

**EUROOPAN PARLAMENTIN JA
NEUVOSTON YLEISEN TIETOSUOJA-ASETUKSEN
VAATIMUKSET REKISTERINPITÄJÄLLE**

Tuula Seppo
Pro gradu -tutkielma
Sosiaali- ja terveydenhuollon
tietohallinto
Itä-Suomen yliopisto
Sosiaali- ja terveysjohtamisen
laitos
toukokuu 2017

ITÄ-SUOMEN YLIOPISTO, Yhteiskuntatieteiden ja kauppatieteiden tiedekunta. Sosi-
aali- ja terveystieteiden laitos, Sosiaali- ja terveydenhuollon tietohallinto

SEPPO, TUULA: Euroopan parlamentin ja neuvoston yleisen tietosuoja-asetuksen
vaatimukset rekisterinpitäjälle

Pro gradu -tutkielma, 81 sivua, 6 liitettä (37 sivua)

Tutkielman ohjaajat: FT Sirpa Kuusisto-Niemi
OTT Ida Sulin

Toukokuu 2017

Avainsanat: henkilötiedot, rekisteri, henkilötietolaki, yksityisyys, EU-tietosuoja-asetus,
rekisterinpitäjä, henkilötietojen käsittelijä, rekisteröity

Tämän tutkimuksen tarkoituksena oli selvittää, miten rekisterinpitäjien vaatimukset
muuttuvat tietosuoja-asetuksen myötä. Lisäksi selvitettiin, mikä on rekisterinpitäjienä
toimivien kuntien, kuntayhtymien ja maakuntien liittojen nykytilanne suhteessa henkilö-
tietolakiin. Tavoitteena oli saada aikaan kehittämissuosituksia rekisterinpitäjiin kohdis-
tuvista tietosuojavaatimuksista.

Tutkimusmenetelminä olivat standardiperusteinen arviointi, sisällönanalyysi sekä sisäl-
lön erittely. Arviointia ja sisällönanalyysiä käytettiin tietosuoja-asetuksen ja henkilötie-
tolain vertailussa. Sisällön erittelyä hyödynnettiin kyselytutkimuksen vastauksen analy-
soinnissa. Tutkimuksen viitekehyksen muodostivat sosiaali- ja terveydenhuollon tie-
dönhallinnan paradigma sekä henkilötietoon, yksityisyyteen ja rekisterinpitoon liittyvät
käsitteet. Tutkimus asettui paradigmassa tiedon ja toiminnan väliseen tutkimusaluee-
seen, jossa mielenkiinnon kohteena on, miten tietoa hallitaan, organisoidaan ja ohjataan
erilaisissa toimintaprosesseissa.

Rekisterinpitäjiin kohdistuvat vaatimukset tulevat lisääntymään tietosuoja-asetuksessa.
Tutkittavien lähtötilanne henkilötietolain noudattamisen suhteen oli tyydyttävällä tasol-
la. Parhaiten oli huomioitu henkilötietojen käyttötarkoitus, käyttöoikeudet, asiakirjalli-
sen tiedon säilyttämisen periaatteet ja rekistereiden yhteyshenkilöt. Kehittämiskohteiksi
tulivat tietosuoja-asetuksen uusien asioiden kuten riskilähtöisen toiminnan, osoitusvel-
vollisuuden, oletusarvoisen ja sisäänrakennetun tietosuojan, tietoturvaloukkausmenette-
lyn, tietosuojavastaavan nimittämisen lisäksi muun muassa rekisteriselosteiden saata-
vuuden parantaminen, suostumusmenettelyn ohjeistaminen, ohjeistus henkilötietojen
käsittelijöille ja henkilötietojen luovutukset. Organisaatioiden tulisi pikaisesti käynnis-
tää kehittämisprojekti tietosuoja-asetukseen valmistumiseen, sillä tietosuoja-asetusta
sovelletaan 25.5.2018 lukien.

Jatkotutkimuksissa voisi keskittyä yhteen tietosuoja-asetuksen osa-alueeseen, esimer-
kiksi osoitusvelvollisuuteen, ja tutkia, miten sitä sovelletaan organisaatioissa.

UNIVERSITY OF EASTERN FINLAND, Faculty of Social Sciences and Business Studies, Department of Health Policy and Management, Health and Human Services Informatics

SEPPÖ, TUULA: The requirements for controllers in the General Data Protection Regulation (GDPR) of the European Parliament and the Council

Master's thesis, 81 pages, 6 appendices (37 pages)

Advisors: PhD Sirpa Kuusisto-Niemi
PhD Ida Sulin

May 2017

Keywords: personal data, register, Personal Data Act, privacy, General Data Protection Regulation (GDPR), controller, processor, data subject

The purpose of this research was to find out how the requirements for data controllers have changed with the adoption of the General Data Protection Regulation (GDPR). The research also examined the current practices of Finnish municipalities, joint municipal authorities and regions acting as controllers in terms of how well they comply with the national Personal Data Act. The aim was to formulate recommendations for controllers on how to improve their practices to better meet the data protection requirements.

The research methods used were standard based evaluation, content analysis and content differentiation. Evaluation and content analysis were used to compare the GDPR and the Finnish Personal Data Act, whereas content differentiation was useful in analysing the responses to the questionnaire survey. The frame of reference used as the background for this research consisted of the Health and Human Services Informatics and concepts related to personal data, privacy and data file maintenance. This research was positioned in a research area between data and action with a focus on information management, steering and organisation in different work processes.

The GDPR will increase the requirements on controllers. The research findings showed that the respondents' data security compliance was satisfactory. They paid most attention to the requirements related to purpose of use of personal data, access rights, principles of data file storage and contact persons for data files. New aspects of data security introduced by the GDPR were designated as development objectives, including risk-based approach, accountability, privacy by default and privacy by design, data breach notification and designation of the data protection officer. In addition, development objectives included better availability of the records of processing activities, instructions for consent procedure, instructions for processors, and disclosures. Organisations should urgently launch a development project for preparing for the GDPR, which has to be applied as of 25 May 2018.

