin tietoihin verrattavissa olevana, koska jos sitä käytetään vääriin siitä voi koitua huomattavia vahinkoja (Nyyssölä 2018, 116;139). Siksi Suomen tuleva tietosuojalain 29 § täsmentää, miten henkilötunnusta saa käsitellä (HE 9/2018 29 §). Käsittely on kuitenkin määritelty hyvin samalla tavalla kuin henkilötietolaissa (Hanninen ym. 2017, 44). Tilitoimiston näkökulmasta olennaista on, että henkilötunnuksen käsitteleminen on sallittua, kun rekisteröity antaa siihen suostumuksen tai rekisteröidyn yksilöiminen on tarpeellista rekisteröidyn tai rekisterinpitäjän oikeuksien ja velvollisuuksien toteuttamiseksi (Henkilötietolaki 22.4.1999/523 13 §; HE 9/2018 29 §). Vaikka käsittely saa perustua rekisteröidyn suostumukseen on kuitenkin suositeltavampaa perustella sitä yksilöimistarpeen takia. Tämä johtuu siitä, että jos perustetta henkilötunnuksen avulla yksilöimiselle rekisterinpitäjän tai rekisteröidyn oikeuksien ja velvollisuuksien näkökulmasta ei ole, on henkilötunnuksen käsittely usein tarpeetonta ja sitä voi olla vaikeaa perustella. (Hanninen ym. 2017, 46.)

4 KESKEISET MUUTOKSET TILITOIMISTOALALLA

4.1 Keskeisimmät käsitteet

Asetuksen 4:nnessä artiklassa käsitellään asetuksen määritelmiä, eli kerrotaan tarkemmin mitä käytetyillä termeillä asetuksessa tarkoitetaan. Määritelmät voivat aiheuttaa tulkintaongelmia, sillä asetus on ollut haasteellista kääntää suomenkielelle, kuitenkin Euroopan unionin oikeuden lähtökohtana on, että kaikki kieliversiot ovat yhtä päteviä. (Nyyssölä 2018, 42.) Yhteensä määritelmiä on 26 kappaletta (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 1.luku 4 artikla). Työssä on käyty läpi jo muutamia käsitteitä, joita uusi asetus pitää sisällään. Alla on vielä muutamia tärkeimpiä termejä tilitoimiston näkökulmasta. Ilman käsitteiden ymmärrystä on tietosuoja-asetuksen vaatimusten täyttäminen lähes mahdotonta (Hanninen ym. 2017, 18).

4.1.1 Rekisteröity ja henkilötieto

Rekisteröidyllä tarkoitetaan henkilöä, jonka henkilötietoja käsitellään (Eurooppa-neuvosto 2015). Henkilötietoja ovat kaikki rekisteröityyn liittyvät tiedot, joiden perusteella hänet voidaan tunnistaa tai hän on tunnistettavissa (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 1. luku 4. artiklan 1 asetus). Olennaista on, että tiedot liittyvät tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön, silloin hänestä käytetään nimitystä rekisteröity. Esimerkiksi tilitoimisto voi antaa toimeksiantajalleen raportin palkkatiedoista, missä palkkatietoja ei voida yhdistää tiettyyn henkilöön, rekisteröityyn. Tiedot eivät ole henkilötietoja vaan tietyn ihmisryhmän tietoja. Tilanne muuttuu, jos tilitoimisto jaottelee miesten ja naisten palkat erikseen ja työyhteisössä sattuu olemaan vain yksi nainen. Tällaisessa tapauksessa nainen voidaan palkkatiedon mukaan tunnistaa ja hänestä tulee rekisteröity, yleinen ihmisryhmän tieto on muuttunut henkilötiedoksi. (Nyyssölä 2018, 43-44.)

Henkilötietoja ovat muun muassa tunnistetiedot kuten nimi, sijainti tai vastaavasti tunnusomaiset piirteet kuten geneettinen, taloudellinen tai sosiaalinen tekijä. Henkilötietoja ovat siis kaikki sellaiset tiedot, joiden avulla luonnollinen henkilö voidaan tunnistaa suoraan tai epäsuorasti. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 1. luku 4. artiklan 1 asetus.) Äkkiseltään voitaisiin ajatella, että kaikki tiedot ovat henkilötietoja, näin ei kuitenkaan ole. Toisaalta henkilötietoja löytyy hyvin monesta ja ehkä yllättävistäkin paikoista. Esimerkiksi blogiteksti voi olla osa kirjoittajan henkilötietoa. (Kajander 2016.)

Henkilötietojen käsite on kuitenkin hyvin samanlailla määritelty kuin henkilötietolaissa 1999/523. Asetuksessa on vain hieman enemmän tarkennuksia sekä esimerkkejä. (Oikeusministeriö, Tietosuojavaltuutetun toimisto 2017.)

4.1.2 Henkilötietojen käsittely ja rekisteri

Henkilötietojen käsittelyllä tarkoitetaan toimintoja, joita tehdään henkilötietoihin tai niitä sisältävään tietojoukkoon. Toiminnot voivat olla manuaalisia tai automaattisia tietojenkäsittelyjä, esimerkiksi:

> — — *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* — — (*Euroopan parlamentin ja neuvoston asetus* (EU) 2016/679 1. luku 4. artiklan 2 asetus).

Käsite on hyvin laaja, se voidaan tulkita niin, että aina kun henkilötietoja käytetään jossain yhteydessä, on kyse niiden käsittelystä (Hanninen ym. 2017, 21). Nyyssölän (2018, 47) mukaan ongelmallista voi olla, kun samaa säännöstä sovelletaan myös henkilötietojen poistamiseen. Toisaalta sama ongelma oli jo Suomen henkilötietolaissa. Tietosuoja-setuksessa oleva henkilötietojen käsittelyn määritelmä ei siis eroa paljoakaan henkilötietolain määritelmästä.

Myös rekisterin käsite on verrattavissa henkilötietolain henkilörekisterin käsitteeseen. Asetuksen mukaan rekisteri on mikä tahansa tietojoukko, joka sisältää henkilötietoja (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 1. luku 4. artiklan 6 asetus). Se voi olla paperilla, sähköisesti Wordissa tai muistilapuilla kiinni näytössä. Rekisteri voi olla hajautettu tai jaettu ja siitä henkilötiedot ovat saatavilla tietyin perustein (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 1. luku 4. artiklan 6 asetus). Esimerkiksi henkilötiedot voivat olla järjestetty aakkosittain tai iän perusteella. Sillä ei ole väliä, miten rekisteri on toteutettu, vaan sillä tarkoitetaan samaa käyttötarkoitusta varten kerättyjä ja käytettäviä tietoja (Hanninen ym. 2017, 22). Jos henkilötietoja ei ole jäsennelty tietyllä tavalla, ne eivät muodosta rekisteriä (Nyyssölä 2018, 50). Tietosuoja-asetuksen pääpaino ei niinkään ole itse rekisteri vaan rekisterissä olevien henkilötietojen käyttötarkoitus (Hanninen ym. 2017, 22).

4.1.3 Rekisterinpitäjä ja henkilötietojen käsittelijä

Rekisterinpitäjä on luonnollinen henkilö, viranomainen tai elin, joka määrittelee henkilötietojen käsittelyn tarkoitukset ja siihen käytettävät keinot (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 1. luku 4. artiklan 7 asetus). Rekisterinpitäjään yhdessä henkilötietojen käsittelijän kanssa kohdistuu suurin osa tietosuoja-asetuksen velvoitteista (Hanninen ym. 2017, 22; Nyyssölä 2018, 51). Käytännössä rekisterinpitäjä on yritys, joka

määrittelee, miten henkilötietoja kerätään ja mihin tarkoitukseen niitä käytetään (Hanninen ym. 2017, 22). Vastaavasti henkilötietojen käsittelijällä tarkoitetaan:

> — — *luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, joka käsittelee henkilötietoja rekisterinpitäjän lukuun* — — (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 1. luku 4. artiklan 8 asetus).

Henkilötietojen käsittelijän käsitteessä Nyyssölän (2018, 56) mukaan olennaisinta on se, että tietoja käsitellään rekisterinpitäjän puolesta. Tämä tarkoittaa sitä, että automaattisesti alihankkijayrityksestä ei tule henkilötietojen käsittelijää, jos hän saa rekisterinpitäjältä henkilötietoja. Vastaavasti alihankkijasta voi tulla itsestään rekisterinpitäjä, jos hän kerää näitä tietoja omiin tarkoituksiinsa.

Rekisterinpitäjäksi voidaan siis ajatella tilitoimistoa, toisaalta monessa tapauksessa tilitoimisto on myös henkilötietojen käsittelijä. Tällainen tapaus syntyy esimerkiksi silloin, kun jokin yritys on ulkoistanut pelkän palkanlaskennan tilitoimistolle. Tällöin tilitoimisto ei hallinnoi varsinaisesti palkanlaskennan rekisteriä, vaan käyttää rekisterin tietoja apunaan. Henkilötietojen käsittelijä ei voi määritellä millä perustein henkilötietoja kerätään tai millä perustein niitä käytetään, vaan hän käsittelee rekisterinpitäjän henkilötietoja annettujen dokumentoitujen ohjeiden mukaisesti (Hanninen ym. 2017, 22).

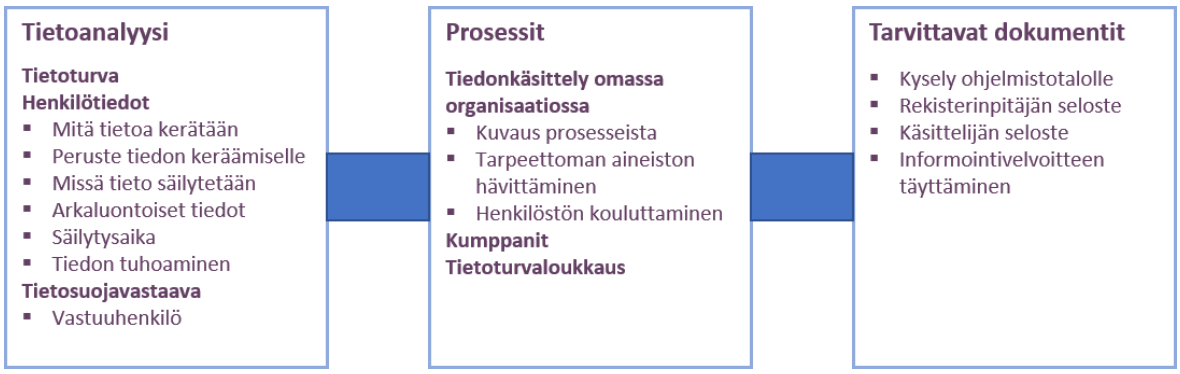
4.2 Keskeisimmät muutokset

Tietosuoja-asetus ei ole mikään täysin uusi asia eikä sen ole tarkoitus lopettaa henkilötietojen käsittelyä, vaikka rajat henkilötietojen käsittelylle tiukentuvatkin nykyisistä säännöistä. Nykyinen lainsäädäntökin on velvoittanut yrityksiä jo pitkään suojelemaan henkilötietoja, esimerkiksi henkilötietolaki vuodesta 1999 ja laki yksityisyyden suojasta työelämässä vuodesta 2004. (Haarma & Leppänen 2018, 4;10-11; Koivuniemi 2018.) Lisäksi on huomioitava, että vaikka henkilötietolaki poistuukin uuden kansallisen tietosuojalain myötä, ei vuonna 2004 annettu laki työelämän yksityisyyden suojasta ole poistumassa. Eli vielä toistaiseksi henkilötietolaki on myös voimassa (Koivuniemi 2018). Tätä on havainnollistettu enemmän kuviossa 2 (Kuvio 2, sivu 6). Hallinnollisen työn lisääntymiseen on hyvä varautua, sillä asetuksen myötä rekisterinpitäjiltä vaaditaan erilaisia dokumentteja ja prosessikuvauksia asetukseen liittyen (Hyppönen 2015).

Uusi asetus vaikuttaa kaikkiin tili- ja isännöintitoimistoihin, koska kummallakin alalla henkilötietojen käsittely on toiminnan kannalta välttämätöntä. Velvoite henkilötietojen keräämiselle tulee monessa asiassa suoraan laista. Myös muita perusteita henkilötietojen keräämiselle voi olla, mutta tilanne missä henkilötietoja ei tarvitsisi kerätä lainkaan, on mahdoton.

4.3 Käytännön toimenpiteet

Varatuomari Petri Holopainen (2018) on Yrittäjäsanomat-lehdessä listannut tärkeimmät käytännön asiat tietosuoja-asetukseen liittyen, joista yrittäjän tulisi huolehtia. Yrityksen tietoturvan on oltava kunnossa, henkilötietojen käsittelylle tulee olla peruste ja seloste käsittelytoimista on laadittava. On selvitettävä, täytyykö tehdä tietosuojaa koskeva vaikutusten arviointi, rekisteröityjen informoinnin toteutuminen on dokumentoitava ja käsittelyn ulkoistamisesta on laadittava sopimukset. (Lehtinen 2018, 8.) Kuviossa 5 on esimerkki tilitoimiston toimenpiteistä asetuksen vaatimusten täyttämiseksi.



Kuvio 5. Käytännön toimenpiteet tilitoimistossa

4.3.1 Tietoanalyysi

Tietoturva

Käytettävien järjestelmien tietosuoja on varmistettava. Asetus edellyttää järjestelmien ja palveluiden jatkuvaa luottamuksellisuutta ja vikasietoisuutta. Vikasietoisuudella tarkoitetaan, että hävinneet tai vioittuneet tiedot on pystyttävä palauttamaan nopeasti fyysisen tai teknisen vian sattuessa. Järjestelmiin liittyen on käytävä läpi tietojen välitys, liittymät ja järjestelmien sekä hakemistojen käyttöoikeudet. Tietojen säilyttämisen tietoturva täytyy myös varmistaa. Palkanlaskennassa käytettäviä järjestelmiä on muun muassa palkkaohjelma, työajanseurantajärjestelmä sekä arkistointijärjestelmä. Käytettävien järjestelmien teknisiä suojaustoimia ovat varmuuskopiointi, palomuuri, virusohjelmat, verkon salaus ja käyttäjäkohtaiset salasanat. (Männistö 2017, 21.) Kaikki tilitoimistossa käsiteltävä aineisto tulisi arkistoida yhtenäisellä tavalla toiminnan jatkuvuuden turvaamiseksi erityistilanteissa (Taloushallintoliitto 2018c). Kuviossa 6 (Kuvio 6, sivu 38) on kuvattu prosessia tietoturvan varmistamiseksi palkkahallinnossa.

Kuvio 6. Tietoturvan varmistaminen palkanlaskentaprosessissa

Hyppönen (2015) on Tilisanomien artikkelissa tuonut esille tietoturvallisuuden liiketoiminnalliset kytkökset sekä asiat mitkä vaativat kannanottoa, jotta henkilö- ja muita tietosuojalainalaisia tietoja koskeva tiedonhallinta saadaan järjestettyä lainsäädännön mukaisesti. Vaikka tietosuoja-asetus kohdistuu tietosuojaan, oletuksena on, että yrityksen tietoturva on myös riittävä. Yrityksen on pystyttävä varmistamaan toimintansa sekä normaali- että poikkeustilanteissa. Tietoturvallisuutta voidaan parantaa jo hyvin pienillä keinoilla. Omasta työhuoneesta poistuessa laitettaan näppäinlukko päälle ja paperit käännetään väärin päin, arkaluontoisia tietoja ei kuljeteta pois työpaikalta eikä henkilökohtaista sähköpostia käytetä työasioiden hoitamiseen.

Ilman tietoturvaa ei ole tietosuojaa (Suvanto 2018)!

Henkilötiedot

Henkilötietojen käsittely yrityksissä on jatkossa lainmukaista, jos vähintään yksi asetuksen määrittelemistä edellytyksistä täyttyy (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 2. luku 6. artiklan 1 asetus). Käsittelyn edellytykset on kuvattu tässä työssä taulukossa 4 (Taulukko 4, sivu 26). Tilitoimistossa käsitellään henkilötietoja erityisesti henkilöstö- ja palkkahallinnossa, mutta myös asiakasrekisteri tulee ottaa huomioon henkilötietojen käsittelyssä (Männistö 2017, 20). Rekisterit täytyy käydä läpi ja selvittää mitä henkilötietoja kerätään sekä missä ja miten henkilötietoja säilytetään. Säilytysaika on määriteltävä, koska tietoja saa säilyttää ainoastaan sen ajan, kun se on toiminnan kannalta tarpeen tai mitä laki edellyttää. Henkilötietojen keräämiselle täytyy olla EU:n tietosuoja-asetuksen (2016/679) 2. luvun 6:nnen artiklan mukainen peruste ja, jos aiemmin on kerätty

jotain muita tietoja, on ne tiedot hävitettävä. Varmuuden vuoksi ei henkilötietoja saa enää kerätä eikä säilyttää. Taulukossa 5 on kuvattu yleisimpiä tilitoimistoissa käytössä olevia tai mahdollisesti käytössä olevia rekistereitä, niiden käsittelyn oikeusperustetta sekä tiedon säilytysaikoja.

Taulukko 5. Henkilötiedot tilitoimistossa

Rekisterin tai rekisterin osan nimi	**Oikeusperuste**	**Tietojen säilytysaika**
Markkinointirekisteri	Oikeutettu etu	
Asiakasrekisteri	Oikeutettu etu	
Rahanpesulain vaatimat tuntemistiedot (osa asiakasrekisteriä)	Laki (Laki rahanpesun ja terrorismin rahoittamisen estämisestä 444/2017)	Viisi vuotta vakituisen asiakassuhteen päättymisestä (Laki rahanpesun ja terrorismin rahoittamisen estämisestä 444/2017 3. luku, 3 §)
Henkilörekisteri	Laki (Työaikalaki 9.8.1996/605) Laki (Kirjanpitolaki 30.12.1997/1336)	Työaika ja palkkakirjanpitoon kuuluvat työvuoroluettelot, työajan tasoittumisjärjestelmät ja palkkakortit on säilytettävä kanneajan päättymiseen asti, eli kaksi vuotta meneillään olevan vuoden jälkeen ja tämän lisäksi kaksi vuotta työsuhteen päättämisestä (Työaikalaki 9.8.1996/605 8. luku 1 §) Se henkilörekisteriin kuuluva aineisto mikä on osa liiketapahtumia koskevaa kirjeenvaihtoa, on säilytettävä vähintään kuusi vuotta sen vuoden lopusta, jonka aikana tilikausi on päättynyt (Kirjanpitolaki 30.12.1997/1336 2. luku 10 §). Se henkilörekisteriin kuuluva aineisto mikä on osa yrityksen kirjanpitoja (ns. palkanlaskennan päivä- ja pääkirja), on säilytettävä vähintään 10 vuotta tilikauden päättymisestä (Kirjanpitolaki 30.12.1997/1336 2. luku 10 §).
Kameravalvontarekisteri	Oikeutettu etu	Pääsääntöisesti hävitettävä heti, tai viimeistään vuoden kuluttua tallentamisen päättymisestä. Poikkeuksena tilanne, joissa säilyttämiselle on erityinen syy, esimerkiksi jos asia on selvittelyssä, voi tallenteita säilyttää selvittelyn ajan. (Nyyssölä 2018, 193.) Tästä säädetään myös laissa yksityisyyden suoja työelämässä (13.8.2004/759) 17§
Rekrytointirekisteri	Oikeutettu etu	Kanneajan päättymiseen asti eli kaksi vuotta (Koivuniemi 2018)
Osakasluettelo	Laki (Osakeyhtiölaki 21.7.2006/624 3.luku 15 §)	Ajantasaisena koko osakeyhtiön olemassaolon ajan

Taulukossa 5 (Taulukko 5, sivu 39) on rahanpesulain vaatimat tuntemistiedot esitetty erikseen, vaikka ovatkin osa asiakasrekisteriä. Uusi rahanpesulaki on astunut voimaan heinäkuussa 2017 ja uuden lain myötä Etelä-Suomen aluehallintovirasto on alkanut pitää rahanpesun valvontarekisteriä (Aluehallintovirasto 2017a). Etelä-Suomen Aluehallintovirasto (AVI) valvoo tahoja, jotka hoitavat kirjanpitotehtäviä toimeksiannosta. Tilitoimistot kuuluvat näihin ilmoitusvelvollisin ja ovatkin avainasemassa rahanpesun ja terrorismin rahoittamisen estämisessä ja selvittämisessä. (Aluehallintovirasto 2017b.) Laki edellyttää ilmoitusvelvollista tunnistamaan asiakkaansa ja todentamaan henkilöllisyys muun muassa vakituista asiakassuhdetta perustettaessa (Laki rahanpesun ja terrorismin rahoittamisen estämisestä 444/2017 3. luku 2 §). Tuntemista koskevat tiedot on säilytettävä luotettavasti viiden vuoden ajan vakituisen asiakassuhteen päätyttyä. Jos kyse on muusta rahanpesulaissa tarkoitetusta satunnaisesta liiketoimesta, on tiedot säilytettävä luotettavasti viiden vuoden ajan liiketoimen suorittamisesta. Tunnistamistietoja, jotka on hankittu ainoastaan rahanpesun tai terrorismin rahoittamisen estämiseksi ja paljastamiseksi, ei saa käyttää muuhun tarkoitukseen. Asiakkaalle on myös ilmoitettava, että hänen tunnistamistietojaan voidaan käyttää vain tässä laissa mainittuun tarkoitukseen. (Laki rahanpesun ja terrorismin rahoittamisen estämisestä 444/2017 2. luku 3 §.)

Jos tilitoimisto hoitaa asunto-osakeyhtiöiden kirjanpitoa ja näin ollen ehkä myös isännöintiä, on taulukossa 5 (Taulukko 5, sivu 39) kuvattujen henkilötietojen lisäksi huomioitava taloyhtiöiden rekisterit. Isännöintiyritys on henkilötietojen käsittelijän roolissa asunto-osakeyhtiön pitämissä rekistereissä (Haarma & Leppänen 2018, 28). Pelkästään isännöintiä harjoittavien toimistojen ei tarvitse kerätä tuntemistietoja koskien lakia rahanpesusta ja terrorismin rahoittamisen estämisestä. Taulukossa 6 (Taulukko 6, sivu 41) on kuvattu asunto-osakeyhtiöiden keräämien tavanomaisimpien rekisterin käsittelyn lainmukaisuutta ja tietojen säilytysaikoja.

Taulukko 6 Taloyhtiön rekisterit

Rekisterin nimi	**Oikeusperuste**	**Tietojen säilytysaika**
Osakeluettelo	Laki (Asunto-osakeyhtiölaki 22.12.2009/1599)	Ajantasaisena koko asunto-osakeyhtiön olemassaolon ajan (Asunto-osakeyhtiölaki 22.12.2009/1599 toinen luku 12 §) Osakkeen aiempaa omistajaa koskevat tiedot on säilytettävä 10 vuotta siitä, kun uusi omistaja on merkitty osakeluetteloon (Asunto-osakeyhtiölaki 22.12.2009/1599 toinen luku 14 §)
Kunnossapito- ja muutostyöilmoitusrekisteri	Laki (Asunto-osakeyhtiölaki 22.12.2009/1599)	Koko asunto-osakeyhtiön olemassaolon ajan (Asunto-osakeyhtiölaki 22.12.2009/1599 seitsemäs luku 28 §)
Kamera- ja kulunvalvonta	Oikeutettu etu	Pääsääntöisesti hävitettävä heti, tai viimeistään vuoden kuluttua tallentamisen päättymisestä. Poikkeuksena tilanne, joissa säilyttämiselle on erityinen syy, esimerkiksi jos asia on selvittelyssä, voi tallenteita säilyttää selvittelyn ajan. (Nyyssölä 2018, 193.) Tästä säädetään myös laissa yksityisyyden suojasta työelämässä (13.8.2004/759) 17 §.
Asukasluettelo	Oikeutettu etu	Säilytysajan tulee olla mahdollisimman lyhyt. Tietoja voi säilyttää asukassuhteen keston ajan, jonka jälkeen niitä voidaan säilyttää, jos henkilötiedot ovat tarpeellisia esimerkiksi laskutuksen, perinnän tai oikeudellisten toimenpiteiden takia. (Kiinteistöliitto 2018.)
Luettelo hallituksen jäsenistä	Oikeutettu etu	
Luettelo tili- ja toiminnantarkastajista	Oikeutettu etu	

Tietosuojavastaava

Tietosuoja-asetus ei yleensä edellytä tietosuojavastaavan nimittämistä tili- ja isännöintitoimistoissa. Yrityksen on kuitenkin hyvä nimetä yksi tai useampi henkilö, joka ottaa vastuun asetuksen vaatimien muutosten toteuttamisessa. Asetus tulee varmasti aiheuttaman paljon kysymyksiä niin yrityksen sisällä henkilöstössä kuin asiakkaissakin. Vastaavan tiimin tai henkilön vastuuttaminen tietosuoja-asioissa isännöintiyrityksillä on edellytys hyvälle tietosuojakäytännölle (Haarma & Leppänen 2018, 35).

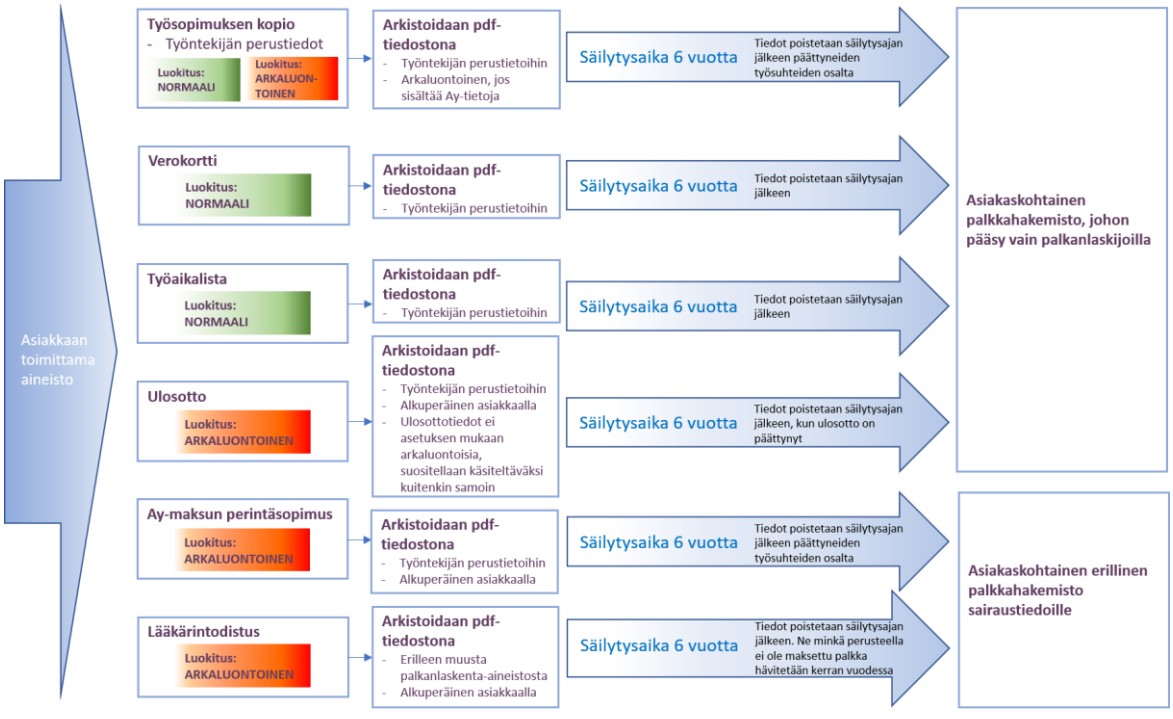
4.3.2 Prosessit

Tiedonkäsittely omassa organisaatiossa

Rekisterinpitäjällä on asetuksen mukaan osoitusvelvollisuus asetuksen noudattamisesta. Osoitusvelvollisuuden voi täyttää kuvaamalla kartoitetut prosessit ja suunnittelemalla suojatoimenpiteet. Prosesseja kuvatessa on huomioitava seuraavat asiat: aineiston

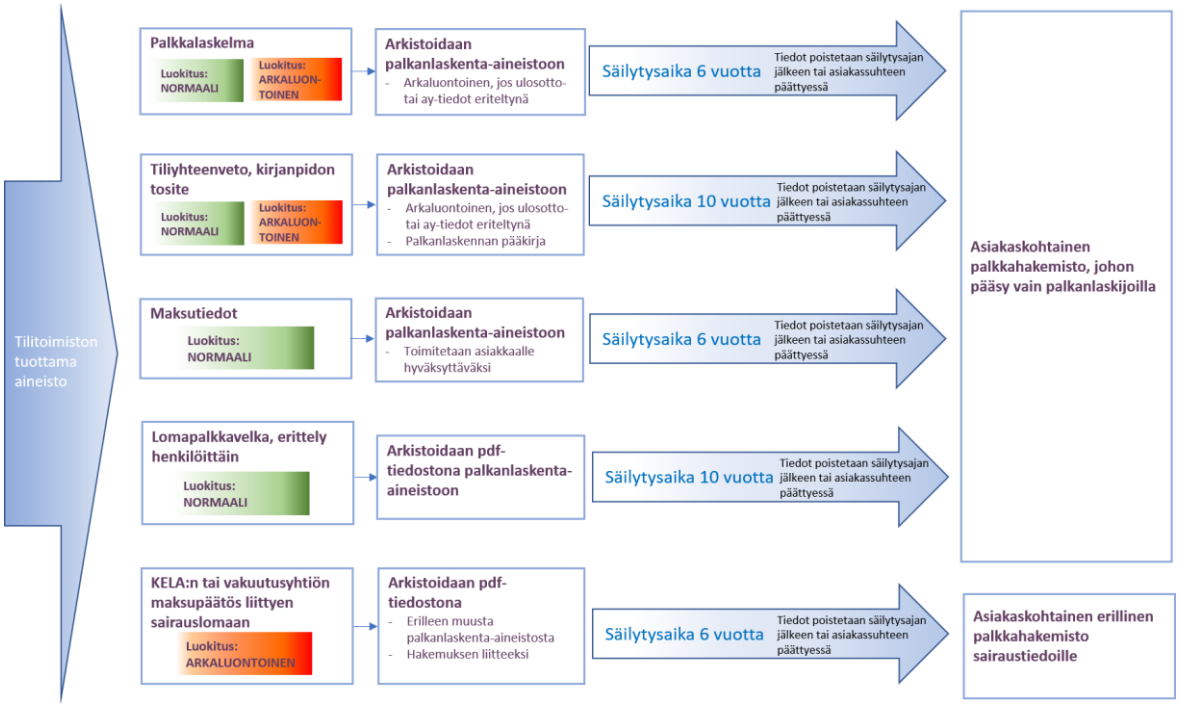
yksilöiminen, aineiston vastaanottotapa, käsiteltävän tiedon luokitus, tietojen käsittelytapa, tietojen säilytystapa ja muoto, sekä tietojen säilytysaika että miten tiedot hävitetään. (Männistö 2017, 20-21.) Henkilöstöhallinnon ja palkanlaskennan osalta tilitoimiston asiakkaan olisi kuvattava omat henkilötietojen käsittelyprosessit. Jos tilitoimiston asiakas, rekisterinpitäjä, tilaa palkanlaskentapalvelun tilitoimistolta, henkilötietojen käsittelijältä, on asiakkaan varmistettava, että tilitoimisto toteuttaa EU:n tietosuoja-asetuksen (2016/679) 4. luvun 28:nnessa artiklassa mainitut riittävät suojatoimet. Tietojen käsittely perustuu asiakasyrityksen ohjeistukseen henkilötietojen käsittelytavoista (Männistö 2017, 21). Tilitoimiston täytyy omassa palkanlaskennan prosessikuvauksessa käydä läpi koko prosessi siitä alkaen, kun asiakas toimittaa keräämiänsä henkilötietoja tilitoimistolle.

Kuviossa 7 on esimerkki asiakkaan palkanlaskentaa varten tilitoimistolle toimittaman aineiston käsittelyprosessista. Aineisto käsitellään sähköisesti ja kuvio lähtee siitä oletuksesta, että koko aineisto toimitetaan sähköpostilla tilitoimistolle. Jos käytössä ei ole salattua sähköpostia, on arkaluontoisen materiaalin toimittamiselle sovittava jokin toinen, suojattu tapa. Kuviossa tietojen poistamistapaa ei ole mainittu erikseen, mutta kaikki tiedot poistetaan säilytysajan päätyttyä tiedostokansio kerrallaan. Tilitoimisto arkistoi aineiston lain edellyttämällä tavalla ja huomioi poistamisajat niin kauan, kun asiakassuhde on voimassa. Asiakassuhteen päättyessä aineisto luovutetaan asiakkaalle säilytettäväksi, jolloin asiakas huomio tietosuoja-asetuksen vaatimat poistamisajat.



Kuvio 7. Esimerkki prosessikuvauksesta, asiakkaan toimittama aineisto

Tilitoimiston palkanlaskentaprosessia on kuvattu kuviossa 8. Esimerkissä kaikki palkanlaskennasta saatu aineisto arkistoidaan sähköisesti. Tässä esimerkissä, kuten ei edellisessäkään, tietojen poistamistapaa ei ole mainittu erikseen, mutta kaikki tiedot poistetaan säilytysajan päätyttyä tiedostokansio kerrallaan. Tilitoimisto arkistoi aineiston lain edellyttämällä tavalla ja huomioi poistamisajat niin kauan, kun asiakassuhde on voimassa. Asiakassuhteen päättyessä aineisto luovutetaan asiakkaalle säilytettäväksi, jolloin asiakas huomio tietosuoja-asetuksen vaatimat poistamisajat.

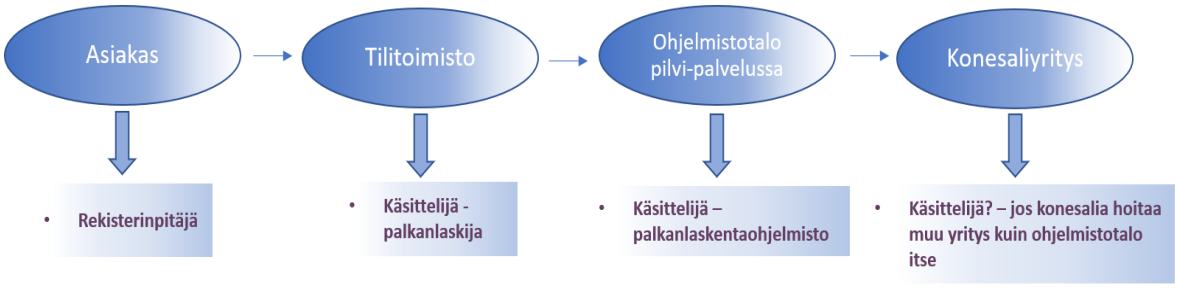


Kuvio 8. Esimerkki prosessikuvauksesta, palkanlaskennan aineisto

Henkilötietoja käsittelevien henkilöiden on asetuksen mukaan oltava sitoutuneita noudattamaan salassapitovelvollisuutta. Yrityksen on koulutettava henkilökuntaa toimintaohjeista koskien yrityksen tietoturvaa ja tietosuoja-asetusta. Toimenkuvat ja käyttöoikeudet on hyvä käydä läpi jokaisen työntekijän kohdalta. (Männistö 2017, 21.)

Kumppanit

Tietosuoja-asetuksen myötä tilitoimistolle tulee velvoitteita myös omien alihankkijoiden ja ohjelmistokumppaneiden osalta (Fredman 2018c). Taloushallintoliiton (2018b, 2) laatimassa sopimusliitteessä, Sopimus henkilötietojen käsittelystä TAL 2018, on määritelty, että kaikki, jotka käsittelevät henkilötietoja kokonaan tai osittain käsittelijän lukuun ovat alihankkijoita. Pelkästään se, että alihankkijan työntekijällä on mahdollisuus nähdä asiakkaan henkilötietoja, on käsittelyä (Fredman 2018c). Kuviossa 9 (Kuvio 9, sivu 44) on kuvattu alihankintaketju, kun palkanlaskenta toteutetaan pilvipalvelussa.



Kuvio 9. Alihankkijoiden käyttö pilvipalvelussa, mukaillen (Fredman 2018a)

Sopimus henkilötietojen käsittelystä TAL 2018 -liitteellä on määritelty, että tilitoimistolla on lupa käyttää henkilötietoja kyseisen sopimuksen perusteella. Asiakkaan pyynnöstä kuitenkin alihankkijat on ilmoitettava sopimuksen alkaessa. (Taloushallintoliitto 2018b, 3.) Tilitoimiston täytyy tehdä kirjallinen sopimus käyttämiensä alihankkijoiden kanssa (Fredman 2018c). Alihankkijoita voivat ohjelmistotalon ja konesaliyrityksen lisäksi olla muun muassa arkistontuhoamispalveluja tarjoava yritys tai jokin muu ulkoistettu ICT-palvelu sekä rekrytointikumppanit. Jos tilitoimisto hoitaa asunto-osakeyhtiöiden kirjanpitoja ja isännöintiä, voi tällöin alihankkijana olla muun muassa ulkoistettu tekninen isännöinti.

Tietoturvaloukkaus

Tietoturvaloukkauksesta on kyse, kun henkilötietoja häviää tai niihin pääsee käsiksi taho, jolla ei ole tietoihin käsittelyoikeutta. Tietoturvaloukkauksia voi olla muun muassa hävinnyt tai varastettu tietokone tai USB-tikku, hakkerointi ja haittaohjelmatartunta sekä tulipalo datakeskuksessa. Kaikki henkilötietojen tietoturvaloukkaukset on dokumentoitava. Jos tietoturvaloukkauksesta aiheutuu riski luonnollisen henkilön oikeuksille ja vapauksille, on siitä tehtävä ilmoitus valvontaviranomaiselle 72 tunnin kuluessa. Ilmoituksen määräaika katsotaan alkaneeksi sitä hetkestä, kun rekisterinpitäjä on tullut tietoiseksi tapahtuneesta. Jos on todennäköistä, että tietoturvaloukkauksesta aiheutuu korkea riski rekisteröidyn oikeuksille ja vapauksille, on rekisterinpitäjän ilmoitettava loukkauksesta rekisteröidylle ilman aiheetonta viivytystä. (Tietosuojavaltuutetun toimisto 2018c.) Tilitoimiston on hyvä miettiä valmiiksi toimintatapa tilanteessa, kun tietoturvaloukkaus on tapahtunut. Kuviossa 10 (Kuvio 10, sivu 45) kuvattu tilitoimiston prosessia, kun tietoturvaloukkaus on tapahtunut. Tilitoimisto toimii sekä rekisterinpitäjänä että asiakkaiden henkilötietojen käsittelijänä, joten myös asiakkaiden kanssa on tärkeä sopia selkeästi, miten tietoturvaloukkaus-tilanteessa toimitaan. Taloushallinto on huomioinut tämän Sopimus henkilötietojen käsittelystä TAL 2018 -sopimuksella.