Further research on the subject could focus on one aspect of the GDPR, for instance on accountability, and examine how it is applied in organisations.

SISÄLTÖ

1 JOHDANTO	7
2 LAINSÄÄDÄNNÖN KEHITYS	10
2.1 Euroopan ihmisoikeussopimus ja henkilötietolainsäädäntö	10
2.2 Julkinen tieto ja yksityinen tieto	12
2.3 Tietosuoja-asetus.....	13
2.4 Rekisterinpitäjän ja henkilötietojen käsittelijän velvollisuudet	14
3 TUTKIMUKSEN TAVOITE JA TARKOITUS	18
4 TIETO JA TIEDONHALLINTA	19
4.1 Tiedonhallinnan paradigma tutkimuksen taustana.....	19
4.2 Käsitteet teoreettisena viitekehyksenä	21
4.2.1 Henkilötietoon liittyvät käsitteet.....	21
4.2.2 Yksityisyyteen liittyvät käsitteet.....	25
4.2.3 Rekisterinpitoon liittyvät käsitteet	28
5 TUTKIMUKSEN AINEISTOT JA ANALYYSIMENETELMÄT	31
5.1 Tutkimuksen aineistot	31
5.2 Analyysimenetelmänä sisällönanalyysi ja sisällön erittely	34
5.3 Analyysimenetelmänä arviointi	37
5.4 Analyysimenetelmien valinta	39
6 TUTKIMUSTULOKSET JA YHTEENVETO	40
6.1 Tietosuoja-asetus selkeyttää	40
6.2 Tietosuoja-asetus täydentää	40
6.3 Tietosuoja-asetus tuo uutta.....	43
6.4 Yhteenveto tietosuoja-asetuksen vaatimuksista rekisterinpitäjälle.....	46
6.5 Kyselytutkimuksen tulokset	47
6.5.1 Taustakysymykset.....	47
6.5.2 Henkilötietojen käsittelyä koskevat yleiset periaatteet	50
6.5.3 Rekisteröidyn oikeudet.....	54
6.5.4 Rekisteriseloste	56
6.5.5 Tietosuojavastaava	58
6.5.6 Tietoturva ja riskienhallinta	59
6.5.7 Valmistautuminen tietosuoja-asetukseen	60
6.6 Yhteenveto arviointitutkimuksen ja kyselytutkimuksen tuloksista	65

6.6.1 Toimenpiteet ennen henkilötietojen käsittelyn aloittamista	66
6.6.2 Rekisterinpitäjään kohdistuvat kehittämistoimet	72
7 JOHTOPÄÄTÖKSET JA POHDINTA	75
7.1 Johtopäätökset.....	75
7.2 Tutkimuksen luotettavuus	78
7.3 Eettinen pohdinta	80
7.3 Jatkotutkimusaiheet.....	81
LÄHTEET.....	82
LIITTEET.....	87

LIITTEET

LIITE 1.	Yksityisyyden käsite Tavanin (2007) teorioita mukailien
LIITE 2.	Henkilötietolain ja tietosuoja-asetuksen arviointitaulukko
LIITE 3.	Yhteenveto henkilötietolain ja tietosuoja-asetuksen arvioinnista
LIITE 4.	Rekisteröidyn oikeudet
LIITE 5.	Kysely lähtötilanne EU-tietosuoja-asetukseen liittyvistä velvoitteista
LIITE 6.	Kehittämissuosituksen rekisterinpitäjille

KUVIOT

KUVIO 1.	Tutkimuksen vaiheet	9
KUVIO 2.	Henkilötietojen käsittelyn elinkaarimalli rekisterinpitäjän velvollisuuksista henkilötietolain mukaan.....	15
KUVIO 3.	Tietosuoja-asetuksen muutokset verrattuna nykyiseen henkilötietolakiin.....	16
KUVIO 4.	Sosiaali- ja terveydenhuollon tiedonhallinnan paradigma.....	20
KUVIO 5.	Henkilötietojen ja yksityiselämän suojan välinen suhde	28
KUVIO 6.	Analyysistä synteisiin	35
KUVIO 7.	Tietosuoja-asetuksen vaatimukset rekisterinpitäjälle	46

TAULUKOT

TAULUKKO 1.	Henkilötietolain ja tietosuoja-asetuksen rakenteet.....	32
TAULUKKO 2.	Kyselylomakkeen ryhmittely	33
TAULUKKO 3.	Vastausten jakautuminen kuntakoon mukaisesti	48
TAULUKKO 4.	Vastaajien asema kaikki organisaatiot.....	49
TAULUKKO 5.	Henkilötietojen tai tiedonhallinnan huomiointi strategiassa tai kehittämistoiminnassa kaikki organisaatiot	49
TAULUKKO 6.	Onko määritelty kenellä on oikeus käsitellä henkilötietoja	50
TAULUKKO 7.	Kaikkien vastaajien vastaukset koskien organisaation ohjeistusta ..	51
TAULUKKO 8.	Ohjeistuksen olemassaolo eri organisaatiotyypeittäin	51