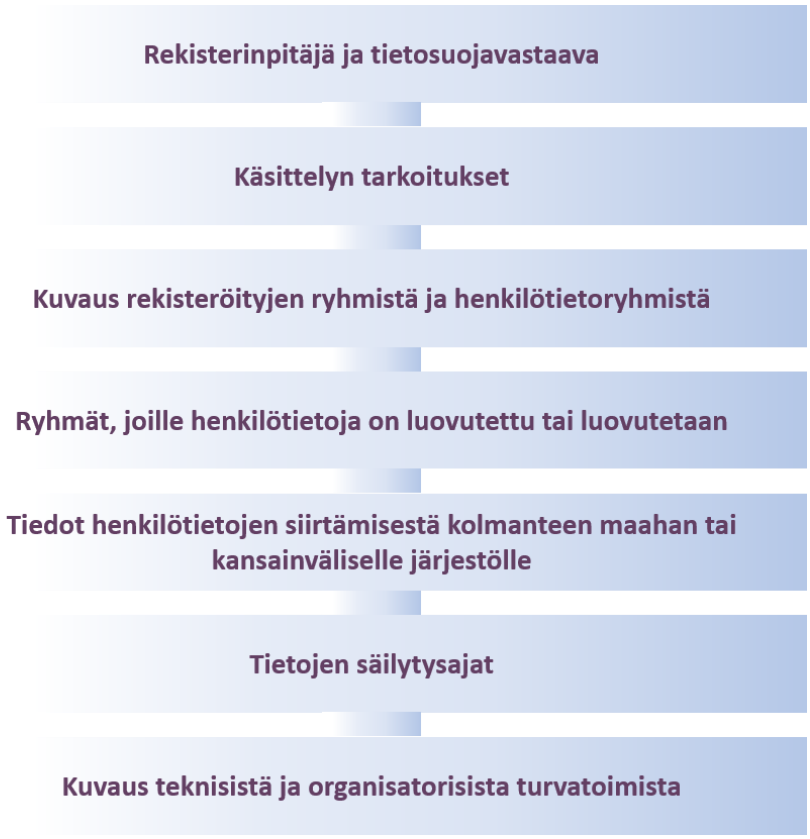
> *Tilitoimiston on ilmoitettava henkilötietojen tietoturvaloukkauksesta asiakkaalle ilman aiheetonta viivytystä siitä, kun tilitoimisto tai sen käyttämä alihankkija on saanut loukkauksen tietoonsa. Elleivät toiset osapuolet ole toisin sopineet, ilmoitus tulee tehdä asiakkaan ilmoittamalle yhteyshenkilölle.* (Taloushallintoliitto 2018b.)

Kuvio 10. Prosessi tietoturvaloukkauksen tapahtuessa

4.3.3 Tarvittavat dokumentit

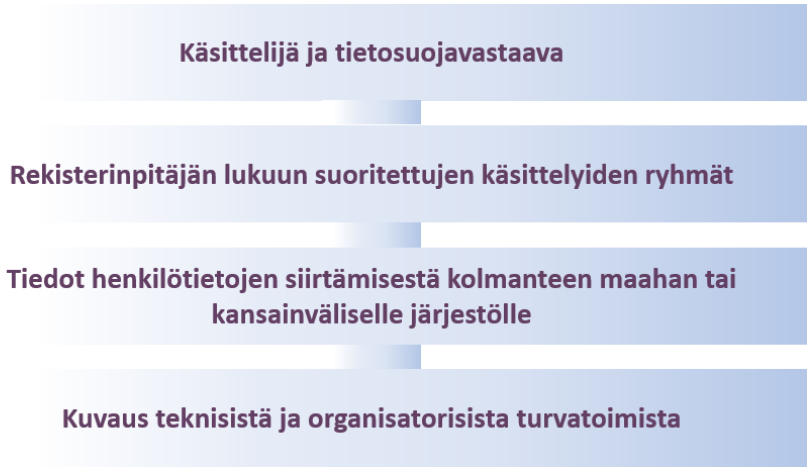
Kun käsiteltävät tiedot ja tilitoimiston prosessit on käyty läpi, on tilitoimiston laadittava vielä erilaisia dokumentteja osoittaakseen noudattavansa tietosuojasäädöksiä (Tietosuojavaltuutetun toimisto 2018d). Jos esimerkiksi palkanlaskentaohjelmiston palvelinten ylläpito on ulkoistettu, on tilitoimiston varmistettava, että ohjelmistotalo on huomioinut tietoturvan ja tietosuoja-setuksen vaatimukset toiminnassaan. Ohjelmistotaloille on lähetettävä kysely tietosuojan tilasta, jollei ohjelmistotalot ole oma-aloitteisesti tiedottaneet asiasta. (Taloushallintoliitto 2018d.)

Tilitoimiston on omaan sisäiseen käyttöön laadittava rekisterinpitäjän seloste käsittelytoimista. Seloste on olennainen osa organisaation osoitusvelvollisuuden toteuttamista ja on pyydettäessä toimitettava valvontaviranomaiselle. (Tietosuojavaltuutetun toimisto 2018e.) Selosteiden ei ole pakko olla tietyllä kaavalla tehtyjä vaan voivat olla vapaamuotoisia infoja (Koivuniemi 2018). Tämä voi hankaloittaa asiaa, kun tarjolla ei ole täysin valmista kaavaketta tietojen täyttämiseksi. Tietosuojavaltuutetun toimiston (2018f) verkkosivuilta löytyy tietosisältö, mitä selosteessa täytyy olla sekä mallipohja rekisterinpitäjälle selosteen laatimista varten. Kuviossa 11 (Kuvio 11, sivu 46) on havainnollistettu rekisterinpitäjän laatiman selosteen tietosisältöä Tietosuojavaltuutetun toimiston ohjeen mukaan.



Kuvio 11. Rekisterinpitäjän selosteen tietosisältö (Tietosuojavaltuutetun toimisto 2018f)

Henkilötietojen käsittelijä, joka käsittelee henkilötietoja rekisterinpitäjän lukuun, on laadittava oma selosteensa henkilötietojen käsittelystä (Tietosuojavaltuutetun toimisto 2018g). Tilitoimisto toimii henkilötietojen käsittelijänä asiakkaiden keräämiin henkilötietoihin esimerkiksi palkanlaskennan yhteydessä. Kuviossa 12 on havainnollistettu rekisterinpitäjän laatiman selosteen tietosisältöä Tietosuojavaltuutetun toimiston ohjeen mukaan.



Kuvio 12. Henkilötietojen käsittelijän selosteen tietosisältö (Tietosuojavaltuutetun toimisto 2018g)

Kaikkien rekisterinpitäjien on täytynyt päivittää informointikäytäntönsä vastaamaan tietosuoja-asetuksen vaatimuksia (Tietosuojavaltuutetun toimisto 2018h). Taloyhtiöissä asukkaiden informointivelvoitteen voi täyttää tietosuojaselosteella, mikä on ymmärrettävässä muodossa esitettävä selostus henkilötietojen käsittelystä. Tieto tulee olla helposti nähtävillä ja se voikin olla esillä esimerkiksi taloyhtiön verkkosivuilla. (Kiinteistöliitto 2018.) Myös tilitoimistoissa voidaan laatia vastaavanlainen tietosuojaseloste rekisteröityjen informoimiseksi sekä ohjeistaa asiakkaita laatimaan oma tietosuojaseloste.

4.3.4 Sopimusuudistukset

Tietosuoja-asetuksen voimaantulon myötä asiakkaan ja tilitoimiston on jatkossa aina tehtävä kirjallinen toimeksiantosopimus, mikäli tilitoimisto käsittelee asiakkaan puolesta henkilötietoja. Käsiteltäviä henkilötietoja voi olla, jos tilitoimisto hoitaa esimerkiksi palkanlaskentaa, yhdistyksen jäsenmaksulaskutusta tai asunto-osakeyhtiöiden kirjanpitoja. (Fredman 2018c.) Ennen yritys ja palkanlaskentaa hoitava tilitoimisto ovat voineet vapaasti sopia, mistä asioista heidän välillään sovitaan (Nyyssölä 2018, 56). Nykyään tietosuoja-asetus määrää mistä asioita on asiakasyrityksen ja palkanlaskijan välillä sovittava.

Tilitoimiston ja asiakkaan välisellä sopimuksella on sovittava käsittelyn kohde ja kesto, käsittelyn luonne ja tarkoitus, henkilötietojen tyyppi ja rekisteröityjen ryhmät sekä rekisterinpitäjän velvollisuudet ja oikeudet. Toimeksiantosopimuksella tai muulla erillisellä kirjallisella asiakirjalla on sovittava, että tilitoimisto saa käsitellä henkilötietoja ainoastaan rekisterinpitäjän antamien dokumentoitujen kirjallisten ohjeiden mukaan. Kirjallisesti on myös sovittava, että tilitoimisto varmistaa, että henkilöt (tilitoimiston sekä alihankkijoiden henkilöstö), joilla on oikeus käsitellä henkilötietoja, ovat sitoutuneet noudattamaan salassapitovelvollisuutta. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 4.luku 28. artiklan 3 asetus.)

Kirjallisessa sopimuksessa tai muussa oikeudellisessa asiakirjassa tilitoimiston täytyy sitoutua noudattamaan asetuksen artiklassa 32 luetellut käsittelyn turvallisuutta koskevat vaatimukset (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 4.luku 28. artiklan 3 asetus). Rekisterinpitäjä saa käyttää ainoastaan sellaisia henkilötietojen käsittelijöitä, jotka toteuttavat riittävät suojatoimet asianmukaisten teknisten ja organisatoristen toimien täytäntöönpanemiseksi. Tämän asetuksen vaatimukset täyttämällä varmistetaan rekisteröidyn oikeuksien suojelu. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 4.luku 28. artiklan 1 asetus.)

Yllämainittujen vaatimusten täyttäminen on tilitoimiston kannalta raskasta ja ne voivat tuntua jopa kohtuuttomilta. Kuitenkin on otettava huomioon, että esimerkiksi

palkanlaskennassa käsitellään hyvin arkaluontoisia tietoja. Taloushallintoliitto on TAL-sopimuksia uudistaessaan ottanut kantaa lisääntyneiden velvoitteiden toteuttamisen laskuttamisesta asiakkaalta. (Fredman 2018c.) Näin ollen kaikki kustannukset asetuksen lisäämistä vaatimuksista eivät jää yksin tilitoimiston kannettavaksi vaan sopimuksella on selkeästi huomioitu myös asiakkaan osallistuminen kustannuksiin.

> *Tilitoimistolla on oikeus laskuttaa yllä kuvatuista avustamis-, korjaamis- ja pyyntöihin vastaamistoimista, auditoinnin tuesta sekä asiakkaan ohjeistuksen muutoksista johtuvista toimista ja kustannuksistaan erikseen* (Taloushallintoliitto 2018b, 2)*.*

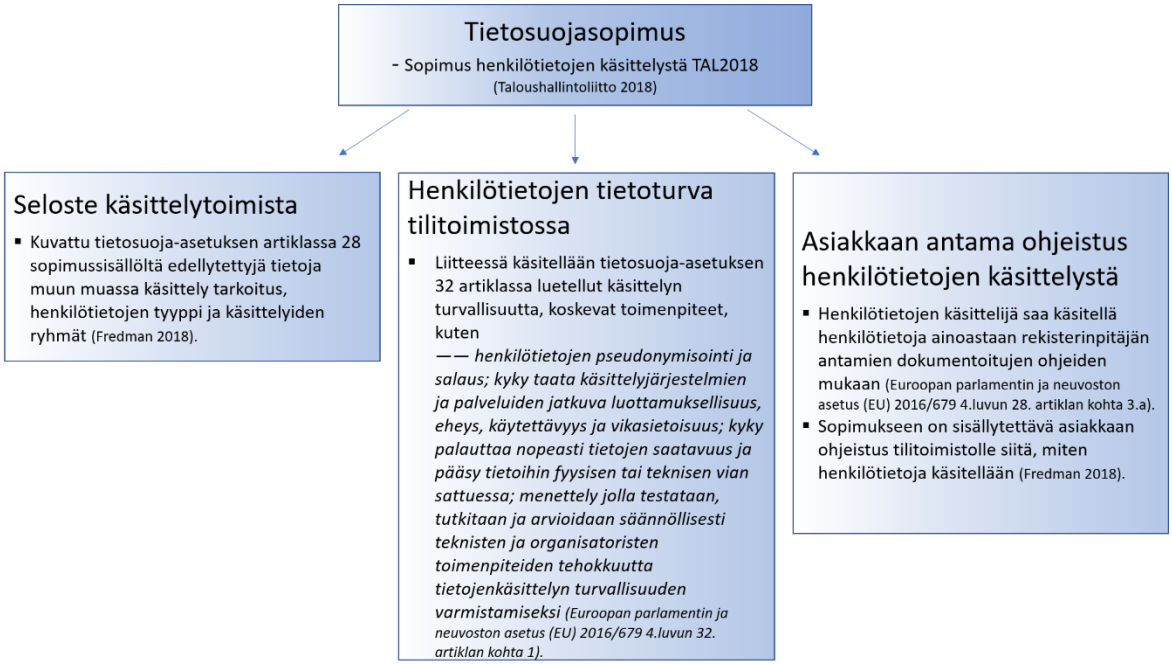
Useassa pienemmässä tilitoimistossa saattaa olla paljon vanhoja asiakkaita, joiden kanssa ei kirjallista sopimusta ole koskaan tehty. Mahdollisesti kirjanpidon yhteydessä ei alun perin ole käsitelty edes muita kuin itse yrittäjän omia henkilötietoja. Vuosien varrella toiminnan kasvaessa asiakkaan yritys on saattanut laajentua. Yhtiömuoto on vaihtunut osakeyhtiöksi, osakkaita on tullut lisää ja yhtiö on palkannut henkilökuntaa. Näin ollen tilitoimisto onkin saattanut jo vuosia käsitellä asiakkaan puolesta henkilötietoja muun muassa palkanlaskennan ja osakerekisterin osalta. Uuteen tietosuoja-asetukseen on kunnolla herätty vasta keväällä 2018. Yrityksillä on iso työ uudistaa kaikki sopimuksensa vastaamaan asetuksen vaatimuksia, varsinkin jos kirjallisia sopimuksia ei ole koskaan laadittukaan. Haasteita tilitoimistolle tuo myös se, että asiakkaat saataisiin ymmärtämään asetuksen merkityksen tärkeys. Vaikka taloushallintoliitto on huomioinut sopimusehtojaan uudistaessa velvoitteiden toteuttamisen laskuttamisen asiakkailta, voi käytännön toteutus olla hankalampaa nimenomaan pienempien asiakkaiden kohdalla.

Koko sopimuspakettia ei ole tarvinnut kevään aikana kuitenkaan uusia, vaan sopimuksia on ollut mahdollista päivittää vaiheittain. Aiemmin laadittuihin sopimuksiin on voinut tehdä päivitykset henkilötietojen käsittelyn osalta. Fredmanin (2018c) mukaan tietosuojasopimuksen tekemisestä ei voida tinkiä, kun toimitaan lakia noudattaen. Kuviossa 13 (Kuvio 13, sivu 49) on kuvattu Taloushallintoliiton TAL2018-sopimuksiin kuuluva tietosuojasopimus liitteineen.

Taloushallintoliiton TAL-sopimukset

Taloushallintoliitto on huomioinut asetuksen vaatimukset TAL-sopimuksia uudistaessaan. Entiset KL2004-sopimukseen kuuluneet henkilötietojen käsittelyn erityisehdot on korvattu tietosuojasopimuksella, jossa luetellaan kaikki asetuksen sekä asiakkaalle että tilitoimistolle asettamat velvollisuudet. Tietosuojasopimukseen sisältyy kolme liitettä: Seloste käsittelytoimista, Henkilötietojen tietoturva tilitoimistossa ja Asiakkaan antama ohjeistus henkilötietojen käsittelystä. (Fredman 2018c.) Kuviossa 13 (Kuvio 13, sivu 49) on kuvattu

Fredmanin (2018c) artikkelin ja EU:n tietosuoja-asetuksen (2016/679) artiklojen 28 ja 32 pohjalta tietosuojasopimuksen sopimusliitteiden sisältöä.



Kuvio 13. Tietosuojasopimus, sekä sopimuksen kolme liitettä

4.4 Tulkintaongelmia

Koska GDPR-uudistus on vielä aika tuore asia, voi asetuksen tulkitseminen olla vielä vähän hakusessa. Vuoden 2018 helmikuussa Kiinteistöliiton apulaispäälakimies Kristel Pynnönen (2018) pohti muodostaako porraskäytävien nimitaulut henkilörekisterin ja täytyisikö nimitaulut poistaa tietosuoja-asetuksen voimaantullessa. Pynnösen mukaan etenkin harvinainen nimi on henkilötieto. Muualla Euroopan maissa ei ole nimitauluja ja tämän takia pohdittiin, pitäisikö niistä luopua Suomessakin. (Manninen, 2018.) Tietosuojavaltuutettu Reijo Aarnion (2018) mukaan nimikylttien pitämiselle on peruste eikä EU-asetus tule poistamaan niiden hyväksyttävyyttä. Aarnion mielestä Pynnösen tulkinta oli myöskin ennenaikaisesti esitetty, koska tuolloin ei vielä ollut riittävästi tietoa Suomen omasta lainsäädännöstä ja siitä, miten se tulee muuttumaan asetuksen myötä. (Blencowe, 2018.)

> *Viranomaisten kantojen mukaan nimitaulu ei muodosta itsenäistä henkilörekisteriä. Nimitaulun käsittelyperuste on hallinnon hoitoon liittyvä oikeutettu etu. Osassa kuntia velvoite nimitaulun pitämiseen kiinteistön rappukäytävässä perustuu myös rakennusjärjestyksen määräyksiin eli tietojen käsittelylle on lakisääteinen peruste.* (Kiinteistöliitto 2018.)

Toisaalta, jos asukas itse haluaa ja pyytää nimensä poistamista nimitaulusta on se poistettava, jollei rekisteriselosteessa ole mainintaa ja laillista perustetta sen säilyttämiseksi (Koivuniemi 2018).

Taloushallintoliiton johtavan asiantuntijan Fredmanin (2018b, 46) mukaan tietosuoja-asetuksen tulkinnassa on näkynyt ylilyöntejä. Palkanlaskennan kirjanpitoaineiston kanssa on tehty tulkintoja, ettei tilintarkastajalla olisi oikeutta, etenkään erityisiä henkilötietoryhmiä, koskeviin tietoihin. Tilintarkastajalla on kuitenkin oltava pääsy tarkastamaan koko palkkaprosessi ja henkilöstökulujen aukoton kirjausketju, vaikka harvemmin lääkärintodistuksia on tarpeen tutkia.

> *Kaikki henkilötiedot, jotka pitää julkaista, saa julkaista* (Fredman 2018b, 47).

Kiinteistöliiton (2018) Usein kysytyt kysymykset -palstalla on otettu kantaa toimintakertomuksessa esitettyihin henkilötietoihin.

> *Osakesiirrot on hyvä mainita huoneiston tunnistetietojen perusteella ilman myyjän ja ostajan nimiä. Myöskään vastikerästeissä ei pidä mainita osakkaiden nimiä, vaan ainoastaan millä huoneistolla rästejä on.* (Kiinteistöliitto 2018.)

5 TUTKIMUKSEN TOTEUTUS JA TULOKSET

5.1 Tutkimuksen toteutus

Tutkimukseen valittiin haastattelumenetelmäksi puolistrukturoitu haastattelu, jossa kysymykset ovat valmiiksi mietittyjä, mutta kysymysten järjestystä on mahdollista vaihdella (Hirsjärvi & Hurme 2001, Saaranen-Kauppinen & Puusniekan 2006 mukaan). Haastattelut toteutettiin pääsääntöisesti puhelimitse ja kasvotusten. Kaksi haastateltavaa vastasivat ennalta saatuihin kysymyksiin kirjallisesti. Haastattelut toteutettiin kahdessa osassa. Ensimmäinen osa ennen asetuksen siirtymäajan päättymistä ja toinen osa siirtymäajan päättymisen jälkeen, viisi kuukautta myöhemmin. Yhteensä haastatteluja tehtiin 14 kappaletta. Molemmissa osissa haastateltiin seitsemää henkilöä. Haastattelut oli suunniteltu 15 – 20 minuutin mittaisiksi. Kummassakin osassa toteutuneiden haastattelujen kestot vaihtelivat hyvin laajasti 7 minuutista 38 minuuttiin.