TAULUKKO 9.	Ulkopuolisten ohjeistus henkilötietojen käsittelystä	52
TAULUKKO 10.	Henkilötietojen käyttötarkoitus	53
TAULUKKO 11.	Käsitteletkö arkaluonteisia henkilötietoja organisaatiotyypeittäin.....	53
TAULUKKO 12.	Onko organisaatiossanne ohjeistusta arkaluonteisten henkilötietojen käsittelystä	54
TAULUKKO 13.	Kaikki vastaajat rekisteröidyn informoinnista	55
TAULUKKO 14.	Kaikki vastaajat organisaation ohjeistuksesta.....	56
TAULUKKO 15.	Onko rekisteriselosteet tehty	56
TAULUKKO 16.	Onko rekisterien yhteyshenkilö määritelty	57
TAULUKKO 17.	Ovatko rekisteriselosteet rekisteröityjen saatavilla	58
TAULUKKO 18.	Tietosuojaavastaava on nimetty ja tehtävät määritelty	59
TAULUKKO 19.	Onko olemassa ohje tai onko nimitetty tietoturvapäällikkö	60
TAULUKKO 20.	Oletko tietoinen tietosuoja-asetuksesta	61
TAULUKKO 21.	Tietosuoja-asetuksen vaatimat kehittämistoimet aloitettu tai suunnitteilla	62
TAULUKKO 22.	Oletteko tietoinen VAHTI-ohjeesta	63
TAULUKKO 23.	Oletteko osallistuneet tietosuojakoulutukseen	63
TAULUKKO 24.	Mihin asioihin kaipaat eniten tukea tietosuoja-asetuksessa.....	64
TAULUKKO 25.	Toimenpiteet ennen henkilötietojen käsittelyn aloittamista	68
TAULUKKO 26.	Toimenpiteet henkilötietojen käsittelyn aikana	69
TAULUKKO 27.	Toimenpiteet käsittelyn perusteen lakattua ja ylläpitovaihe.....	71

1 JOHDANTO

Ihmisten, tavaroiden ja palveluiden vapaa liikkuvuus, teknologian nopea kehitys älysovelluksineen, verkko-ostosten lisääntyminen ja globaali toimintaympäristö ovat lisänneet voimakkaasti henkilötietojen käyttöä. Nykyiset tietosuojaa koskevat säädökset perustuvat vuoden 1995 EU-direktiiviin (95/46/EY) koskien yksilöiden suojelua henkilötietojen käsittelyssä ja näiden tietojen vapaata liikkuvuutta. Direktiivin periaatteet, kuten sisämarkkinoiden toiminnan turvaaminen sekä yksilön perusoikeuksien ja vapauksien suojaaminen, ovat päteviä nykyaikanakin, mutta direktiivi on jäänyt jälkeen digitaalisesta ajasta. Lisäksi ongelmia on tullut siitä, että Euroopan alueella on 28 erilaista tietosuojaan liittyvää lakia. Tästä syystä tietosuoja-asetuksen (Euroopan parlamentin ja neuvoston yleinen tietosuoja-asetus (EU 2016/679, annettu 27 päivänä huhtikuuta 2016), luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus; myöhemmin tietosuoja-asetus), säätämisen lähtökohtana oli se, että tietosuojalainsäädäntöä halutaan kehittää Euroopan Unionin (myöhemmin EU) tasoiseksi. Tällä voidaan paremmin taata kansalaisten luottamus henkilötietojensa käyttöön ja yhtenäistää toimintatapoja unionin tasoisesti. (Euroopan komissio 2016; Tietosuojavaltuutetun toimisto 2016; Valtiovarainministeriö 2016; Nurmi 2016.)

Euroopan komission vuonna 2015 tekemän eurobarometrin (Euroopan komissio 2015a) mukaan 89 % (Suomessa 94 %) vastaajista pitää tärkeänä sitä, että henkilötietoja koskevat samat oikeudet ja suoja riippumatta palvelua tarjoavan viranomaisen tai yrityksen kotimaasta. 71 % (Suomessa 80 %) vastaajista on sitä mieltä, että henkilötietojen antaminen on jatkuvasti kasvavaa osa nykyelämää. Melkein 60 % (Suomessa 67 %) kokee, että tuotteiden ja palveluiden saamiseksi on pakko antaa henkilötietoja ja 43 % (Suomessa 48 %) kokee, että henkilötietoja on pakko antaa verkossa. Kyselyn mukaan tärkeäksi koetaan se, että henkilötietojen suojausta tulisi valvoa Euroopan unionin tasolla 45 % (Suomessa 36 %) tai kansallisella tasolla 42 % (Suomessa 54 %).

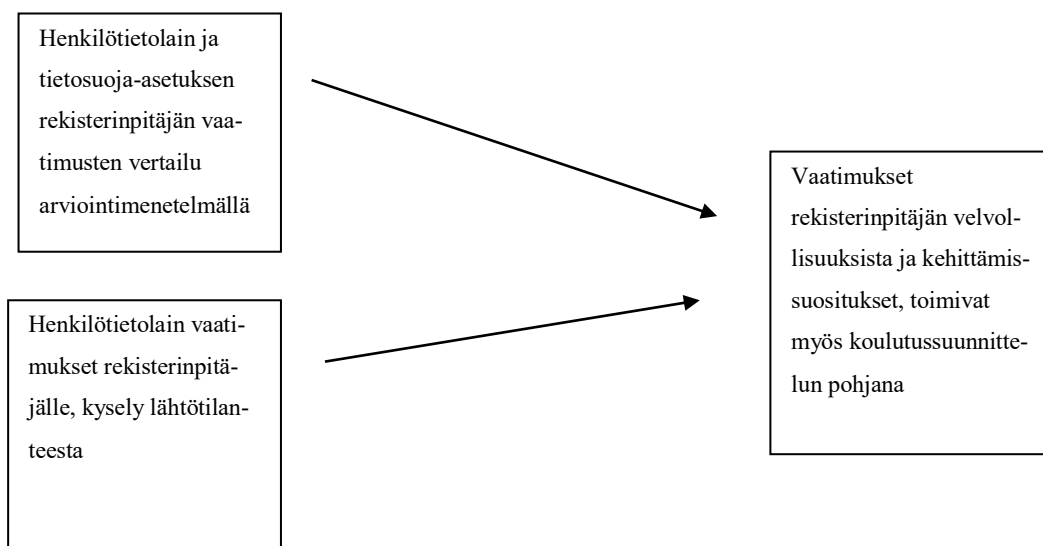
Tietosuoja-asetus on osa EU:n tietosuojauudistusta, johon kuuluu tietosuoja-asetuksen lisäksi direktiivi lainvalvontatarkoituksessa käsiteltävien henkilötietojen suojasta. Tietosuoja-asetus on suoraan sovellettavaa lainsäädäntöä, mutta se sisältää joitakin mahdolli-

suuksia kansalliseen sääntelyyn. Tietosuoja-asetuksella on tarkoitus vahvistaa muun muassa yksilön oikeuksia ja henkilötietojen vapaata liikkuvuutta jäsenvaltioiden välillä, yhdenmukaistaa lainsäädäntöä, vahvistaa EU:n sisämarkkinoiden toimivuutta, huomioida henkilötietojen suojan globaali ulottavuus sekä tehostaa valvontaa henkilötietojen käsittelyssä. Tietosuoja-asetusta sovelletaan 25.5.2018 lukien ja sillä kumotaan samasta päivästä alkaen direktiivi (95/46/EY) koskien yksilöiden suojelua henkilötietojen käsittelyssä ja näiden tietojen vapaata liikkuvuutta. (Nurmi 2016; Oikeusministeriö 2016a.)

Rekisterinpitäjän rooli ja merkitys lisääntyvät tietosuoja-asetuksen mukana. Merkittävä rooli rekisterinpitäjällä on ollut jo vuonna 1999 säädetyssä henkilötietolaissa (L523/1999, myöhemmin henkilötietolaki), mutta tietosuoja-asetuksen myötä rekisterinpitäjälle tulee lisää velvoitteita. Velvoitteita asetetaan suoraan myös henkilötietojen käsittelijälle. Tietosuoja-asetus tuo muutoksia, jotka selventävät, täydentävät tai tuovat uusia velvollisuuksia rekisterinpitäjälle ja henkilötietojen käsittelijöille. (Sulin 2016; Valtiovarainministeriö 2016.) Rekisterinpitäjän tulee huomioida muutokset omassa toiminnassaan; sen on muun muassa muutettava sellaisten palveluiden ostopalvelusopimukset, joissa käsitellään henkilötietoja, vastaamaan tietosuoja-asetuksen vaatimuksia. Lisäksi rekisterinpitäjälle tulee osoitusvelvollisuus. On näytettävä toteen se, miten asetuksen vaatimukset näkyvät toiminnassa ja ohjeissa. (Hoppu-Mäenpää 2016; Sulin 2016.) Tietosuoja-asetus aiheuttaa muutoksia valvontaviranomaisen, nykyisen tietosuojavaltuutetun, toimivaltuuksiin, sidosryhmiin, asiakkaisiin, työmenetelmiin, työkaluihin, päätöksentekojärjestelmiin ja toimenkuviin. EU-tasoinen sääntely tarkoittaa muun muassa sitä, että jokainen rekisteröity, joita Euroopan unionin alueella on noin 500 miljoonaa, voi jatkossa asioida halutessaan Suomen valvontaviranomaisen kanssa. Lisäksi valvontaviranomaisen tulee palvella kansallisten yritysten lisäksi ylikansallisia yrityksiä. (Aarnio 2016.)

Työskentelen Suomen Kuntaliitossa tiedonhallinnan erityisasiantuntijana ja käsittelen työssäni muun muassa henkilötietolakiin liittyviä kysymyksiä. Näen työssäni erilaisten sähköisen asiointipalveluiden sekä digitalisaation nopean kehityksen. Henkilötietojen suoja on tärkeää ottaa huomioon nopeasti muuttuvassa toimintaympäristössä. Nurmen (2016) mukaan olemme siirtymässä tietoyhteiskunnasta verkkoyhteiskuntaan, missä tieto liikkuu ja sitä käsitellään verkoissa. Rekisterinpitäjät ja henkilötietojen käsittelijät

ovat avainasemassa toteuttamassa rekisteröityjen oikeuksia. Tämän pro gradu -työn tarkoituksena on arvioida henkilötietolain ja tietosuoja-asetuksen rekisterinpitäjille kohdistettujen vaatimusten eroja sekä selvittää, kuinka kunnat, kuntayhtymät ja maakuntien liitot rekisterinpitäjinä noudattavat toiminnassaan voimassaolevaa henkilötietolakia. Tämä tehdään nykytilan kuvauksella. Nykytilan kuvaus pohjautuu henkilötietolaissa oleviin vaatimuksiin ja sen perusteella tehtävään kyselyyn kunnille, kuntayhtymille ja maakuntien liitoille. Tavoitteena on saada aikaan kehittämissuosituksia rekisterinpitäjille ja koulutuksen suunnittelijoille. Kehittämissuosituksia pohjautuvat tietosuoja-asetuksen ja henkilötietolain eroavaisuuksia mittaavaan arviointiin sekä saatuihin nykytilakuvauksiin. Tutkimuksen tulos on hyödyllinen rekisterinpitäjälle ja myös niille henkilötietojen käsittelijöille, joiden tulee noudattaa tietosuoja-asetuksen vaatimuksia. Tutkimus vaiheista, jotka on kuvattu kuviossa 1.



KUVIO 1. Tutkimuksen vaiheet

Ensimmäisessä vaiheessa arvioidaan rekisterinpitäjän velvollisuuksien eroavaisuuksia v henkilötietolain ja tietosuoja-asetuksen välillä. Toisessa vaiheessa tehdään selvitys kyselytutkimuksella kuntien, kuntayhtymien ja maakuntien liittojen (myöhemmin tutkittavien) nykytilasta. Kolmannessa vaiheessa arvioidaan, miten rekisterinpitäjä pääsee lähtötilanteesta tavoitetilaan, toisin sanoen, mitä rekisterinpitäjän tulee tehdä noudattaakseen asetuksen vaatimuksia. Näistä kolmesta osiosta muodostetaan kehittämissuositus rekisterinpitäjän ja henkilötietojen käsittelijän velvollisuuksista. Kehittämissuosituksia käytetään koulutussuunnittelun pohjana.