Ensimmäiseen osaan valittiin haastateltaviksi pieniä yksityisyrittäjiä eri aloilta ja pieniä tilitoimistoyrittäjiä sekä muutamia isompien yritysten asiantuntijoita, jotka ovat olleet toteuttamassa asetuksen vaatimuksia omassa yrityksessään. Haastattelut suoritettiin 9.4.2018 – 2.5.2018. Toiseen osaan valittiin yrittäjiä sekä kirjanpitäjiä tili- ja isännöintitoimistoista sekä muuten työtehtävässään asiaan perehtynyttä talousjohtajaa sekä ohjelmistotalon toimitusjohtajaa. Toisen osan haastattelut suoritettiin 22.10.2018 - 9.11.2018. Haastateltavista ei selvitetty tarkempia taustatietoja, koska niiden ei katsottu olleen olennaisia tutkimuksen kannalta. Aiheen todettiin olevan kaikille yhtä uusi, riippumatta haastateltavien koulutus- tai työtaustasta. Kumpaankin osaan on haastateltu yhtä samaa tilitoimistoyrittäjää. Tutkimusosien kysymykset poikkeavat osittain toisistaan; toisessa tutkimusosassa kysymyksiä oli enemmän. Ensimmäisestä tutkimusosasta kävi ilmi, että asetuksen vaatimat käytännön toimenpiteet olivat vielä kesken ja ne oli tarkoitus saattaa valmiiksi ajallaan. Tämän vuoksi toiseen tutkimusosaan tuli täydentäviä lisäkysymyksiä koskien asteuksen vaatimien muutosten valmistumista.

Haastattelut litteroitiin, eli kirjoitettiin puhtaaksi, puhekielen mukaisesti riittävällä tarkkuudella. Tässä riittävällä tarkkuudella tarkoittaa sitä, että mielipiteet tulevat hyvin esille, mutta sanasta sanaan litterointi ei olisit tuonut työlle lisäarvoa. Tämän jälkeen vastaukset koottiin pääkohdat tiivistäen taulukkomuotoon. Osa haastatelluista haluisivat pysyä anonyymeinä, jonka takia haastateltavat nimettiin tunnisteella. Ensimmäisenä haastateltu nimettiin H1, seuraava H2 ja niin edelleen. Ensimmäinen tutkimusosa koostuu ensimmäisen osan haastatteluista ja toinen tutkimusosa koostuu toisen osan haastatteluista.

Tutkimustulokset perustuvat vastaajien kokemuksiin tietosuoja-asetuksesta ja sen aiheuttamista muutoksista.

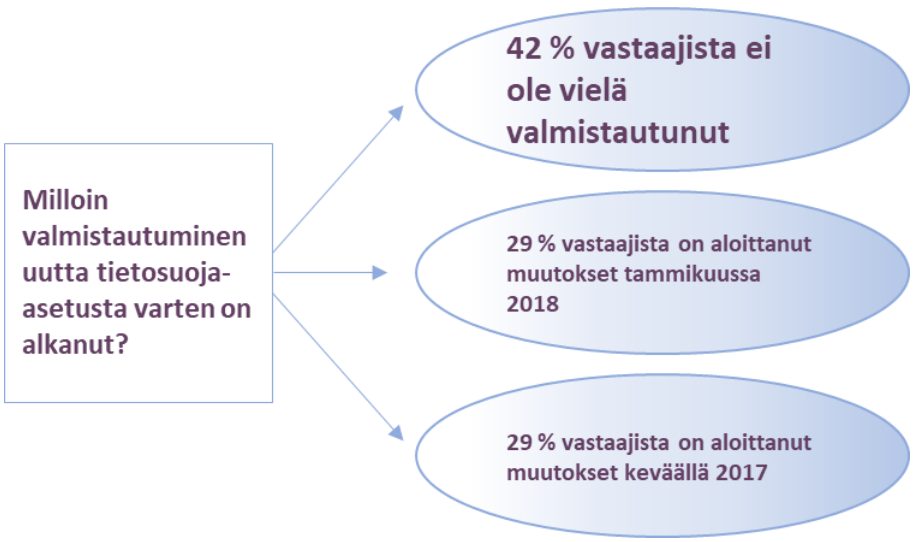
Tutkimustulokset on esitetty jaoteltuna alla oleviin alalukuihin. Luvussa 5.1.1 on esitetty tutkimusosan 1 tulokset ja luvussa 5.1.2. on esitetty tutkimusosan 2. vaiheen tulokset. Kaikki haastattelujen vastaukset on käyty ensin sanallisesti läpi, tämän jälkeen on esitetty haastateltavien vastauksista suoria lainauksia ja lopuksi niistä on esitetty kuvio. Kuviossa vastaukset on tiivistetty ja vastaukset on luokiteltu karkeammin tiettyihin ryhmiin, mielipiteiden jakaantumisen mukaan. Eniten vastauksia saanut mielipide on korostettu suuremmalla fontilla. Lopuksi näiden molempien lukujen pohjalta on koottu yhteenveto, johtopäätökset luku 5.2., joissa verrataan molempien tutkimusten tuloksia keskenään.

5.1.1 Kevään 2018 haastattelujen tulokset

Kysymys 1: Milloin valmistautuminen uutta tietosuoja-asetusta varten on alkanut?

Lähes puolet vastaajista ei vielä ollut aloittanut asetuksen muutoksiin valmistautumista huhtikuussa 2018. Vajaa kolmannes vastaajista oli aloittanut muutokset jo keväällä 2017 ja sama määrä vastaajista oli aloittanut muutokset tammikuussa 2018. Suuremmissa yrityksissä valmistautuminen oli aloitettu huomattavasti aikaisemmin. Kuviossa 14 on kuvattu vastaajien valmistautumista asetusta varten.

> *Ei ole vieläkään aloitettu* (H2).
>
> *Pikkuhiljaa vuodenvaihteesta alkaen. Viimeisimmän kuukauden ajan aktiivisemmin ryhdytty miettimään konkreettisia käytännön toimia.* (H3.)
>
> *Tammikuussa 2018* (H5).



Kuvio 14. Valmistautuminen tietosuoja-asetusta varten

Kysymys 2: Oletteko saaneet mielestänne hyvin tietoa asetuksesta ja mistä tieto on tullut?

Haastatteluista kävi ilmi, että tietosuoja-asetuksesta on ollut informaatiota saatavilla. Monet olivat saaneet tietoa yhteistyökumppaneiltaan ja etenkin internetissä on vastaajien mukaan ollut tietoa saatavilla. Toisaalta kaikkia tieto ei ole tavoittanut, sillä eräs vastaajista ei vielä huhtikuussa tiennyt koko asetuksesta mitään. Monet vastaajat kertoivat saaneensa tiedon jonkun toisen kautta, muun muassa kirjanpitäjältään, konsulttifirmalta tai yhteistyökumppanilta. Eräs vastaaja kertoi, että internetissä on tullut paljon tietoa vastaan. Osalle vastaajista asetuksen sisältö ei ole ollut vielä täysin selvää ja siksi vastaajat odottavat ennakkotapauksia.

Tämän perusteella voidaan todeta, että tietoa voi olla vaikeasti saatavilla, jos sitä ei osaa itse oikeasta paikasta etsiä. Toisaalta tietoa kyllä tuntuu löytyvän, jos on tarpeeksi kiinnostusta asiaa kohtaan. Esimerkiksi yksi vastaajista oli nähnyt aiheeseen liittyvän dokumentin. Vastaavasti toinen vastaajista kertoi, että heidän yritys on ohjeistanut ja jakanut tietoa asetuksesta myös muille. Vastaajien saaman tiedon jakautuminen on kuvattu kuviossa 15 (Kuvio 15, sivu 54).

> *Kirjanpitäjä on kertonut tämän vuoden puolella, olisiko ollut helmikuussa, asiasta* (H1).
>
> *En tiedä koko asetuksesta mitään* (H2).
>
> *Mielestäni valtaosa tiedosta on ollut jokseenkin epäselvää, paljon infoa asetuksesta, mutta tosi vähän ”suomennettuna” ja pilkottuna konkreettisiin käytännön toimiin. Paras tieto on tullut webinaarista, jossa asiaa on lähestytty tilitoimiston näkökulmasta.* (H3.)
>
> *Aika paljon oman harrastuneisuuden kautta — — katsoin nimittäin aiheeseen liittyvän dokumentin* (H6).

Kuvio 15. Tiedon saanti asetuksesta

Kysymys 3: Onko kaikki asetuksen vaatimat toimenpiteet jo tehty tai millä aikataululla toimenpiteet on tarkoitus toteuttaa?

Haastattelujen perusteella pienemmissä yrityksissä on havahduttu sekä käytännön muutoksiin että aloitettu asetuksen vaatimat valmistelut vasta vuoden 2018 vaihteessa. Tämän johdosta monessa yrityksessä valmistelut olivat vielä haastatteluhetkellä eli huhtikuussa kesken. Kuitenkin suurin osa vastaajista oli sitä mieltä, että asetuksen vaatimat muutokset saadaan valmiiksi toukokuun 25 päivään mennessä. Asetuksen vaatimien toimenpiteiden toteutumisaikaa on kuvattu kuviossa 16 (Kuvio 16, sivu 55).

> *Pitää ensiks opetella ne mitä tarvii tehdä muutoksia. Kai ne tarvii siihen toukokuun alkuun saada.* (H1.)
>
> *Kaikkea ei ole tehty, toimenpiteet toteutetaan 25.5. mennessä* (H3).
>
> *Nyt varmaan tehdään mitä pystytään, osataan ja voidaan ja sitte se muotoutuu vielä siitä sitte tulevina aikoina tai jonku ennakkotapausten kautta* (H4).
>
> *Kartoitus käynnissä, toteutus kestänee pari vuotta, jotta kaikki valmista* (H5).

Kuvio 16. Toimenpiteiden toteuttaminen

Kysymys 4: Mitä suurimpia muutoksia teidän/yrityksenne toiminnassa tuleva asetus on aiheuttanut tai tulee aiheuttamaan?

Monessa yrityksessä joudutaan tekemään käytännön muutoksia ja hankintoja asetuksen vaatimusten täyttämiseksi. Muun muassa konekantaa sekä palveluntarjoajia on täytynyt vaihtaa ja tehdä järjestelmiin muutoksia. Lisäksi muutoksia on täytynyt tehdä, jotta sähköpostin ja sähköisten kansioiden suojaukset sekä salaukset saatetaan ajan tasalle. Huomiota pitää kiinnittää myös konkreettisiin sopimuspapereihin. Suurimpina muutoksina koettiinkin tietojärjestelmien muutokset, joihin liittyi järjestelmien kartoitus ja uusiminen. Myös sopimuksien uusiminen ja päivittäminen sekä asetuksen sisällön opiskelu on koettu suureksi muutokseksi.

Lisäksi työtä tulee aiheuttamaan asiakkaiden ohjeistaminen, jolloin asetuksen vaatimukset pitää myös miettiä erikseen jokaisen asiakkaan näkökulmasta, jotta heitä osaa ohjeistaa. Tätä ajatusta tuki myös haastattelun lopusta toisen asiantuntijan kommentti tili- ja isännöintitoimistojen vastuusta ja velvollisuudesta informoida asiakkaitaan, vaikka ei olisi tarkoitus toisen puolesta hoitaakaan asiaa. Kuviossa 17 (Kuvio 17, sivu 56) on kuvattu asetuksen vaatimien toimenpiteiden aiheuttamia suurimpia muutoksia.

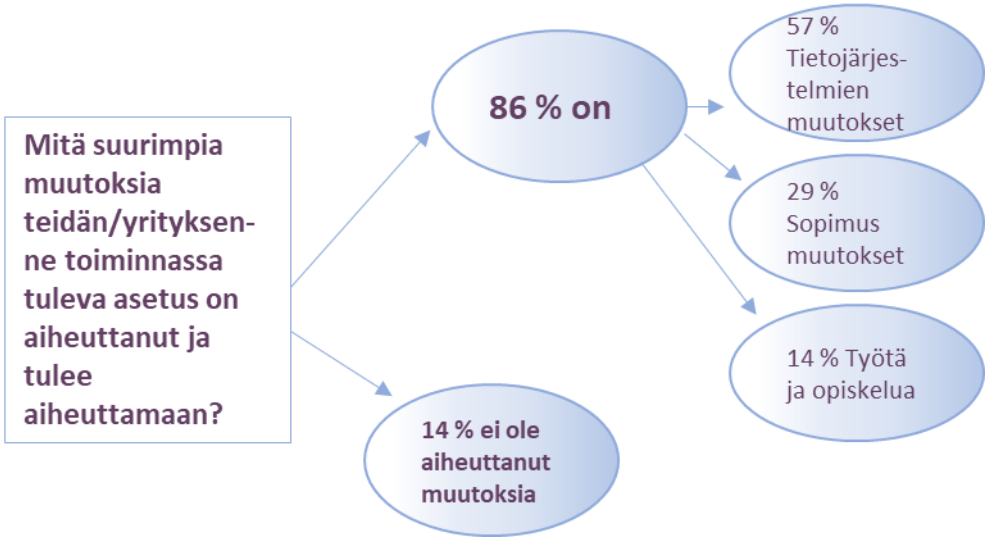
> *Lisää työtä ja opiskelua. Olen joutunut lukemaan pirun monta tiedonantoa siitä, miten saa olla ja miten ei saa olla* (H1).

> *Sähköpostin ja sähköisten kansioiden suojaukset/salaukset ajan tasalle. Lisäksi sopimusten laadinta tietosuoja-asetuksen osalta. Asiakkaiden ohjeistaminen ja tarvittavien lomakkeiden sekä prosessikuvausten yms. laadinta. Tietosuoja-asetuksen vaatimukset pitää miettiä erikseen jokaisen asiakkaan näkökulmasta, jotta osaa ohjeistaa jokaista juuri oman yrityksen tarvittavissa toimenpiteissä.* (H3.)

No meillä ainakin IT:n näkökulmasta taas kolmannen osapuolen sopimukset ulkopuolisiin toimittajiin tai palveluntarjoajiin. Me ollaan nyt jouduttu uusimaan niitä sopimuksia tai täydentämään, sisällyttää sinne tietosuoja-asetuksen vaatimia juttuja et saadaan vieritettyä sitä vastuuta myös kumppaneille. (H4.)

Konekannan vaihto ja palvelin palveluntarjoajan vaihto ja järjestelmän muutokset (H5).

Perustiedot niistä (tietojärjestelmistä) ja me lähdettiin sitä taulukkoa — — täydentämään ja hiukan laajentamaan nyt sitä silmällä pitäen et me saadaan ajan tasalla oleva kuva siitä, mitä järjestelmiä miellä on täällä käytössä ja mitkä tietojärjestelmät niistä on sellassia, joissa käsitellään henkilötietoja — — (H7).



Kuvio 17. Asetuksen aiheuttamat suurimmat muutokset

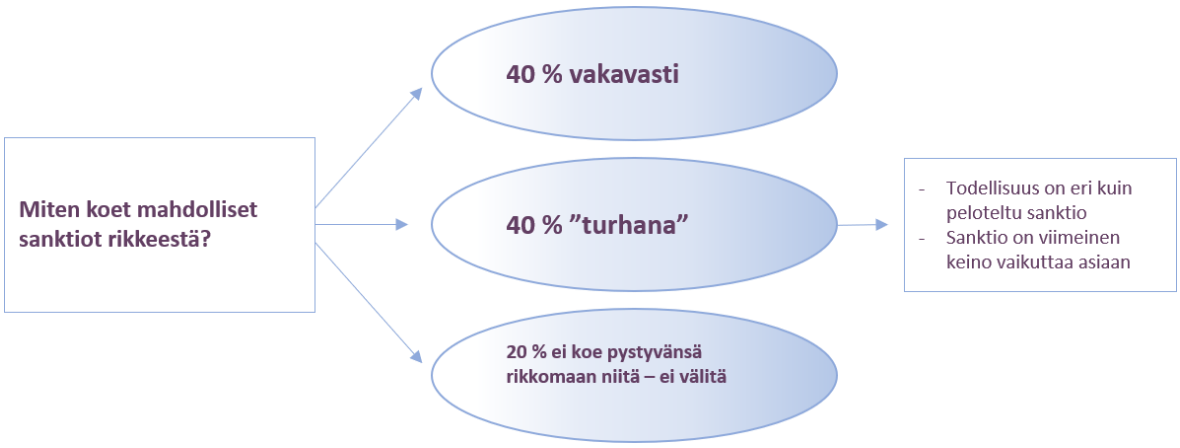
Kysymys 5: Miten koet mahdolliset sanktiot rikkeestä?

Sanktioihin suhtauduttiin ristiriitaisesti. Kysymyksiin sanktioista vastasi 6 haastateltavista ja sanktioihin suhtautumiseen liittyvät vastaukset on tiivistetty kuvioon 18 (Kuvio 18, sivu 57). Sanktioita ei koettu kohtuuttomiksi ja niitä pidettiin jopa tarpeellisena ja niihin suhtauduttiin vakavasti. Osalle vastaajia sanktioilla ei tuntunut oleva kovinkaan paljon merkitystä. Eräs yrittäjä muun muassa totesi, että uutisoitu sanktioiden pelote on ihan eri kuin todellisuus. Toinenkin vastaajista oli sitä mieltä, että häntä eivät sanktiot pelota, sillä hän ei koe pystyvänsä rikkomaan asetusta. Toisaalta osa vastaajista koki, että sanktiot ovat tarpeellisia kaupallisille toimijoille vaatimusten täyttämiseksi. Yksi vastaajista mainitsi, että sanktiot ovat edesauttanet sitä, että asetuksen vaatimat muutokset tehdään ajoissa. Mielenkiintoista on siis seurata, minkälaisia sanktiota näistä tietosuoja-asetuksen rikkomuksista käytännössä annetaan, ja millä lailla näitä aiotaan käytännössä valvoa.

Höpöhöpö juttuja, todellisuus on eri kuin uutisoitu sanktio pelote. (H5).

— —mun mielestäni kohtuu kohtuulliset — — mun mielestä ne on ihan ok. Noille kaupallisille toimijoillehan se on, et kyl mä ymmärrän et se on pakko olla et se toimii niille sitte taloudellisena pelotteena — —. (H6.).

Tietosuojavaltuutettu Reijo Aarnio on aika hyvin tätä asiaa toppuutellu niiden sanktioiden osalta eli hän on tuonut sitä useammassa yhteydessä esille, että ne sanktiot on todellakin vasta viimeinen keino laittaa asioita järjestykseen. On lukuisa määrä muita työkaluja esimerkiks, valvovalla viranomaisella käytettävissään, missä ei tarvi mennä sinne sanktioihin asti. (H7.)



Kuvio 18. Sanktiot

Pk-yritysten valmistautuminen

Kahdelta asiantuntijalta kysyttiin vielä pääkysymysten lisäksi, miten he ovat kokeneet pk-yritysten suoriutuneen muutoksista. Toinen oli sitä mieltä, että pk-yritykset ovat heränneet muutoksiin vasta tämän vuoden keväällä ja kiireellä yrittävät täyttää keskeisimpiä muutoksia. Kuitenkin hän epäilee, ettei kukaan ole voinut välttyä tiedolta asetuksen osalta. Myös toinen vastaajista epäili, että pk-yritykset ovat perehtyneet asiaan huonosti. Hän oli kuitenkin sitä mieltä, että syynä saattaisi olla tiedonpuute. Näkevätkö yritykset tarpeeksi uutisointia ja ymmärtävätkö he vaatimusten täyttämisen.

Taulukko 7. Ensimmäisen tutkimusosan tulokset

Ensimmäisen osan tulokset	
Valmistautuminen alkanut	42 % vastaajista ei ole vielä valmistautunut
Mistä tieto on saatu	86 % on saanut hyvin tietoa joko itse etsimällä tai tietoa on tarjottu
Suurimmat muutokset	57 % tietojärjestelmien muutokset
Onko toimenpiteet jo tehty?	57 % valmista tai aikoo saada valmiiksi 25.5. mennessä
Sanktiot	40 % suhtautuu vakavasti ja 40 % pitää sanktiota vasta viimeisenä keinona

Ensimmäisen osan tuloksista, jotka on esitetty taulukossa 7, voidaan todeta, että asetukseen on valmistauduttu suhteellisen hyvin, vaikka valmistautuminen on monella yrityksellä vielä kesken. Suurin osa vastaajista on kuitenkin saanut hyvin tietoa asetuksesta ja tästä voidaan päätellä, että valmistautumisen puute ei johdu tiedonsaannista. Silti yli puolet vastaajista aikoo kuitenkin tehdä asetuksen vaatimat muutokset määräaikaan eli toukokuun 25 päivään mennessä. Osalle muutoksien tekemisen motivaationa toimivatkin suurehkot sanktiot, jotka saavat yritykset ottamaan asetuksen vakavasti. Osa kokee sanktioiden olevan vasta viimeinen ja kovin keino puuttua henkilötietojen käsittelyn epäkohtiin. Suurimpia asetuksen aiheuttamia muutoksia ovat tietojärjestelmien muutokset, joilla tässä tarkoitetaan muun muassa järjestelmien vaihtoa, sähköisten kansioiden suojauksien ja salauksien päivittämistä.