2 LAINSÄÄDÄNNÖN KEHITYS

Tässä luvussa kuvataan tietosuojalainsäädännön kehitystä Suomessa alkaen henkilörekisterilaista ja päättyen tietosuoja-asetukseen. Tietosuoja-asetuksen osalta kuvataan olennaisimmat muutokset rekisterinpitäjän velvollisuuksiin ja esitetään henkilötietolain mukaiset rekisterinpitäjän velvollisuudet tiedon elinkaaren eri vaiheissa. Luvussa käsitellään myös kahden perusoikeuden: oikeus saada tietää julkisesta asiakirjasta ja oikeus yksityisyyden suojaan, välisiä kysymyksiä.

2.1 Euroopan ihmisoikeussopimus ja henkilötietolainsäädäntö

Euroopan ihmisoikeussopimus muodostaa perustan Euroopan ihmisoikeuksille ja toimii Euroopan perusoikeusasiakirjan pohjana. (Council of Europe, 2014; Euroopan unioni 2017). Euroopan ihmisoikeussopimus ja Euroopan ihmisoikeustuomioistuimen ratkaisut ovat vaikuttaneet EU:n perusoikeusjärjestelmän kehitykseen. Sen 8. artiklan otsikkona on oikeus nauttia yksityis- ja perhe-elämän kunnioitusta. Kyseisessä artiklassa ei ole suoraa mainintaa henkilötietojen suojasta, mutta *Leander vs. Ruotsi* tuomion jälkeen henkilötietojen suojan on katsottu kuuluvan yksityisyyden suojan alle. (European Court of Human Rights 1987; Koillinen 2012, 177; Kivi 2016). Vaikutukset näkyvät sekä EU:n tulkintaratkaisuihin henkilötietojen suojaa koskevista asioista, että EU:n tietosuoja-oikeudessa. (Kivi 2016).

Euroopan tietosuojavaikuttetun Buttarellin (2015) mukaan henkilötietojen käsittelyn lainsäädäntö suojelee perusoikeuksia ja arvoja sekä yksilön oikeutta yksityisyyteen. Euroopan unionin perusoikeusasiakirjassa (2012/C326/02) 7. artiklassa säädetään yksityis- ja perhe-elämän kunnioittamisesta ja 8. artiklassa henkilötietojen suojasta. 8. artiklan mukaan jokaisella on oikeus henkilötietojen suojaan. Tietoja on käsiteltävä asianmukaisesti, käyttötarkoitussidonnaisesti ja asianomaisen henkilön suostumuksella tai laissa säädetyn oikeuden perusteella. Lisäksi jokaisella on oikeus tutustua omiin tietoihinsa ja saada virheelliset tiedot oikaistuksi. Riippumattoman viranomaisen on valvottava sääntöjen noudattamista. Vastaavasti Suomen perustuslain (L731/1999) 10 §:ssä koskien yksityiselämän suojaa säädetään, että jokaisen yksityiselämä, kunnia ja kotirauha on turvattu. Kirjeen, puhelun ja muun luottamuksellisen viestin salaisuus on louk-

kaamaton. Laissa säädetään lisäksi, että henkilötietojen suojasta säädetään erikseen lailla.

Suomessa ensimmäinen yksityisyyden suojaamista koskeva lainsäädäntö oli henkilörekisterilaki (L471/1987). Laki astui voimaan vuonna 1988. Tämän jälkeen säädettiin henkilötietolaki, lyhennettynä HeTiL (L523/1999), jolla EU:n henkilötietodirektiivi vuodelta 1995 (95/46/EY) saatettiin voimaan ja jolla kumottiin henkilörekisterilaki. Henkilötietolaki (HeTiL) on yleislaki, jota tulee noudattaa henkilötietojen automaattisessa käsittelyssä. Lisäksi lakia sovelletaan silloin, kun henkilötiedot muodostavat tai niiden on tarkoitus muodostaa henkilörekisteri tai sen osa. Lakia ei sovelleta sellaiseen henkilötietojen käsittelyyn, jota luonnollinen henkilö käyttää henkilökohtaisiin tarkoituksiin. Lain tarkoituksena on toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia. Perusoikeudeksi oikeus yksityiselämän suojaan tuli 1.8.1995. (Tietosuojavaltuutetun toimisto 2013; L523/1999.)

Suomen henkilötietolain 1 §:ssä säädetään henkilötietolain tarkoituksesta. Tarkoituksena on toteuttaa yksityiselämän suojaa ja muita yksityisyyden turvaavia perusoikeuksia henkilötietoja käsiteltäessä, sekä edistää hyvän tietojenkäsittelytavan kehittämistä ja noudattamista. Suomessa henkilötietojen suojaa säädetään myös muissa laeissa kuin henkilötietolaissa, ja näitä erityislakeja on noin 1000 kappaletta (Nurmi 2016). Niitä ovat esimerkiksi laki yksityisyyden suojasta työelämässä (L759/2004) ja laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (L159/2007).

Suomen henkilötietolain vaatimukset täyttävät Euroopan perustusasiakirjan kriteerit: jokaisen oikeus henkilötietojensa suojaan, asianmukaiseen henkilötietojen käsittelyyn, henkilötietojen käytön käyttötarkoitussidonnaisuuteen ja käsittelyn perustumiseen asianomaisen henkilön suostumukseen tai muussa laissa säädettyyn oikeuttavaan perusteseen. Jokaisella on oikeus tutustua hänestä kerättyihin tietoihin ja saada ne oikaistuiksi. Lisäksi riippumaton viranomainen, Suomessa tietosuojavaltuutettu, valvoo säädösten noudattamista. (Pitkänen, Tiilikka & Warma 2013, 27–39.)

2.2 Julkinen tieto ja yksityinen tieto

Suomessa on voimassa julkisuusperiaate, jonka mukaan viranomaisen asiakirjat ovat julkisia, joille laissa muuta säädetä. Viranomaistoiminnassa julkisuusperiaate tarkoittaa avoimuutta ja velvollisuutta tiedottaa. Poikkeukset julkisuusperiaatteesta edellyttävät aina erityisiä perusteita. Julkisuusperiaatteen vastakohta on salassapito. (Mäenpää 2016, 2-3.) Yksityisyyden ja julkisuuden välisen rajan määrittelee laki. Perustuslakivaliokunnan (PeVL) lausunnoissa henkilötietojen suojalla on korkea-asteinen suoja (Pitkänen ym. 2013). PeVL:n (14/2002) mukaan on tärkeää, että säädettäessä henkilötietojen suojasta säädetään ainakin rekisteröinnin tavoite, rekisteröitävien henkilötietojen sisältö, sallittu käyttötarkoitus, tietojen säilytysaika ja rekisteröidyn oikeusturvasta. Lisäksi PeVL (12/2002) on arvioinut tärkeäksi, että erikseen säädetään henkilötietojen luovuttamisesta teknisellä käyttöyhteydellä.

Suomen perustuslaki (L731/1999, 12.2.§) määrittelee viranomaisen asiakirjat ja tallenteet julkisiksi, jollei julkisuutta ole erikseen rajoitettu. Jokaisella on oikeus saada tietää julkisesta asiakirjasta tai tallenteesta. Henkilötietolaki ja julkisuuslaki linkittyvät toisiinsa siten, että julkisuuslaissa viitataan joissakin kohdissa henkilötietolakiin, esimerkiksi 21 § tietoaineistojen tuottaminen pyynnöstä ja 16 § asiakirjan antamistavat. Toisaalta taas henkilötietolaissa viitataan julkisuuslakiin (L621/1999), kuten 8 § käsittelyn yleiset edellytykset *”Oikeudesta saada tieto ja muusta henkilötietojen luovuttamisesta viranomaisen henkilörekisteristä on voimassa, mitä viranomaisten asiakirjojen julkisuudesta säädetään.”*

Kansalaisilla on näin ollen oikeus saada tietää viranomaisen julkisista asiakirjoista, mutta myös perusoikeus yksityisyyden suojaan. Kautto ja Henttonen (2017) ovat määritelleet näiden kahden oikeuden välistä suhdetta tavoiksi, joilla organisaatiot tiedottavat kansalaisia heidän oikeudestaan saada tietää viranomaisen hallussa olevasta digitaalisesta ja analogisesta julkisesta tiedosta sekä miten viranomaiset informoivat yksityisyyden suojaan liittyvistä käytännöistä. Tietosuoja-asetus tuo Suomessa painetta kehittää tiedonhallinnan sääntelyä ja arviointia kokonaisuudessaan (Valtioneuvosto 2016). Julkisen hallinnon tiedonhallintaa koskeva yleislainsäädäntö on pääosin 1990-luvulta. Sitä on muun muassa laki (L621/1999) ja asetus (A1030/1999) viranomaisen toiminnan julki-

suudesta, arkistolaki (L831/1994), laki sähköisestä asioinnista viranomaistoiminnassa (L13/2003) ja laki julkisen hallinnon tietohallinnon ohjauksesta (L634/2011).

Tiedonhallintaa koskeva lainsäädännön rakenne on epäselvä, eikä se ole kaikilta osin käyttäjien hallinnassa (Voutilainen, Oikarinen & Vartiainen 2016), minkä vuoksi valmistelussa on lainsäädännön uudistaminen. Uuden tiedonhallintalain suunniteltu voimaantulo on vuonna 2018. Eri laeissa olevat yleissäännökset on tarkoitus säätää yhtenäistävasti koskien tiedonhallintaa, julkisuutta ja sen käyttöä sekä arkistointia. Tarkoitus on vahvistaa yhtenäinen tiedon hallinnan, tietovarantojen hyödyntämisen ja kansalaisen oikeuksien toimintamalli sekä mahdollistaa julkisten palveluiden digitalisointi. (Valtioneuvosto 2016.)

2.3 Tietosuoja-asetus

Toukokuun 25. päivänä vuonna 2018 lähtien sovellettava tietosuoja-asetus tulee suoraan velvoittavaksi lainsäädännöksi Suomessa ja kaikissa EU-maissa. Sitä sovelletaan kaikkien unionin alueella tapahtuvaan henkilötietojen käsittelyyn riippumatta rekisterinpitäjän kotimaasta. Tietosuoja-asetus koskee sekä julkista että yksityistä sektoria, ja se antaa jonkin verran mahdollisuuksia kansallisiin täsmennyksiin. (Oikeusministeriö 2016b.) Oikeusministeriö on asettanut kansallisen työryhmän selvittämään kansallisten lainsäädäntötoimien ja erityisesti tietosuojan yleislain tarvetta, niin sanotun ”minihenkilötietolain” tarvetta. (Nurmi 2016). Työryhmän tehtävänä on selvittää kansallista tietosuojan valvontaviranomaista koskevaa sääntelyä, tehdä linjauksia kansallisesta liikkumavarasta tietosuoja-asetuksessa sekä koordinoita ja avustaa erityislainsäädännön tarkistamisessa. Työryhmän tulee saada mietintönsä muutosehdotuksista valmiiksi 31.5.2017 mennessä. Työryhmän toimikausi kestää 16.2.2018 asti. (Oikeusministeriö 2016b; Nurmi 2016.)