5.1.2 Syksyn 2018 haastattelujen tulokset

Kysymys 1: Oletteko saaneet mielestänne hyvin tietoa asetuksesta ja mistä tieto on tullut?

Suurin osa vastaajista koki, etteivät he ole saaneet tietoa asetuksista tarpeeksi, mutta samassa yhteydessä he sanoivat löytäneensä tietoa, kunhan vain itse olivat sitä etsineet. Vastaukset on tiivistetty kuvioon 19 (Kuvio 19, sivu 59). Vastauksista voi päätellä, että vastaajat olisivat odottaneet saavaansa enemmän tietoa esimerkiksi viranomaistahoilta ilman, että tietoa on täytynyt lähteä oma-aloitteisesti etsimään. He, jotka kokivat saaneensa riittävästi tietoa, olivat saaneet sitä verkkokursseista, webinaareista, Kiinteistö- ja Isännöintiliitosta, Tietosuojavaltuutetun internetsivuilta sekä koulutustarjoajien kautta ja tiedotusvälineistä. Myös opinnäytetöitä sekä muiden tekemiä tiedotteita aiheesta on käytetty apuna. Lisäksi eräs vastaajista totesi, ettei ollut saanut isoimmilta liitoiltakaan

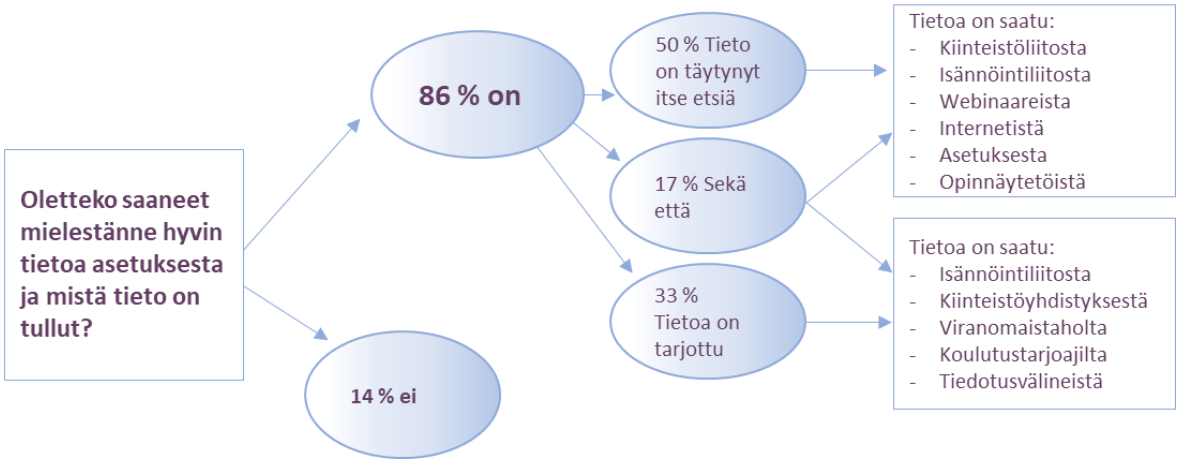
selkeää ohjeistusta ja oli siksi hieman hämillään, että miten pienemmät yritykset voivat selvitä muutoksista, kun asia ei ole vielä täysin selkiytynyt isommillekaan toimijoille.

> *— — en oo etsiny enkä oo saanukkaan et se on hieman vieras. En oo tarvinnu sitä työssä sillä lailla nii se on jääny vähä muiden kiireiden jalkoihin.* (H8.)

> *Et sitähä oli sitä tietosuoja–asetusta joku julkinen kampanja radiosta, mut ei se mun mielestä tommonen kampanjointi, olis pitäny kohdistaa suoraan yrityksille enemmän — — . — — ite haettiin tietoa siitä kiinteistöliitosta ja isännöintiliiton kautta, itte jouduttiin aika paljon selvittään ja siitä ei oikein kukaan liitosta tienny mitään, että ite selvitettiin ja siitä sitte tehtii. — — kysyttiin viimesiä kantoja (liitolta) ni ne oottaa noita EU:n tarkennuksia. Se on vähä silleen ongelma tietenkin meille pienemmille yrittäjille ja muille, et jos isotkaan ei tiedä, eikä oikein kukaan tiedä miten.* (H10.)

> *Tietoa on runsaasti tarjolla ja kyl sitä on hyvin saatu, mutta oma-aloitteisuutta se on edellyttänyt. — — Tietosuojavaltuutetun toimiston kotisivut on ollut hyvä tietolähde.* (H12.)

> *— — se on tullut ihan viranomaistaholta aikanaan kun ne on julkistanu, et tällanen Eu:n tietosuoja-asetus tulee* (H13).



Kuvio 19. Tiedonsaanti asetuksesta

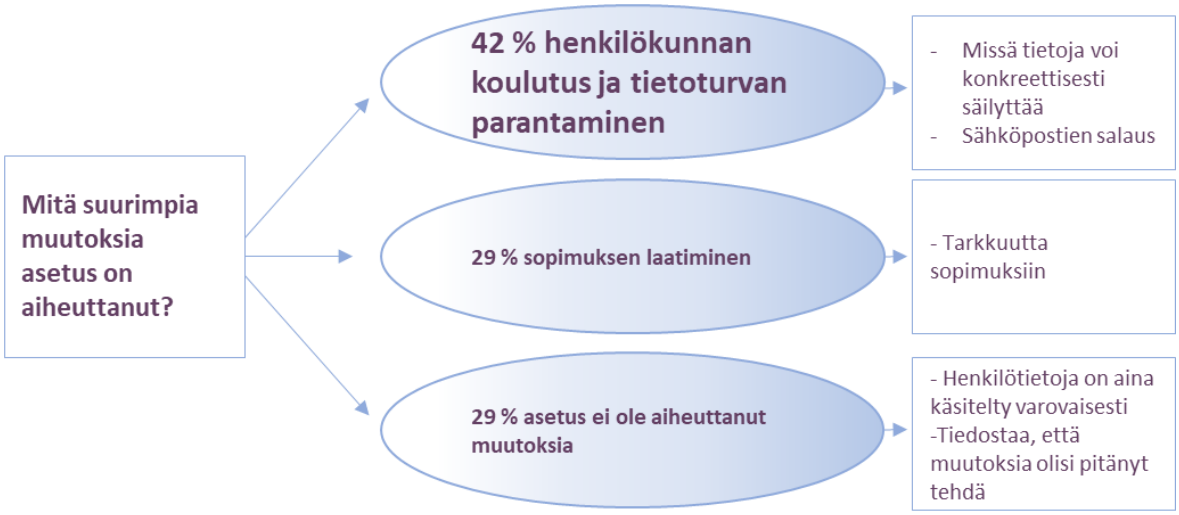
Kysymys 2: Mitä suurimpia muutoksia asetus on aiheuttanut?

Suurimpina muutoksina vastaajat kokivat tietoturvan parantamisen ja henkilökunnan kouluttamisen. Myös sopimuksien päivittäminen vastaamaan asetuksen vaatimuksia on ollut suuri muutos. Lisäksi asetus on saanut monet pohtimaan palvelutilojaan, sähköpostin suojaamista ja asiakastietojen turvallista säilyttämistä. Vastaavasti eräs haastateltava koki asetuksen tuomana lieveilmiönä liioitellun varovaisuuden henkilötietoja käsiteltäessä työpaikan sisällä. Suurimpia muutoksia on kuvattu kuviossa 20 (Kuvio 20, sivu 60).

No täytyy myöntää, että ei juuri mitään, tullu tehtyä muutoksia aikasempaan, koska näitä nyt muutenki, näitä henkilötietoja täytyy tietysti aika varovasti käsitellä eikä tietysti aikasemminkaan niitä voinu eikä oo mitenkää käytetty muuhun — —. — —se mikä varmasti olis pitäny tällänen tiedote asiakkaille tehdä niin, se on tekemättä (H9).

— —mehän ennakoitiin tätä asetusta puoltoista vuotta aikasemmin vähäse, et me tehtiin tohon palvelutiimit itse ja palvelutilat että kaikil on lukolliset työhuoneet — — (H10).

Yks semmonen todella typerä käytännön seikka. Me ei uskalleta enää puhua nimillä silloin, ku pitäis puhua nimillä. Et tulee sellai tietosuojaneuroosi, et puhutaan mr B:stä ja kukaan ei tiedä mistä puhutaan ja meil menee hirveesti hukkaan työaikaa siinä, et pelätään hoitaa asiaa silloin kun työ edellyttää nimillä tietosuojan vuoksi. Tää on yks semmonen suuri käytännön muutos mikä on aika hupsu. (H12.)



Kuvio 20. Suurimmat muutokset

Kysymys 3: Miten koet mahdolliset sanktiot rikkeestä?

Yli puolet vastaajista kokee sanktiot etäisiksi, koska Suomessa henkilötietojen käsittelyn liittyvät asiat ovat jo ennestään hyvällä mallilla. Vastaukset on esitetty kuviossa 21 (Kuvio 21, sivu 61). Osa vastaajista vähättelee sanktioita ja kokee ettei voi saada niitä. Hieman alla puolet vastaajista kokee sanktiot kohtuuttomiksi ja isoiksi ja siksi ne halutaan ottaa vakavasti. Henkilöt, jotka eivät pelkää sanktioita ajattelevat, että ensimmäisenä ei lähdetä antamaan isoja sakkoja vaan ohjeistetaan toimimaan oikein. Yksi vastaajista kokee

sanktioiden toimivan sisäisenä työkaluna, koska niiden johdosta voi vaatia, että tietyt asiat yrityksessä laitetaan kuntoon.

> *On ne nyt aika kovia, vaikka toki sitten se fakta, että niitä ei ehkä ihan heti määrätä, että ensin kyl ohjeistetaan* (H3).

> *Mä en nyt muista oliko se 2miljoonaa vai mitä se nyt oli ni ohan se nyt ihan älytön summa — —. — — tarkennuksia siihen tarvis aika paljon tulla jos aateltas et sitä alettais käyttää sanktio mielessä. Tommosenaan se ei oo, koska siellä ei oo tarkentavaa ohjeistusta eikä mitään.* (H10.)

> *Sanktiot jossain määrin toimii työkaluna sisäisesti, et ku koko ajan tulee joka tuutista määräyksiä ja säädöksiä nii sillon ku vastaa jostakin asiasta, ni voin sanoa, että hei nää sanktiot on niin kovat et meil pitää olla nää jutut tietyl taval kunnossa. Silloin johto ja kollegat hyväksyy sen, et hei onhan tälle asialle tehtävä jotain. — — uskon et yleisesti Suomessa asiat on niin hyvässä kunnossa, että ei me nyt ihan heti jouduta maksumiehiks. Mutta onhan ne sanktiot aivan järjettömät suomalaisessa mittakaavassa. Et jos ne napsahtas maksuun, niin sehän kaatais minkä tahansa toimijan.* (H12.)

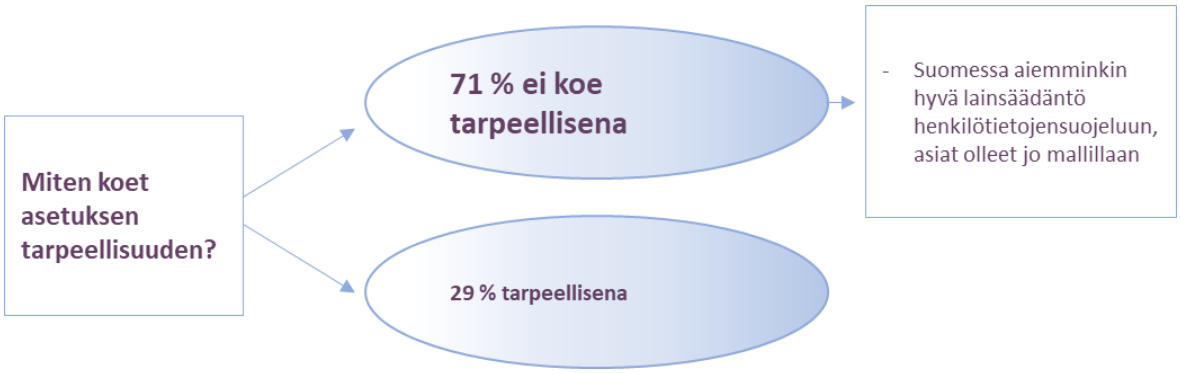
Kuvio 21. Sanktiot

Kysymys 4: Miten koet asetuksen tarpeellisuuden sekä sisällön ymmärrettävyyden?

Asetukseen tarpeellisuutta ja asetuksen sisällön ymmärrettävyyttä kysyttiin vastaajilta samassa kysymyksessä, mutta selkeyden vuoksi tuloksissa nämä on esitetty erikseen. Asetuksen tarpeellisuus jakaa vastaajien mielipiteitä ja tätä on kuvattu kuviossa 22 (Kuvio 22, sivu 63). Tämän tutkimuksen mukaan ajatellaan yleisesti, että Suomessa henkilötietojen käsittelyn taso on ollut hyvällä mallilla ilman uutta asetustakin, ja tästä syystä asetusta ei pidetä tarpeellisena, mutta muutama vastaaja koki asetuksessa olevan hyvääkin. Eräs vastaajista (H8) koki, että ei ole koskaan huono asia, jos uudellaan muistutetaan

käsittelemään henkilötietoja huolella, koska vastaajan mielestä Suomessakin on monenlaista toimijaa eikä välttämättä kaikille huolellinen henkilötietojen käsittely ole itsestään selvää. Asetuksen tavoitteena on edistää kilpailukykyä erityisesti sisämarkkinoilla, mutta eräs vastaajista (H13) oli sitä mieltä, että USA:han ja Aasiaan verrattuna asetus ei välttämättä ole ainakaan kilpailukykyä parantava tekijä.

> *— — tälläsestä pienyrittäjästä se ei nyt tunnu kovin tarpeelliselta, kun sitä kokkee sillälailla, että ei ne asiakastiedot oo aikasemminkaan ollu mitää yleistä jaettavaa tietoa — —* (H9).
>
> *No on varmaan tarpeellinen mutta olis nyt voinu olla vähän paremmin tarkennettu — — ennen ku se tulee, ni ois sisältöä tarkentaa aika, tai todella paljon että se on sisällöltään aika avoin* (H10).
>
> *— — se on täl hetkellä tälle alalle, ku henkilötietoja nyt muutenkin lähtökohtaisesti käsitellään huolellisesti et ei oo silleen uutta — —. — — tuntuu että tarviiko nää ihan nyt sitte kattaa tuota kaikki firmat sitten tuota sieltä vaikkapa isosta verkkokaupasta tälläseen pieneen tuota tilitoimisto tilitoimistoon sitten mutta kaikkeen täytyy sopeutua.* (H11.)
>
> *— — suomalaiset tietosuojasäännökset ja tää kansallinen sääntely oli oikeestaa — — että eihän tää meijän toimintaan ja muuhun tuo mitään uutta. Et turhaahan tää meille on, et byrokratiaahan tää vaan on — — ei me olla ennenkää asiakkaitten tietoja käsitelty välinpitämättömästi.* (H12.)
>
> *Siit voidaan olla tietyllä tavalla montaa mieltä, et toki mä nään sen, et sil on paikkansa et totta kai henkilösuoja — —ja tän tyyppisiä asioita pitää suojella. Suomessa toisaalta on jo ollu tietynlainen lainsäädäntö mikä suojaa jo. — —Suomessa välttämättä on mikään maata mullistava, varmasti se tuo siihen parannusta, mutta sillon myös liiketoiminnallisesti, jos me verrataan Eurooppaa Aasiaan, Yhdysvaltoihin mitkä ei ehkä tee asioita ihan samalla tavalla, ni ei tää nyt ehkä välttämättä oo mikään ainakaan kilpailukykyä parantava tekijä — — on siinä hyviä asioita, mutta se et, jos muut maanosat ei noudata sitä, niin mehän hävitään kilpailukykyä siinä.* (H13.)

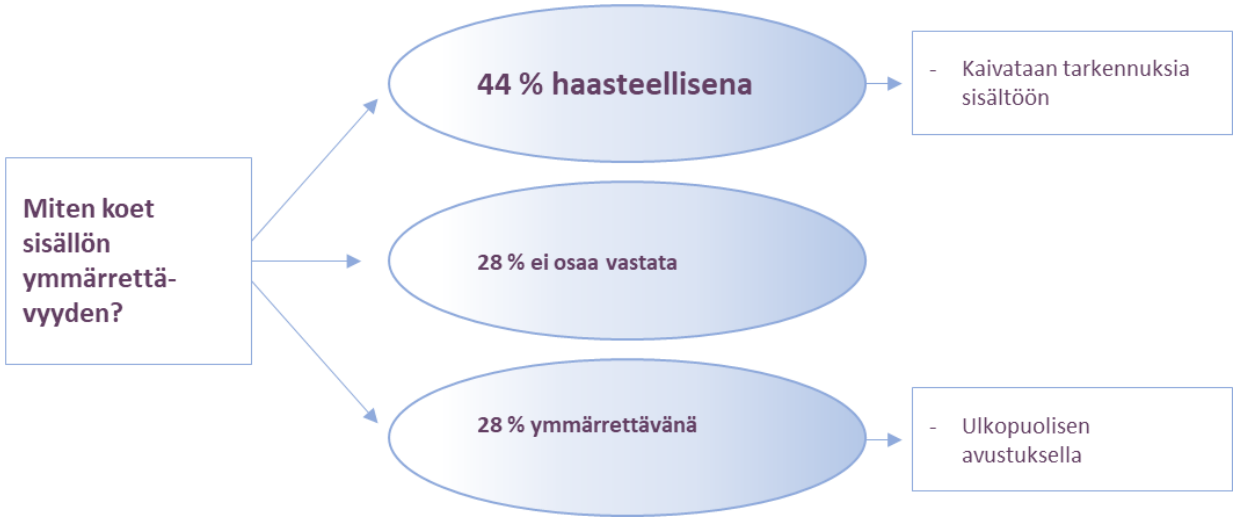


Kuvio 22. Asetuksen tarpeellisuus

Asetuksen sisällön ymmärrettävyys koetaan pääasiassa haasteelliseksi ilman koulutuksia tai asiantuntija-apua. Tämä voi johtua siitä, että sisältö koetaan avoimeksi ja sieltä täytyy osata hakea tarvittavaa tietoa. Sisältö toivottaisiin paremmin eritellyksi ja sisältävän enemmän tarkennuksia. Yksi haastateltava oli kokenut asetuksen sisällön kohtalaisen ymmärrettäväksi, mutta toteaa heti perään, ettei ole paljoa perehtynyt asetukseen. Vastauksien jakaantumista sisällön ymmärrettävyydestä on kuvattu kuviossa 23.

> *No eihän se nyt kauheen ymmärrettävää oo. Sieltä täytyy osata hakee ne, mitä sä haet. Et se vähä riippuu jokaisen ymmärryksestä, luetun sisällön ymmärtämisestä ja sanotaan näin et vähän joudut hakeen. Persoonat on erilaisia ja henkilöitä on erilaisia. Kaikki ei välttämättä sisäistä yhtä hyvin.* (H10.)

> *Ku jaksaa tarpeeks tavata ni kylhän sielt ne. Tässä nää koulutukset on ollu hirveen hyviä, ku ammattilainen on poiminu sielt ne avainkohdat. Mut onhan se hirveen pitkä prosessi ollu miettiä, et mitä se meille tarkottaa, mitä se meijän arkityössä oikeesti tarkottaa. Että kyllä se on ollu iso homma.* (H12.)