Tietosuoja-asetuksella vahvistetaan säännöt luonnollisten henkilöiden suojelulle sekä henkilötietojen vapaalle liikkuvuudelle. Suojelun kohteena ovat erityisesti luonnollisten henkilöiden perusoikeudet ja -vapaudet ja oikeus henkilötietojen suojaan. Tietosuoja-asetuksella parannetaan kansalaisten mahdollisuutta omien tietojensa valvontaan ja tarkastamiseen. Tavoitteena on vähentää kansallista sääntelyä ja suojata henkilötiedot yhtäläisesti riippumatta yrityksen tai organisaation kotipaikasta, yksi maanosa ja yksi lain-

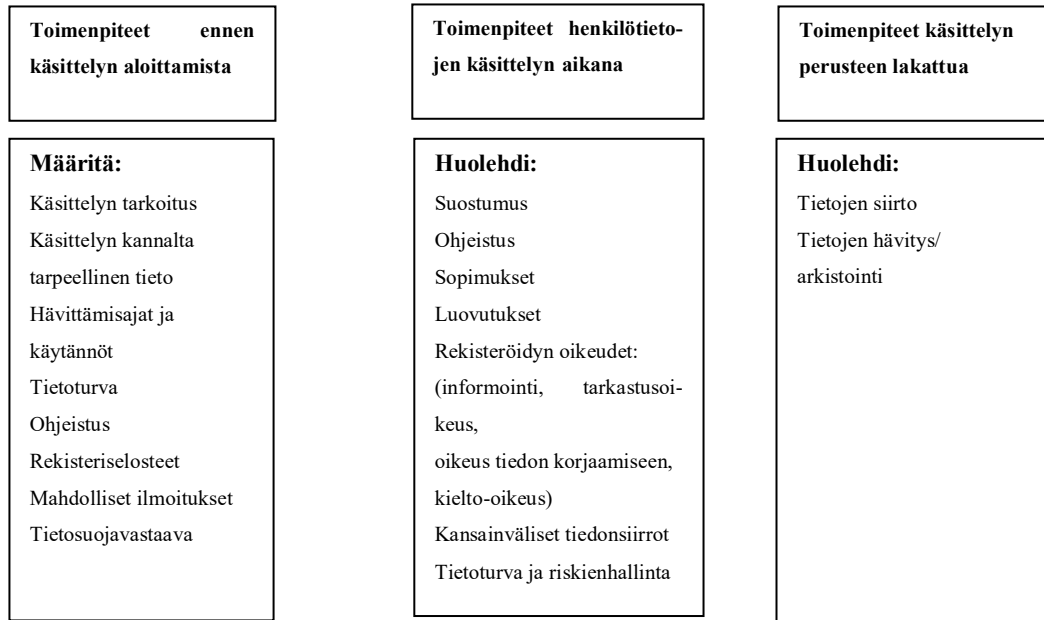
säädäntö -periaatteella. Kansalaisten pääsy omiin tietoihinsa helpottuu ja joissakin tapauksissa kansalaiselle tulee oikeus tulla unohdetuksi. Kansalaisille tietosuoja-asetus näkyy myös henkilön oikeutena siirtää tietoja palveluntarjoajalta toiselle. Lisäksi vahvistetaan ilmoittamismenettelyä vakavien tietoturvaloukkauksien suhteen. Yritykset voivat jatkossa asioida yhden valvontaviranomaisen kanssa; puhutaan niin sanotusta yhden luukun periaatteesta. Lisäksi eri maiden valvontaviranomaisten yhteistyö tiivistyy. (Euroopan komissio 2015b; Euroopan komissio 2016.)

Organisaatioiden toimintaedellytykset tasaantuvat, sillä tietosuoja-asetus koskee myös Euroopan ulkopuolisia yrityksiä, jos yritykset tarjoavat palveluitaan EU:ssa. Buttarellin (2015) mukaan nykyistä lainsäädäntöä haluttiin täydentää sisäänrakennetulla ja oletusarvoisella yksityisyyden suojalla ja vastuuvollisuudella. Tietojärjestelmät ja palvelut on suunniteltava siten, että tietosuoja on huomioitu jo suunnitteluvaiheessa. Lisäksi uudistuksella kannustetaan massadatan hyödyntämiseen ja uusien innovaatioiden käyttöön. Yritykset voivat anonymisoinnilla ja pseudonymisoinnilla poistaa kokonaan tai häivyttää henkilötietoja. (Euroopan komissio 2015b; Euroopan komissio 2016.)

2.4 Rekisterinpitäjän ja henkilötietojen käsittelijän velvollisuudet

Henkilötietolain mukaan henkilötietoja on käsiteltävä huolellisesti, laillisesti ja noudattaen hyvää tietojenkäsittelytapaa. Henkilötietojen käsittelyn tulee olla suunniteltua, asiallisesti perusteltua sekä käyttötarkoitussidonnaista. Henkilötietoja koskevat tarpeellisuusvaatimus ja virheettömyysvaatimus. (L523/1999, 5-7, 9 §.) Rekisterinpitäjän on huolehdittava rekisteröidyn oikeuksista. Rekisterinpitäjän on informoitava rekisteröityä tietojen käsittelystä, tietojen käyttötarkoituksesta sekä siitä, mihin tietoja säännönmukaisesti luovutetaan ja miten rekisteröity voi käyttää oikeuksiaan. Rekisteröidyllä on oikeus tarkastaa omat tietonsa, saada virheelliset tiedot oikaistua ja oikeus kieltää henkilötietojensa käyttö muun muassa suoramarkkinointiin. (L523/1999, 24 §, 26 §, 29 §, 30 §.) Rekisterinpitäjän velvollisuus on suojata tiedot toteuttamalla tarpeelliset tekniset ja organisatoriset toimenpiteet (L523/1999, 32 §). Henkilötietolain mukaiset rekisterinpitäjän velvollisuudet voidaan kuvata Pitkäsen kollegoiveen kehittämällä (2013, 309) elinkaarimallilla (kuvio 2).