Kuvio 23. Sisällön ymmärrettävyys

Kysymys 5: Miten olette kokeneet selosteiden laatimisen ja informaatio velvoitteen täyttämisen?

Selosteiden laatiminen ja informointivelvoitteen täyttäminen on koettu tärkeämmäksi toukokuussa juuri ennen asetuksen siirtymäajan päättymistä kuin myöhemmin syksyllä. Yksi vastaajista on kokenut selosteiden laatimisen hyväksi, koska samalla on tullut mietittyä mitä henkilötietoja yrityksessä kerätään ja miksi niitä kerätään. Yksi vastaajista on sitä mieltä, että heillä tietosuoja-asetuksen vaatimat muutokset ovat olleet suhteellisen selviä, mutta heidän asiakkaillaan ei nämä ole niin hyvin ehkä auennut. Kuten kuviosta 24 (Kuvio 24, sivu 65) selviää, suurin osa vastaajista on kokenut selosteiden laatimisen helpoksi, mutta työlääksi. Ainoastaan yksi vastaaja on kokenut selosteiden laatimisesta olleen hyötyä.

> *— — ne ohjeet on ollu vähän ympäripyöreitä ja heikohkoja, se on ollut ehkä vähän haastavaa, et jos ois ollu selkeemmät lomakkeet tai selkeemmät ohjeet ni se olis ehkä ollu helpompaa* (H3).
>
> *Meille oli suhteellisen selvää mitä tehdään niitten (sopimusten ja tietosuoja-asetuksen vaatimien muutosten) osalta, mutta ei se nyt esimerkiksi normaalille hallituksen puheenjohtajalle kauheesti auennut* (H10).
>
> *— — sen rekisteriselosteen täyttäminen sillon tietysti ku on hyvä malli ni tavallaan sitä ei sillo paljon muokata koen aika turhauttavaks — —* (H11).
>
> *Iso työ ja paljon ollaan käytetty esimerkiks muitten toimijoitten laatimia tietosuojaselosteita, rekisteriselosteita avuks — —* (H12).
>
> *— — et toisaalta me ollaan saatu lakimiehen kautta tietoa siitä, miten pitää olla, mut taas toisaalta viranomaistaholta ei oo tullu välttämättä ihan riittävästi ja kun — —. — — puuttuu se, kansallisen lainsäädännön vahvistus ja mahdollisesti ne omat poikkeamat tai jotku muut asiat siitä.* (H13.)

Kuvio 24. Selosteiden laatiminen

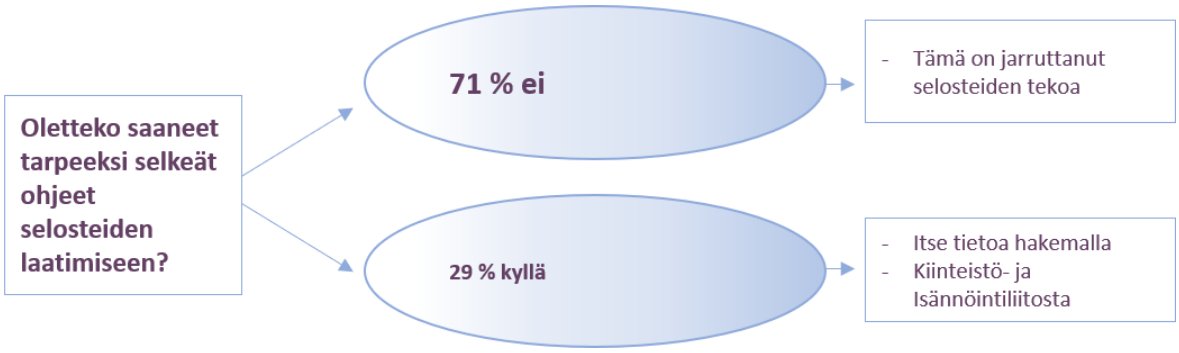
Kysymys 6: Oletteko saaneet tarpeeksi selkeät ohjeet selosteiden laatimiseen?

Kuten kuviosta 25 (Kuvio 25, sivu 66) käy ilmi, että vastaajat eivät ole kokeneet saaneensa tarpeeksi selkeitä ohjeita selosteiden laatimiseen. Selkeiden ohjeiden puuttuminen on hidastanut selosteiden laatimista. Yksi vastaajista oli kuitenkin sitä mieltä, että yleispätevää ohjetta ei voi olla olemassakaan, koska kaikki toimijat ovat niin erilaisia. Hänen mielestään ohjeista ja mahdollisista koulutuksista tulee poimia olennainen.

> *No ehkä alun perin ei, sitte taas tankkaa ja tankkaa ni sit se pikkuhiljaa siit selkiytyy* (H3).

> *— — ei ollu mitään sellasta ohjeistusta, ohjeistusta mulla tässä. Se osittain ehkä jarrutti sitä, et mä en lähteny sitä tekemään.* (H9.)

> *— —ei, eikä niit voikkaan, niiku mä täs äsken mainitsin, ni meijän toiminta on niin monimuotosta että kylhän meijän täytyy näistä ohjeista ja koulutuksista poimia se olennainen eli just se, mitä kerätää, miten kerätää, missä säilytetään ja miks säilytetään. Ja sit itte pohtia ne lait ja asetukset minkä perusteella tää meijän tietojen käsittely ja säilyttäminen tapahtuu, et ei kukaan voi. Kaikki toimijat on niin erilaisia, et ei siit voi olla mitään yleispätevää ohjetta "Tän ku lyöt ni kaikki on kunnossa". Ja sit vielä, vaik ne on nyt kunnossa ni ku maailma muuttuu ja säädökset muuttuu ni näitähän pitäs ehtiä sitte päivittää.* (H12.)

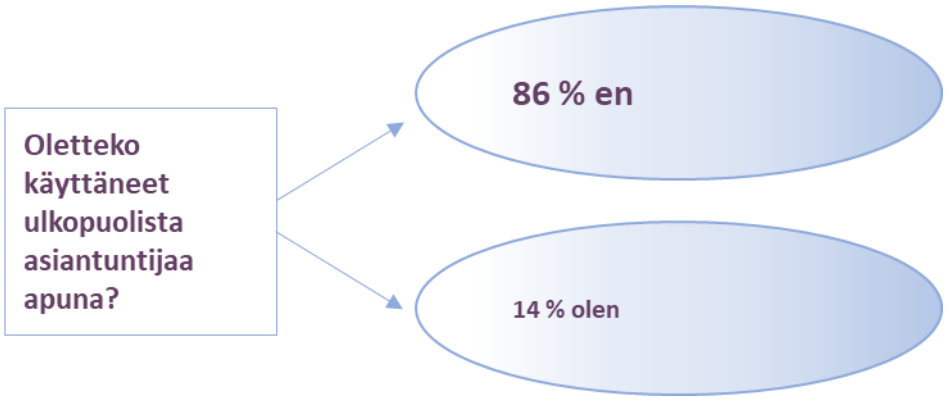


Kuvio 25. Selkeät ohjeet selosteisiin

Kysymys 7: Oletteko käyttäneet ulkopuolista asiantuntijaa apuna?

Vaikka selosteiden laatiminen on koettu työlääksi, vain yksi vastaajista oli käyttänyt ulkopuolista asiantuntija-apua selosteiden laatimiseen, kuvio 26.

> *Ei olla käytetty. Näitä kaupallisii tarjoajia on ollu paljon ja esimerkiks silloin, noin kaks vuotta sitte kevään korvalla nii meijän tilintarkastusyhteisöhän tarjos tälläst palvelua, et ne olis hoitanu tän homman ja tarkastellu ulkopuolisin silmin ja ihan sertifioinu meijän toiminnan. Se oli niin kallista, et se ollu mahdollista. Mut kyl ne nyt varmana aika oikeita ja asiallisia ne meijän selosteet, vaik ne nyt on itse omin pikku käsin näperrelty.* (H12.)



Kuvio 26. Apuna ulkopuolinen asiantuntija

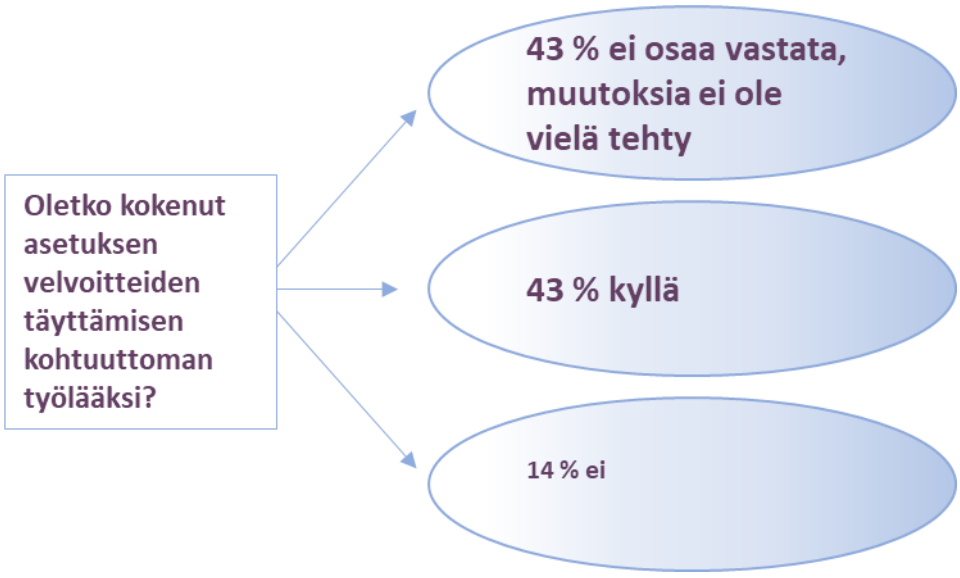
Kysymys 8: Oletko kokenut asetuksen velvoitteiden täyttämisen kohtuuttoman työlääksi?

Suurin osa vastaajista on kokenut asetuksen velvoitteiden täyttämisen työlääksi, tämä käy ilmi kuviosta 27 (Kuvio 27, sivu 67). Vastaajista puolet on ottaneet huomioon myös sen, että asetus tulee työllistämään jatkossakin. Tietoja täytyy säännöllisesti päivittää ja kansallinen tietosuojalaki on vasta tulossa täydentämän asetusta.

Mitä pitää sisällään se on ongelma, et jouduttiin polttamaan aika paljon omaa aikaa tai yrityksen työntekijöiden aikaa, et mitä kaikkee siihen nyt kuuluu ja mitä kaikkea meidän tulee tehdä. — — Kylhä se jatkossa tulee työllistämään aika paljonkin, että joudutaan nostaan hintoja ynnä muita. (H10.)

Noku ei me olla viel tehty sitä työtä totatota siis niin ettei me olla niiku muutaku — — kevyesti perehdytty tavallaan siihen sitten ja todettu et me nyt ei ihmeempiä — — muutoksia vaadia se silleen niiku toimintaan muuta ku tää netissä tää meidän ohjelma ja kaikki mitä nyt kyl nyt kaikki henkilötunnukset ja kaikki muut on vaan — — pilvessä (H11).

No kyllä. — — Et kylhän nää ihan älyttömän kuormittavia tämmöset uudistukset on, että ei se oo mikä sillee, et ku se kerran tehdään, ni se on siinä. Vaan mistä ne resurssit otetaa. (H12.)



Kuvio 27. Asetuksen velvollisuuksien täyttämisen kohtuullisuus

Kysymys 9: Miten koette asiakkaiden ohjeistamisen

Velvoitetta asiakkaiden ohjeistamisesta ei koeta negatiivisena asiana, haasteellisena kylläkin. Tämä johtuu siitä, ettei asiakkaita kiinnosta, vaikka osaa asiakkaista on tiedotettu ja kerrottu avoimesti asiasta. Lisäksi asiakkaat eivät ota asiaa niin vakavasti. Vastaukset on esitetty kuviossa 28 (Kuvio 28, sivu 69). Toisaalta yksi vastaaja toteaakin, että:

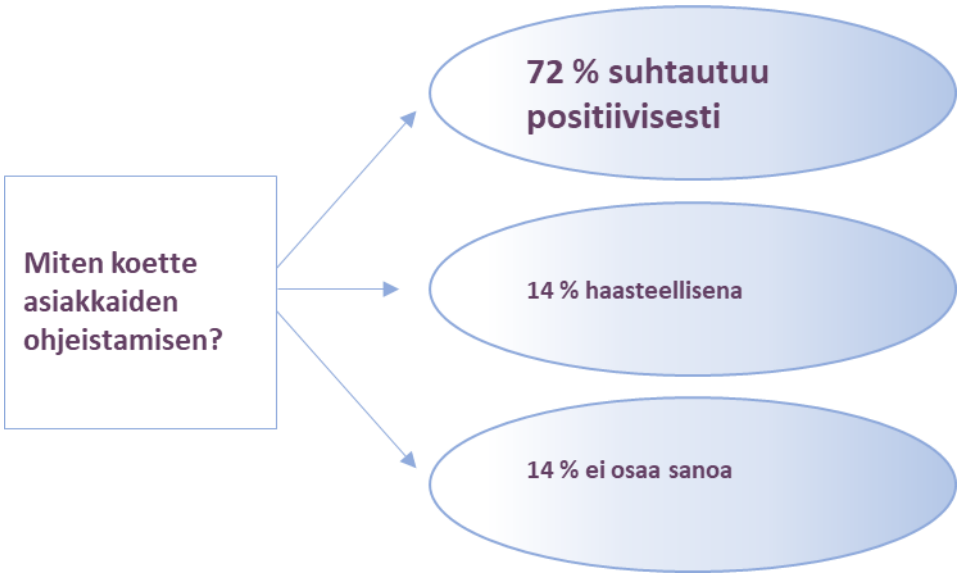
— — ehkä vähän haasteellista ja sit kun ehkä valtaosa asiakkaista ei pidä tota nyt mitenkään semmosena asiana, mitä ne haluis noteerata millään lailla, niin se ehkä tuo siihen vielä sen haasteen et kun niitä ei kiinnosta ja sit ehkä itsekin pitäis osata esittää se asia jotenki vielä selkeemmin (H3).

No eihän siinä ny mitään, me ollaan ohjeistettu sen tiedon varassa mikä meil on ollut — —mitä me tuolt kiinteistöliitost ja isännöintiliitosta ollaan saatu ja sen mukaan informoitu sitten hallituksenjäseniä ja puheenjohtajia. Ei siinä oikein voi muuta, ku ei isotkaan liitot osannu vastata selkeesti meijänkään kysymyksiin, täytyy jättää nilltä osin auki. (H10.)

No ne ketkä on kysyny niitten kanssa ollaan sit juteltu mut aika vähän ne on niistä ollut kiinnostuneita (H11).

— — kerrottiin näist rekistereist, et mitä siel säilytetään ja miks säilytetään. Tällänen ohjeistus on tehty ja sit on nää tiedonkeruulomakkeet, asiakastietolomakkeet, on yritetty saada mahdollisimman informatiivisiks ja kotisivuill on tietoa ja lomakkeita. En tiedä onks tää tämmönen saatavilla oleva ja vähän etupainotteisesti tehty tiedottaminen auttanu, mut — — ei oo tullu kysymyksiä. Sitähän me ehkä eniten pelättiin, että tulee hirveen paljon rekisteröintikyselyitä ja ku on aika tarkkaa tän asetuksen mukaan se, et kelle vaan ei voi antaa. Ni meilhän on hirveen tarkat ehdot, että missä se rekisteröidyn tiedon tietopyyntö tehdään ja että pitää olla viralliset henkkarit mukana. Ei niit oo tullu ensimmäistäkään. — — en tiedä sitte eikö suomalaisia kiinnosta vai mistä se johtuu, mutta ei sellasii kyselyitä oo tullu. (H12.)

— — me oltiin siinä tietyllä tavalla edelläkävijöitä. Me ollaan pidetty oma tilaisuus meidän asiakkaille. Me ollaan lähetetty heille infokirjettä ja pyritty kertomaan heille aika avoimesti, että mitä me tehdään ja mitä heidän pitää huomioida. Me ollaan tehty kaikkien meidän asiakkaiden kanssa henkilötietokäsittely sopimus missä on kerrottu nää asiat ja sovittu niistä — —heillä on tietyt velvollisuudet ja meillä on omat velvollisuutemme. (H13.)



Kuvio 28. Asiakkaiden ohjeistaminen

Osa vastaajista totesi, että asetus on jäänyt hieman ilmaan ja unohtunut toukokuun jälkeen. Yksi vastaajista sanoi, että aluksi oli asetuksesta paljon puhetta ja sitten pelotteltiin sanktioilla. Vastaaja itse käytti sanaa ”hype”. Vastaaja lisäsi vielä, ettei asetuksesta yhtäkkiä olekaan mitään kuulunut pitkään aikaan.

Taulukko 8. Toisen tutkimusosan tulokset

Toisen osan tulokset	
Mistä tieto on saatu	86 % on saanut hyvin tietoa joko itse etsimällä tai tietoa on tarjottu
Suurimmat muutokset	42 % henkilökunnan koulutus ja tietoturvan parantaminen
Sanktiot	Hieman suurempi osa (57 %) kokee niiden olevan etäisiä, mutta niihin suhtaudutaan kuitenkin vakavasti
Asetuksen tarpeellisuus ja sisällön ymmärrettävyys	71 % ei koe tarpeellisena ja 40 % kokee sisällön ymmärrettävyyden haasteellisena
Selosteiden laatiminen ja informointivelvoite	57% työlääksi, mutta suhteellisen helpoksi
Selkeät ohjeistukset selosteiden laatimiseen	71 % ei koe, että olisi saanut tarpeeksi ohjeita selosteiden laatimiseen
Apuna ulkopuolinen asiantuntija	86 % ei ole käyttänyt ulkopuolista asiantuntijaa apuna
Asetuksen vaatimusten täyttämisen työmäärä	57 % niistä, jotka ovat asetuksen vaatimat velvoitteet tehneet, ovat kokeneet niiden työllistäneen kohtuuttomasti.
Asiakkaiden ohjeistaminen	72 % suhtautuu positiivisesti asiakkaidensa ohjeistamiseen

Toisen osan tuloksista, taulukosta 8, voidaan todeta, että EU:n tietosuoja-asetuksesta on saatu tietoa hyvin. Tietoa on saatu monista eri lähteistä, ja asetuksesta on myös

itsenäisesti haettu täydentävää lisätietoa muun muassa koulutuksista, webinaareista ja opinnäytetöistä. Suurimpina muutoksina esiin nousi henkilökunnan kouluttaminen ja tietoturvan parantaminen. Henkilökunta pitää ohjeistaa käsittelemään henkilötietoja oikein, asetuksen mukaisesti. Vastaavasti tietoturvan parantamisella tarkoitetaan aina konkreettisten henkilötietoja sisältävien papereiden säilyttämisestä, henkilötietoja sisältävien pilvipalveluiden ja sähköpostien turvallisuuteen. Vastaajat olivat pohtineet missä voisivat säilyttää papereita, mihin lukolliset kaapit sijoitetaan ja toisaalta miten sähköisessä muodossa olevia tiedostoja säilytetään turvallisesti.

Yli kaksi kolmesta pitää asetusta tarpeettomana, koska vastaajat ajattelevat, että Suomessa on aina käsitelty henkilötietoja huolella ja meillä on hyvä henkilötietolaki. Toisesta vastaajasta tuntui myös siltä, että häviämme tällä kilpailukykyä verrattuna maihin, joissa tämä asia tehdään eri tavalla. Toisen vastaajan mielestä tämä on vain byrokratiaa. Toisaalta eräs vastaajista totesi, ettei ole koskaan paha muistutella käsittelemään henkilötietoja huolella, koska monenlaista toimijaa on alalla. Silti yritykset ovat suhtautuneet pääasiassa asetukseen vakavasti, koska sanktiot koetaan koviksi. Toisaalta moni vastaaja uskoo, että kovat sakot eivät ole ensisijainen keino puuttua, jos henkilötietoja on käsitelty väärin, siksi suurin osa vastaajista kokee niiden olevan aika etäisiä.

Vain yksi seitsemästä on käyttänyt ulkopuolista asiantuntijaa apuna, vaikka sisällön ymmärrettävyys on koettu haasteelliseksi. Tämä johtuu siitä, että asetuksen pääkohtia on ollut vaikea itse asetuksesta poimia. Luultavasti tästä johtuen myös selosteiden laatiminen ja informointivelvoitteen täyttäminen on koettu työlääksi, eikä selosteiden laatimiseen ole saatu tarpeeksi ohjeistusta. Puutteelliseksi koetut ohjeistukset ovat olleet joillekin osasyynä siihen, ettei selosteita ole laadittu. Osa vastaajista on käyttänyt selosteiden teon apuna muiden toimijoiden laatimia selosteita.

Asetuksen velvoitteiden täyttäminen on koettu jopa kohtuuttoman työlääksi. Tuloksista kävi ilmi, että asetuksen muutokset oli koettu aikaa vieviksi, sekä monet ottivat huomioon myös asetuksen vaatimat jatko toimenpiteet, kuten kansallisen lainsäädännön mahdolliset muutokset sekä rekistereiden pitämisen ajan tasalla. Toisaalta yhtä suuri osa vastaajista ei osannut ottaa kysymykseen kantaa, koska heillä tarvittavia muutoksia ei ollut vielä tehty. Selkeästi suurin osa suhtautuu asiakkaiden ohjeistamiseen positiivisesti ja vaikka asetus ei ole vielä monilla ihan hyvin hanskassa on asenne se, että kerrotaan niin hyvin kuin voidaan ja se mitä tiedetään. Tuloksista kävi myös ilmi, että rekisteröidyt eivät ole olleet kauhean kiinnostuneita heistä kerätyistä tiedoista tai itse asetuksestakaan.

5.2 Johtopäätökset

Taulukko 9. Yhteenveto tuloksista

	Ensimmäisen osan tulokset	Toisen osan tulokset
Valmistautuminen alkanut	42 % vastaajista ei ole vielä valmistautunut	
Mistä tieto on saatu	86 % on saanut hyvin tietoa joko itse etsimällä tai tietoa on tarjottu	86 % on saanut hyvin tietoa joko itse etsimällä tai tietoa on tarjottu
Suurimmat muutokset	57 % tietojärjestelmien muutokset	42 % henkilökunnan koulutus ja tietoturvan parantaminen
Onko toimenpiteet jo tehty?	57 % valmista tai aikoo saada valmiiksi 25.5. mennessä	
Sanktiot	40 % suhtautuu vakavasti ja 40 % pitää sanktiota vasta viimeisenä keinona	Hieman suurempi osa (57 %) kokee niiden olevan etäisiä, mutta niihin suhtaudutaan kuitenkin vakavasti
Asetuksen tarpeellisuus ja sisällön ymmärrettävyys		71 % ei koe tarpeellisena ja 40 % kokee sisällön ymmärrettävyyden haasteellisena
Selosteiden laatiminen ja informointivelvoite		57% työlääksi, mutta suhteellisen helpoksi
Selkeät ohjeistukset selosteiden laatimiseen		71 % ei koe, että olisi saanut tarpeeksi ohjeita selosteiden laatimiseen
Apuna ulkopuolinen asiantuntija		86 % ei ole käyttänyt ulkopuolista asiantuntijaa apuna
Vaatimusten täyttämisen työmäärä		57 % niistä, jotka ovat asetuksen vaatimat velvoitteet tehneet, ovat kokeneet niiden työllistäneen kohtuuttomasti.
Asiakkaiden ohjeistaminen		72 % suhtautuu positiivisesti asiakkaidensa ohjeistamiseen

Tutkimustulokset on koottu taulukkoon 9. Taulukosta olevien tulosten perusteella voi päätellä, että asetukseen valmistautuminen on ollut aika heikkoa, vaikka tietoa asetuksesta on ollut hyvin saatavilla. Ennen asetuksen siirtymäajan päättymistä ei ollut selkeää eroa sillä, mitä kautta tietoa oli saatu. Tietoa oli etsitty itse yhtä paljon kuin sitä oli tarjottukin. Vastaavasti päättymisajan jälkeen koettiin, että tietoa on pitänyt enemmän itse etsiä, vaikka vastausten perusteella tietoa on myös silloin ollut yhtä hyvin tarjolla. Tähän voi olla syynä heikko ennakkovalmistautuminen ja se, että kiinnostus tiedon etsimiseen sekä tarve tiedon saamiseen on lisääntynyt vasta siirtymäajan jälkeen. Lisäksi moni oli havahtunut vasta vuoden 2018 alussa, että asetus vaatiikin toimenpiteitä, ja varsinkin tilitoimistoissa vuoden vaihde on hyvin kiireistä aikaa, siksi toimenpiteet on osalta vastaajista lykkääntynyt.

Tulosten perusteella tietoa asetuksesta on siis ollut koko ajan hyvin tarjolla. Tästä huolimatta hieman alle puolet ensimmäiseen osaan vastanneista eivät olleet vielä huhtikuussa alkaneet tehdä valmisteluja asetuksen eteen. Huono valmistautuminen ei siis selity tiedonpuutteella, mutta tuloksista selvisi, että saatu tai löydetty tieto, on koettu epäselväksi. Ongelmana on ollut, että selkokielistä ohjeistusta ja käytännönesimerkkejä ei ole ollut tulosten perusteella hyvin saatavilla. Tämä on ollut osan kohdalla syy, miksi asetuksen vaatimia muutoksia ei ole tehty. Toinen mahdollinen syy selvisi syksyn tutkimusosassa: kaksi

kolmannesta vastaajista ei pidä asetusta tarpeellisena. Tämä selittää osittain syyn huonoon valmistautumiseen. Yritykset eivät ole kokeneet riittävää motivaatiota muuttaa henkilötietojen käsittelyn tapojaan asetuksen mukaiseksi, koska eivät koe sitä tarpeelliseksi. Tämä vastaavasti selittyy sillä, niin kuin moni vastaajakin erikseen mainitsi, että Suomessa on aina ollut henkilötietojen suojelu hyvällä mallilla. Tätä varten Suomessa on aiemmin ollut ja vielä toistaiseksi voimassa oleva henkilötietolaki. Yritykset ovat kuitenkin lähteneet tekemään asetuksen vaatimia käytännön muutoksia motivaationa mahdolliset sanktiot. Sanktiot ajatellaan kaukaisina, mutta kuitenkin kohtuuttoman suurina. Suurin osa vastaajista kokee, että suuret sanktiot eivät ole ensimmäinen keino puuttua, jos henkilötietoja on käsitelty väärin.

Suurimmiksi muutoksiksi todettiin ennen asetuksen siirtymäajan päättymistä tietotekniikkaan liittyvät muutokset, kuten sähköpostien salaukset, palvelutarjoajan ja tietojärjestelmien muutokset, kun taas siirtymäajan jälkeen suurimmiksi koettiin henkilökunnan koulutus ja tietoturvan parantaminen. Tietoturvan parantamiseen liittyy myös tietotekniikan muutokset, mutta tuloksista ilmeni myös, että pohdittiin myös sitä, missä ja miten henkilötietoja sisältäviä papereita, muistivälineitä aiotaan fyysisesti säilyttää. Ensimmäisen osassa vastauksissa ei tullut selkeästi ilmi tarvetta henkilökunnan kouluttamiselle. Tämä voi johtua siitä, että vastaajista suurin osa oli pienyrittäjiä, joilla ei ollut henkilökuntaa.

Sisällön ymmärrettävyys on aiheuttanut päänvaivaa monille yrittäjille, koska selkeää ohjeistusta ei ole saatu. Tulosten perusteella voisi tulkita, että moni olisi toivonut saavan enemmän ohjeistusta, mutta nyt sitä on pitänyt itse etsiä ja se on koettu osittain haastavaksi itse sisäistää. Osa oli käyttänyt tulkinnassa apuna koulutuksia, joista asetuksen pääkohdat ovat olleet helpommin ymmärrettävissä. Koska yrittäjät eivät itsekään ole sisäistäneet asetusta vielä, on asiakkaidenkin ohjeistaminen koettu haastavaksi. Toisaalta selkeästi suurin osa vastaajista kuitenkin suhtautui asiakkaidensa ohjeistamiseen myönteisesti. Yksi vastaajista korosti, että heidän tilitoimistossaan se on ollut aina velvollisuus opastaa asiakkaitaan.

Omaa pohdintaa

Kaikessa yksinkertaisuudessaan asetuksen tavoite oli vastata nykypäivän haasteeseen, jossa kaikki tieto, palvelut sekä tuotteet ovat kovaa vauhtia siirtymässä sähköiseen ympäristöön. Kansalaiset arkailevat edelleen tietojensa tallentamista nettiin. Monen yrityksen sivuille pitää ensin luoda käyttäjätunnus, jotta esimerkiksi jonkun tuotteen voi tilata itselleen ja monet pelkäävät, että heidän tietonsa päätyvät tätä kautta vääriin käsiin. Pelko onkin aiemmin ollut varsin aiheellinen, koska ennen EU:n tietosuoja-asetusta ei ole ollut selkeitä määräyksiä siitä, miten rekisterinpitäjän tulee käsitellä henkilötietoja. Usein

esimerkiksi tavaran tilaamista varten on kirjauduttava ja luotava käyttäjätunnus. On hyvä, että nykyään näitä tietoja ei voi enää kerätä vain ”huvin vuoksi” vaan siihen tarvitaan lainsäädännöstä tuleva peruste.

Sääntelyä tarvitaan, jottei henkilötiedot joudu vääriin käsiin. Tätä kirjoittaessa on vielä varsin epäselvää, miten tietosuoja-asetuksen toteutumista käytännössä aletaan valvomaan. Lisäksi tämän tutkimuksen mukaan asetus on aiheuttanut suunnattoman paljon työtä myös yrityksiin, jotka eivät varsinaisesti toimi asetuksen tavoitteiden takia. Tällä tarkoitetaan sitä, että asetusta laadittaessa nämä toimijat eivät ole olleet lainsäätäjän ensisijaista kohderyhmää. Kun asetuksella esimerkiksi haetaan sisämarkkinoiden kehitystä, on varsin epätodennäköistä, että pienehkö tilitoimisto olisi edes kiinnostunut laajentamaan toimintaansa Suomen ulkopuolelle.

Asetuksen tavoite on yhtenäistää käytäntöjä EU:n sisällä, mutta kuitenkin selosteiden laadinta ja informointivelvoitteen täyttäminen on hyvin vapaamuotoista, kunhan vaadittu tietosisältö täyttyy. Esimerkiksi henkilötietolaissa rekisteripohja oli hyvin selkeä ja kaikilla samanlainen, nyt kun sen saa jokainen itse päättää niin rekisteröidyn näkökulmasta se ei välttämättä ole kauhean selkeää ja yhtenäistä.

Tili- ja isännöitsijätoimistojen ei kannata pitää asetusta mörkönä, koska kyseisillä yrityksillä on ollut jo ennen asetusta velvollisuus käsitellä henkilötietoja huolellisesti. Esimerkiksi palkanlaskennan yhteydessä arkaluontoiset tiedot on aiemminkin pidetty salassa. Jos henkilötietolain edellyttämät rekisteriselosteet ovat kunnossa, ei rekisteriselosteiden lisäksi laadittava seloste henkilötietojen käsittelystä ja informointivelvoitteen täyttäminen ole mahdoton tehtävä.

6 YHTEENVETO

Opinnäytetyön tarkoituksena oli luoda selkeä kuva siitä, miten EU:n tietosuoja-asetusta tulisi soveltaa käytännössä tilitoimistoissa. Sopimuksiin ja toimintatapoihin on asetuksen myötä täytynyt tehdä paljon muutoksia. Lisäksi asetuksen mukana tuoma osoitusvelvollisuus edellyttää tilitoimistoilta tarkempia suunnitelmia henkilötietojen käsittelyn koko elinkaaresta. Tilitoimiston on myös dokumentoitava tarkemmin henkilötietojen käsittelyyn liittyvät prosessit ja laadittava erilaisia selosteita osoittaakseen noudattavansa lakia ja asetusta. Tutkimuksen pääongelmaksi muodostui tarkastella, miten uusi tietosuoja-asetus on vaikuttanut tilitoimistojen toimintaan. Tutkimuksessa selvitettiin myös, miten yritykset ovat kokeneet saaneensa tietoa asetuksesta ja miten valmistautuminen on sujunut. Työhön otettiin mukaan henkilötietojen käsittelyn näkökulmaa myös asunto-osakeyhtiöiden kannalta, vaikka pääpaino oli tilitoimistoissa.

Työn teoreettinen puoli koostui kolmesta osasta, joista ensimmäisessä ja toisessa osassa tarkasteltiin sekä tietosuoja-asetusta yleisemmin että henkilötietojen käsittelyä koskevia periaatteita tarkemmin. Kolmannessa teoriaosassa käsiteltiin asetuksen tilitoimistoalalle aiheuttamia keskeisiä muutoksia ja vaadittavia käytännön toimenpiteitä. Teoriaosuudet yhdessä loivat perustaa tutkimusosalle, joka toteutettiin kvalitatiivisena tutkimuksena. Tutkimusmenetelmänä käytettiin puolistrukturoitua haastattelua ja haastattelut kohdistettiin tilitoimistoihin, pk-yrityksiin sekä asiantuntijoihin.

Tästä tutkimuksesta kävi ilmi, että haastatelluista suomalaisista yrityksistä aika monella on henkilötietojen käsittely ollut hyvin hoidettu jo ennen uutta tietosuoja-asetusta; varsinkin, jos lähes 20 vuotta olemassa olleen henkilötietolain mukaiset vaatimukset on ollut täytettynä ennestään. Yrityksissä ei ehkä oltu tajuttu, että tietosuoja-asetus toi kuitenkin aika vähän uusia muutoksia henkilötietolakiin verrattuna. Suurimmat muutokset tämän tutkimuksen mukaan tilitoimistoissa ovat olleet tietojärjestelmien ja tietoturvan parantaminen sekä erilaisten dokumenttien laadinta. Tietoa asetuksesta on ollut runsaasti tarjolla, mutta asetus on ehkä esitetty liian vaikeaselkoisesti. Tuntuukin, että asetuksen vaatimista toimenpiteistä on haluttu luoda mielikuva vaikeammasta asiasta kuin se todellisuudessa on. Tätä ovat myös hyödyntäneet koulutustarjoajat, jotka ovat pelotelleet yrityksiä “Asetus tulee, oletko jo valmis” -tyylisillä otsikoilla. Tutkimuksesta kävi myös ilmi, että varsinkin pienissä yrityksissä valmistautuminen asetukseen on ollut hidasta ja aloitettu myöhään. Samaan tulokseen oli päädytty myös toisessa aiemmin valmistuneessa aihetta käsittelevässä opinnäytetyössä. Vastaavasti suuremmissa yrityksissä asian eteen oli tehty jo töitä huomattavasti aikaisemmin. Suurempien yritysten asiantuntijat myös arvioivat valmistautumisen olevan heikkoa pienissä yrityksissä. Tilitoimistot olivat saaneet hyvin tietoa

asetuksesta, mutta valmistautuminen oli kuitenkin ollut heikkoa ja vaatinut tilitoimistoilta paljon lisätyötä. Osa kokikin lisätyön niin suurena haasteena, että tarvittavat toimenpiteet olivat jääneet tekemättä. Yhteenvetona voidaan todeta, että tutkimuskysymykseen saatiin vastaus ja tavoitteeseen päästiin.

Pätevyyttä ja luotettavuutta arvioitaessa tulee ottaa huomioon, että osa haastatteluista toteutettiin kasvotusten, osa puhelimitse ja kahteen saatiin vastaukset lomakkeella. Haastatteluja ei voi siksi täysin verrata eri häiriötekijöistä johtuen. Lisäksi tutkimuksessa haastattelut tehtiin eri aikaan, toiset ennen ja toiset jälkeen asetuksen soveltamisen, siksi täysin samoja kysymyksiä ei voitu käyttää, koska lähestymistapa oli haastatteluissa hieman eri. Tämä aiheutti tutkimustulosten analysoinnissa tiettyä problematiikkaa. Tästä huolimatta molemmissa kysymyskokonaisuuksissa saatiin selville selkeä vastaajien näkemyksiä tietosuoja-asetuksen tarpeellisuudesta, tiedonsaannista, sanktioista, tiedonhankinta tavoista, suurimmista muutoksista ja käytännön muutoksista mitä vastaajien organisaatioissa oli tehty.

Tutkimukseen haastateltiin yrityksien edustajia useista eri toimialoista eikä pelkästään tilitoimistoista. Suurin osa haastatteluun vastanneista yrityksistä oli pieniä ja vastaajat joko itse yrittäjiä tai muuten hoitivat tietosuoja-asetuksen vaatimuksia kyseisessä yrityksessä. Vain muutama asiantuntija työskenteli suuremmassa organisaatiossa. Edellä mainitut asiat vaikuttavat tutkimuksen pätevyyteen ja luotettavuuteen, koska tutkimuksen pääongelmana haluttiin tutkia vaikutusta tilitoimistoihin. Tässä työssä korostettiin paljon pienten yritysten näkökulmaa, koska suurin osa Suomessa toimivista tilitoimistoista on pienehköjä toimijoita ja näin ollen myös muilla aloilla toimivien yritysten edustajien vastauksia pystyttiin vertaamaan tilitoimistojen edustajien vastauksiin. Tämä seikka, sekä se että suurempien yritysten asiantuntija toimivat pienten tilitoimistojen yhteistyökumppaneina, parantaa hieman tutkimuksen pätevyyttä.

Tutkimustuloksia ei voi yleistää koskemaan koko tilitoimistoalaa, koska otanta oli pieni ja laaja-alainen; vastaajat edustivat muitakin aloja eikä pelkästään tilitoimistoja. Vastaajien yhtenevä näkemys pienten yritysten valmistautumisesta asetukseen kuitenkin parantaa tutkimustulosten yleistettävyyttä. Objektiivisuuttaa arvioitaessa tulee ottaa huomioon se, että tutkimuksen suorittajat tekivät opinnäytetyötä tarkoituksenaan hyödyntää sitä myös omassa nykyisessä työssään. Vaikka tekijät työskentelevät tilitoimistoyrittäjänä ja kirjanpitäjänä, ei kumpikaan osallistunut haastatteluihin vastaajan roolissa. Tekijöiden henkilökohtaisilla mielipiteillä on kuitenkin voinut olla vaikutusta haastatteluiden kulkuun. Objektiivisten johtopäätösten tekeminen pelkästään tutkimustulosten perusteella oli haasteellista, koska tekijöillä on ollut vahvat mielipiteet asetuksesta.

Jatkotutkimuksena tälle työlle voitaisiin toteuttaa tutkimus, jossa selvitetään miten tilitoimistot jatkossa päivittävät tietojaan, jotta tiedot pysyvät asetuksen vaatimalla tavalla ajan tasalla ja millä toimenpiteillä tiedot poistetaan järjestelmistä.

LÄHTEET

Painetut lähteet

Fredman, J. 2018b. Henkilötietojen suoja ja kirjanpitolaki – onko vaatimuksissa ristiriitaisuuksia? Tilisanomat 5/2018, 45-47.

Haarma, K. & Leppänen, T. 2018. Tietosuoja taloyhtiössä – Miten taloyhtiön ja isännöitsijän tulee hallita henkilötietoja. 1. painos. Helsinki: Hansaprint Oy.

Hanninen, M., Laine, E., Rantala, K., Rusi, M. & Varhela, M. 2017. Henkilötietojen käsittely: EU-tietosuoja-asetuksen vaatimukset. Helsinki: Kauppakamari.

Hassinen, H. 2018. Henkilötietojen käsittelyn säännöt yhtenäisiksi. Etelä-Suomen Sanomat.

Hirsjärvi, S., Remes, P. & Sajavaara, P. 2007. Tutki ja kirjoita. 13. osin uudistettu painos. Helsinki: Tammi.

Koivisto, P. 2018. Petkuttajia on nykyisin autovarkaita enemmän. Etelä-Suomen Sanomat. 8.9.2018.

Lehtinen, P. 2018. GDPR tuli, teitkö ainakin nämä asiat. Yrittäjäsanomat. 4/2018. 8.

Männistö, E. 2017. Miten palkkahallinnossa tulee valmistautua tietosuoja-asetukseen. Tilisanomat. 6/2017. 20-21.

Nevasalo, T & Parviainen, E. 2017. Vuosi aikaa valmistautua Eu:n uuteen tietosuoja-asetukseen. Tilisanomat. 3/2017, 28-31.

Nyyssölä, M. 2018. Yksityisyyden suoja työsuhteessa. 8. uudistettu painos. Helsinki: Alma Talent.

Elektroniset lähteet

Aluehallintovirasto. 2017a. Uusi rahanpesulaki voimaan 3.7.2017, valvontarekisteri perusteilla. Tiedote. [viitattu 20.11.2018]. Saatavissa: https://www.avi.fi/web/avi/-/uusi-rahanpesulaki-voimaan-3-7-2017-valvontarekisteri-perusteilla-etela-suomi-

Aluehallintovirasto. 2017b. Rahanpesulain valvonta. [viitattu 13.10.2018]. Saatavissa: https://www.avi.fi/web/avi/rahanpesulain-valvonta

Bergström, E., Karhula, K. & Kipinoinen, K. 2018. EU:n tietosuojauudistuksen kansallinen täytäntöönpano. [viitattu 29.5.2018] Saatavissa: https://www.eduskunta.fi/FI/tietoaeduskunnasta/kirjasto/aineistot/kotimainen_oikeus/LATI/Sivut/EUn-tietosuojauudistus.aspx

Blencowe, A. 2018. Katoavatko nimitaulut porraskäytävistä uuden tietosuoja-asetuksen takia? Tietosuojavaltuutettu tyrmää tulkinnan. [viitattu 13.10.2018]. Saatavissa: https://yle.fi/uutiset/3-10076507

Eduskunta. 2018a. EU:n yleisen tietosuoja-asetuksen (GDPR) täytäntöönpano – Uusi tietosuojalaki. [viitattu 8.6.2018]. Saatavissa: https://www.eduskunta.fi/FI/tietoaeduskunnasta/kirjasto/aineistot/kotimainen_oikeus/LATI/EUn-tietosuojauudistus/Sivut/EUn-yleinen-tietosuoja-asetus.aspx

Eduskunta. 2018b. HE 9/2018 vp. Hallituksen esitys eduskunnalle EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi. Lain säätäminen. [viitattu 25.6.2018]. Saatavissa: https://www.eduskunta.fi/FI/vaski/KasittelytiedotValtiopaivaasia/Sivut/HE_9+2018.aspx

Ellonen, N., Danielsson, P. & Virtanen, M. 2018. Omaisuusrikokset. Luku 5 kokonaisuudesta Niemi, H. (toim.) 2018. Rikollisuustilanne 2017 - Rikollisuuskehitys tilastojen ja tutkimusten valossa. Katsaus 29/2018. [viitattu 15.10.2018]. Saatavissa: http://hdl.handle.net/10138/239656

Euroopan komissio. 2015. Eurobarometri 83.1 Suomen tulokset. [viitattu 30.7.2018]. Saatavissa: http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/ResultDoc/download/DocumentKy/66610

Euroopan komissio. 2018. Mitä tarkoittaa 'oikeutettu etu'? [viitattu 21.10.2018]. Saatavissa: 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 unionin perusoikeuskirja. 2000. Euroopan yhteisöjen virallinen lehti. [viitattu 20.6.2018]. Saatavissa: http://www.europarl.europa.eu/charter/pdf/text_fi.pdf

Eurooppa-neuvosto. 2015. EU:n tietosuojauudistus: neuvosto ja parlamentti yhteisymmärrykseen. Lehdistötiedote 951/15. [viitattu 5.6.2018]. Saatavissa: http://www.consilium.europa.eu/fi/press/press-releases/2015/12/18/data-protection/pdf

Eurooppa-neuvosto. 2016. Tietosuojauudistus. [viitattu 11.6.2018]. Saatavissa: http://www.consilium.europa.eu/fi/templates/content.aspx?id=4138

European Comission. 2015a. Special Eurobarometer 431 Data protection - Summary. Survey. TNS Opinion & Social network. [viitattu 30.7.2018]. Saatavissa: http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/ResultDoc/download/DocumentKy/66373

European Comission. 2015b. 431- Data protection. Factsheets in national language. [viitattu 2.10.2018]. Saatavissa: http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/Survey/getSurveyDetail/instruments/SPECIAL/surveyKy/2075

European Data Protection Supervisor. 2018. The History of the General Data Protection Regulation. [viitattu 8.6.2018]. Saatavissa: https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en

Fredman, J. 2018a. Alihankkijoiden käyttö pilvipalvelussa. [viitattu 13.10.2018]. Saatavissa: https://tilitoimistossa.taloushallintoliitto.fi/wp-content/uploads/2018/03/alihankkijoiden-kaytto.jpg

Fredman, J. 2018c. Tietosuoja-asetus TAL2018-sopimusuudistuksessa. Tilitoimistossa. 2/2018. [Viitattu 11.11.2018]. Saatavissa: https://tilitoimistossa.taloushallintoliitto.fi/teknologia-ja-ohjelmistot/tietosuoja-asetus-tal2018-sopimusuudistuksessa

Forrester. 2018a. About Forrester [viitattu 15.9.2018]. Saatavissa: https://www.forrester.com/marketing/about/about-us.html

Forrester. 2018b. Predictions 2018. A year of reckoning [viitattu 15.9.2018]. Saatavissa: https://www.slideshare.net/eraser/predictions-2018-a-year-of-reckoning-forrester

Forsgård, C. 2018. Lehto T 2018, mukaan artikellissa Gdpr-paniikki aiheutti turhien sähköpostien tulvan – isojen sakkojen uhka pelottaa. Tekniikka&Talous. [viitattu 21.10.2018]. Saatavissa: https://www.tekniikkatalous.fi/talous_uutiset/gdpr-paniikki-aiheutti-turhien-sahkopostien-tulvan-isojen-sakkojen-uhka-pelottaa-6726574

Hallituksen esitys 9/2018 vp. Hallituksen esitys eduskunnalle EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi. [viitattu 27.7.2018]. Saatavissa: https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Documents/HE_9+2018.pdf

Hienola, E. 2018. Saitko sähköpostitse tiedon 244,79 euron veronpalautuksista? Poista viesti, kyseessä on huijaus. [viitattu 15.10.2018]. Saatavissa: https://www.ksml.fi/kotimaa/Saitko-sähköpostitse-tiedon-24479-euron-veronpalautuksista-Poista-viesti-kyseessä-on-huijaus/1255442

Hyppönen, J. 2015. EU-asetus muuttaa yritysten ja yhteisöjen tietosuojakäytäntöjä. [viitattu 6.11.2018]. Saatavissa: https://tilisanomat.fi/teknologia/eu-asetus-muuttaa-yritysten-ja-yhteisojen-tietosuojakaytantoja

ID BBN. 2017. Vain harva selviytyy GDPR:stä menestyjänä. Blogi. [viitattu 6.10.2018]. Saatavissa: http://blogi.idbbn.fi/vain-harva-selviytyy-gdpr

Jourová, V. 2016. Tietosuojauudistus vahvistaa kansalaisten oikeuksia. Euroopan komission tiedote tammikuu 2016. [viitattu 30.7.2018]. Saatavissa: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=41726

Kajander, K. 2016. 02.11.2016 — Mitä tarkoittaa tietosuoja? [viitattu 14.10.2018]. Saatavissa: https://tietosuoja.info/blogi/mita-tarkoittaa-tietosuoja

Kiinteistöliitto. 2018. Usein kysytyt kysymykset. [viitattu 14.11.2018]. Saatavissa: https://www.kiinteistoliitto.fi/palvelut/tietosuoja/ukk/#q2

Koivumäki. E. 2017. EU:n tietosuoja-asetus ja henkilötietojen käsittelyperusteet. Blogi [viitattu 21.10.2018]. Saatavissa: http://www.elinakoivumaki.com/tietosuoja-asetus-ja-henkilotietojen-kasittelyperusteet/

Lehmusvirta, A. 2018. Ruotsissa jännitetään ensimmäisiä GDPR-tuomioita - tutkinnassa tunnettuja yhtiöitä. Artikkeli. [viitattu 12.10.2018]. Saatavissa: https://www.kauppalehti.fi/uutiset/ruotsissa-jannitetaan-ensimmaisia-gdpr-tuomioita-tutkinnassa-tunnettuja-yhtioita/a1044794-1bea-3e89-9e17-0b2643e2968e

Lehto, T. 2017. EU:n tietosuoja-asetus vaatii isot muutokset – suuri osa yrityksistä ei varautunut. Tekniikka & talous [viitattu 18.9.2018]. Saatavissa: https://www.tekniikkatalous.fi/ttpaiva/eu-n-tietosuoja-asetus-vaatii-isot-muutokset-suuri-osa-yrityksista-ei-varautunut-6630447

Lehtola, S. 2016. Uusi EU:n tietosuoja-asetus astuu voimaan 25.5.2018 – Ketä se koskee ja mitkä ovat sen keskeisimmät muutokset? [viitattu 6.2.2018] Saatavissa: https://www.emce.fi/blog/uusi-eun-tietosuoja-asetus-astuu-voimaan-25-5-2018-keta-koskee-mitka-keskeisimmat-muutokset/

Manninen, K. 2018. Tietosuoja kiristyy: Nimitaulut saattavat kadota porraskäytävistä. Savon Sanomat. [viitattu 13.10.2018]. Saatavissa: https://www.savonsanomat.fi/kotimaa/Tietosuoja-kiristyy-Nimitaulut-saattavat-kadota-porrask %C3 %A4yt %C3 %A4vist %C3 %A4/1109409

Millar, S. & Marshall, T. 2018. German Court Issues First GDPR Ruling. [viitattu 15.11.2018]. Saatavissa: https://www.natlawreview.com/article/german-court-issues-first-gdpr-ruling

Milt, K. 2018. Faktatietoja Euroopan unionista. Henkilötietojen suoja. [viitattu 20.6.2018]. Saatavissa: http://www.europarl.europa.eu/ftu/pdf/fi/FTU_4.2.8.pdf

MTV Uutiset. 2018. Europol huolissaan – EU:n tietosuoja-asetus on vaikeuttanut nettirikosten tutkintaa. [viitattu 15.11.2018]. Saatavissa: https://www.mtvuutiset.fi/artikkeli/europol-huolissaan-eu-n-tietosuoja-asetus-on-vaikeuttanut-nettirikosten-tutkintaa/6973282

Niemi, H. 2018a. EU:n Tietosuoja-asetuksen muutoksen vaikutukset tilitoimistossa. Satakunnan ammattikorkeakoulu, Liiketalouden koulutusohjelma [viitattu 26.11.2018]. AMK-opinnäytetyö. Saatavissa: https://www.theseus.fi/handle/10024/147435

Niemi, H. 2018b. Rikollisuustilanne 2017 - Rikollisuuskehitys tilastojen ja tutkimusten valossa. Katsaus 29/2018. [viitattu 15.10.2018]. Saatavissa: http://hdl.handle.net/10138/239656

Näpärä, L. 2017. Haastattelun lajityypit. Spoken Oy. Blogi. [viitattu 17.11.2018]. Saatavissa: https://www.spoken.fi/blogi/haastattelun-lajityypit

Oikeusministeriö. 2017. EU:n yleisen tietosuoja-asetuksen täytäntöönpanotyöryhmän (TATTI) mietintö. Mietintöjä ja lausuntoja 35/2017. Helsinki. [viitattu 30.5.2018]. Saatavissa: http://urn.fi/URN:ISBN:978-952-259-612-3

Oikeusministeriö, Tietosuojavaltuutetun toimisto. 2017. Miten valmistautua EU:n tietosuoja-asetukseen. Oikeusministeriön julkaisu 4/2017. Helsinki. [viitattu 9.9.2018]. Saatavissa: http://urn.fi/URN:ISBN:978-952-259-558-4

Oikeus.fi. 2017. Työryhmä ehdottaa uutta tietosuojalakia [viitattu 26.6.2018]. Saatavissa: https://oikeus.fi/fi/index/ajankohtaista/tiedotteet/2017/06/tyoryhmaehdottaauuttatietosuojalakia.html

Rissanen, R. 2006. 5.1 Fenomenografia. [viitattu 14.10.2016]. Saatavissa: http://www.fsd.uta.fi/menetelmaopetus/kvali/L5_1.html

Saaranen-Kauppinen, A & Puusniekka, A. 2006. KvaliMOTV - Menetelmäopetuksen tietovaranto. [Viitattu 18.11.2018]. Saatavissa: https://www.fsd.uta.fi/menetelmaopetus/kvali/L6_3_3.html

Taloushallintoliitto. 2018a. Sopiminen ja hinnoittelu. [viitattu 11.11.2018]. Saatavissa: https://taloushallintoliitto.fi/laatu-tyokalut/tilitoimiston-ohjeet-ja-tyokalut/sopiminen-ja-hinnoittelu

Taloushallintoliitto. 2018b. SOPIMUS HENKILÖTIETOJEN KÄSITTELYSTÄ TAL 2018. [viitattu 20.11.2018]. Ei saatavissa: https://sopimuskone.koho-online.com/framework_agreements/accounting_assignment_pdf

Taloushallintoliitto. 2018c. Työvälineet ja tietotekniikka. [viitattu 27.11.2018]. Saatavissa: https://taloushallintoliitto.fi/laatu-tyokalut/tilitoimiston-ohjeet-ja-tyokalut/tyovalineet-ja-tietotekniikka

Taloushallintoliitto. 2018d. Tietosuoja tilitoimistossa. [viitattu 27.11.2018]. Saatavissa: https://taloushallintoliitto.fi/laatu-tyokalut/tal-laatutyokalut-ja-ohjeet-tilitoimistolle/tietosuoja-tilitoimistossa

Tietosuojavaltuutetun toimisto. 2018a. Vaikutusten arviointi. [viitattu 13.10.2018]. Saatavissa: https://tietosuoja.fi/vaikutustenarviointi

Tietosuojavaltuutetun toimisto 2018b. Rekisterinpitäjän oikeutettu etu. [viitattu 21.10.2018]. Saatavissa: https://tietosuoja.fi/rekisterinpitajan-oikeutettu-etu

Tietosuojavaltuutetun toimisto 2018c. Tietoturvaloukkaukset. [viitattu 20.11.2018]. Saatavissa: https://tietosuoja.fi/tietoturvaloukkaukset

Tietosuojavaltuutetun toimisto 2018d. Osoita noudattavasi tietosuojasäädöksiä. [viitattu 27.11.2018]. Saatavissa: https://tietosuoja.fi/osoitusvelvollisuus

Tietosuojavaltuutetun toimisto 2018e. Seloste käsittelytoimista. [viitattu 27.11.2018]. Saatavissa: https://tietosuoja.fi/seloste-kasittelytoimista

Tietosuojavaltuutetun toimisto 2018f. Rekisterinpitäjän seloste käsittelytoimista. [viitattu 27.11.2018]. Saatavissa: https://tietosuoja.fi/rekisterinpitajan-seloste-kasittelytoimista

Tietosuojavaltuutetun toimisto. 2018g. Henkilötietojen käsittelijän seloste käsittelytoimista. [viitattu 27.11.2018]. Saatavissa: https://tietosuoja.fi/henkilotietojen-kasittelijan-seloste-kasittelytoimista

Tietosuojavaltuutetun toimisto. 2018h. Kerro käsittelystä rekisteröidylle. [viitattu 27.11.2018]. Saatavissa: https://tietosuoja.fi/rekisteroidyn-informointi

Valtiovarainministeriö. 2016. EU-tietosuojan kokonaisuudistus. VAHTI-raportti 1/2016 [viitattu 29.5.2018]. Saatavissa: https://www.vahtiohje.fi/c/document_library/get_file?uuid=c97ee414-1fc0-4a91-969c-2ef0657605d1&groupId=10128

Virtanen, J. 2018. Saksa ehti ensimmäisenä – gdpr-päätös napsahti, tärkeä ennakkotapaus. [viitattu 15.11.2018]. Saatavissa: https://www.tivi.fi/Kaikki_uutiset/saksa-ehti-ensimmaisena-gdpr-paatos-napsahti-tarkea-ennakkotapaus-6732521

Öljymäki, J. 2017. EU:n Tietosuojauudistus. Vaasa: Vaasan ammattikorkeakoulu, Liiketalous [viitattu 26.11.2018]. AMK-opinnäytetyö. Saatavissa: https://www.theseus.fi/handle/10024/130588

Lait, asetukset, direktiivit ja hallituksen esitykset

Asunto-osakeyhtiölaki 22.12.2009/1599.

Euroopan parlamentin ja neuvoston asetus (EU) 2016/679. [viitattu 6.11.2018]. Saatavissa: https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=celex %3A32016R0679

Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/680. [viitattu 6.11.2018]. Saatavissa: https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX:32016L0680

Henkilötietodirektiivi 95/46/EY. [viitattu 6.11.2018]. Saatavissa: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:fi:HTML

Henkilötietolaki 22.4.1999/523.

Kirjanpitolaki 30.12.1997/1336.

Laki rahanpesun ja terrorismin rahoittamisen estämisestä 444/2017.

Laki yksityisyyden suojasta työelämässä 13.8.2004/759.

Neuvoston puitepäätös 2008/977/YOS. [viitattu 6.11.2018]. Saatavissa: https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX %3A32008F0977

Osakeyhtiölaki 21.7.2006/624.

Työaikalaki 9.8.1996/605.

Työsopimuslaki 26.1.2001/55.

Suulliset lähteet

Kantelinen, T. 2018. Luotonhallintaseminaari. Ajankohtaista lainsäädännöstä. Seminaari. 9.10.2018.

Koivuniemi, J. 2018. Tiedonhallinnan perusteet – Arkistointisuunnitelma ja uuden tietosuojalain merkitys. Koulutus. 4.10.2018.

Suvanto, M. 2018. EU-tietosuoja-asetuksen vaikutukset ja käytännöt. Käyttäjäpäivät. 9.11.2018.

LIITTEET

Kysymykset, osa 1

- ☐ Milloin valmistautuminen uutta tietosuoja-asetusta varten on alkanut?
- ☐ Oletteko saaneet mielestänne hyvin tietoa asetuksesta ja mistä tieto on tullut?
- ☐ Mitä suurimpia muutoksia teidän/yrityksenne toiminnassa tuleva asetus on aiheuttanut ja tulee aiheuttamaan?
- ☐ Onko kaikki asetuksen vaatimat toimenpiteet jo tehty tai millä aikataululla toimenpiteet on tarkoitus toteuttaa?
- ☐ Miten koet mahdolliset sanktiot rikkeestä? (Hallinnollinen sakko voi olla jopa 20 miljoonaa euroa tai 4 % maailmanlaajuisesta liikevaihdosta.)
- ☐ Mikä on yleiskäsityksenne siitä, miten pk-yritykset ovat muutoksista suoriutuneet?

Kysymykset, osa 2

- ☐ Oletteko saaneet mielestänne hyvin tietoa asetuksesta ja mistä tieto on tullut?
- ☐ Mitä suurimpia muutoksia asetus on aiheuttanut?
- ☐ Miten koet mahdolliset sanktiot rikkeestä?
- ☐ Miten olette kokeneet asetuksen tarpeellisuuden ja sisällön ymmärrettävyyden?
- ☐ Miten olette kokeneet selosteiden laatimisen ja informointi velvoitteen täyttymisen?
- ☐ Oletteko mielestänne saaneet tarpeeksi selkeät ohjeet selosteiden laatimiseen?
- ☐ Oletteko käyttäneet ulkopuolista asiantuntijaa apuna? Jos olette niin ketä?
- ☐ Onko tietosuoja-asetuksen velvoitteiden täyttäminen mielestänne työllistänyt teitä kohtuuttomasti?
- ☐ Miten koette asiakkaidenne ohjeistamisen? / Miten olette kokeneet saaneen opastusta tilitoimistoltanne asetuksesta?