Mallissa rekisterinpitäjällä on erilaisia velvollisuuksia henkilötietojen käsittelyn eri vaiheissa. Käsittelyvaiheita ovat ennen henkilötietojen käsittelyä liittyvät valmistelut, toimenpiteet henkilötietojen käsittely aikana sekä toimenpiteet käsittelyn perusteen lakattua



KUVIO 2. Henkilötietojen käsittelyn elinkaarimalli rekisterinpitäjän velvollisuuksista henkilötietolain mukaan (Pitkänen ym. 2013, 309).

Tietosuojasetus tulee aiheuttamaan muutoksia rekisterinpitäjän toimintatavoissa ja tietojärjestelmissä. Rekisterinpitäjillä on noin vuosi aikaa muuttaa toimintaansa siten, että tietosuojasetuksen vaatimukset tulevat noudatetuksi. Tietosuojasetuksen 5., 6. ja 12. artiklan mukaisesti rekisterinpitäjän on käsiteltävä henkilötietoja niin, että se on laillista, asianmukaista ja läpinäkyvää. Rekisteröidyn on tiedettävä, miten henkilötietoja kerätään, käytetään, käsitellään tai on määrä käsitellä ja miten niihin pääsee tutustumaan. Rekisterinpitäjän on myös ilmoitettava mahdollisista riskeistä, säännöistä, suoja-toimista ja rekisteröidyn oikeuksista.

Kuvioon 3 on koottu tietosuoja-asetuksen keskeiset piirteet sen suhteen, miten ne poikkeavat henkilötietolain vaatimuksista. Osa muutoksista selkeyttää nykyistä toimintaa, osa täydentää toimintaa ja osittain tietosuoja-asetus tuo kokonaan uutta (Sulin 2016).

Selkeyttää nykyistä	Täydentää nykyistä	Kokonaan uutta
<ul style="list-style-type: none"> ▪ peruskäsitteet ▪ yleisperiaatteet ▪ käsittelyn oikeutus ▪ suostumus ▪ tarkastus- ja korjausoikeus ▪ oikeus tulla unohdetuksi ▪ riskiarvot korostuvat 	<ul style="list-style-type: none"> • tietosuojavastaavan asema • oikeus käsitellä – oikeutettu etu • informointivelvollisuus • käsittelijän roolin määrittely • lapsen asema • suoramarkkinointiin muutokset • henkilötietojen siirrot kolmansiiin maihin • profilointi 	<ul style="list-style-type: none"> • sisäänrakennettu ja oletusarvoinen tietosuoja • osoitusvelvollisuus • käsittelytoimintojen kuvaaminen • tietojen siirrettävyys • vaikutusten arviointi • ilmoitus loukkauksesta • ennakkohyväksyntä ja ennakkokuuleminen • sanktiot, hallinnolliset seuraamukset • viranomaisorganisaatio – one stop shop • korvausperusteet ml. vahingonkorvaus

KUVIO 3. Tietosuoja-asetuksen muutokset verrattuna nykyiseen henkilötietolakiin (Sulin 2016).

Ei riitä, että rekisterinpitäjä noudattaa asetusta, sen on voitava myös osoittaa asia eli rekisterinpitäjällä on osoitusvelvollisuus (*accountability*) (Valtiovarainministeriö 2016). Tietosuoja-asetus sisältää 25. artiklassa periaatteet sisäänrakennetusta (*privacy by design*) ja oletusarvoisesta (*privacy by default*) tietosuojasta. Ensimmäinen tarkoittaa, että henkilötietojen suoja on huomioitava kaikissa uusissa palvelu- ja tuotantoprosesseissa ja kyettävä todistamaan se. Toinen tarkoittaa, että tietosuoja on sisällytettävä palvelu- ja tuotantoprosesseihin ja oletusarvoisesti käsitellään vain tarpeellisia henkilötietoja. (Euroopan komissio 2015b.) Kyseessä on paradigman muutos: rekisterinpitäjille tulee näyttövelvollisuus (Sulin 2016).

Henkilötietojen käsittelijän velvollisuudet määritellään tietosuoja-asetuksessa laajemmin kuin henkilötietolaissa. Käsittelijä on tietosuoja-asetuksen mukaan luonnollinen henkilö, oikeushenkilö, viranomainen, virasto tai muu elin, joka käsittelee henkilötietoja rekisterinpitäjän lukuun. (Tietosuoja-asetus, 4 art., 28 art.) Henkilötietojen käsittelijän velvollisuuksiin kuuluu huolehtia rekisteröidyn oikeuksien toteuttamista. Käsittelijän velvollisuuksiin kuuluu toimia rekisterinpitäjän ohjeiden ja tehdyn sopimuksen mukaisesti ja sen on varmistettava riittävät suojatoimet asianmukaisten teknisten ja organisatoristen toimien täytäntöönpanemiseksi. Käsittelijää sitoo salassapitovelvollisuus, ja tietoturvaloukkauksista on ilmoitettava ilman aiheetonta viivytystä rekisterinpitäjälle. (Tietosuoja-asetus, 28 art., 29 art. ja 33 art.)

Tietosuoja-asetuksen myötä valvontaviranomainen voi määrätä hallinnollisia seuraamuksia tai hallinnollisia sakkoja. Sakkojen määrä voi olla enintään 10–20 miljoonaa euroa tai 2-4 prosenttia edeltävän tilikauden vuotuisesta maailmanlaajuisesta kokonaisliiknevaihdesta. Sakkojen määrään vaihtelu riippuu muun muassa rikkomuksen luonteesta, vakavuudesta, kestosta, rikkomisen tahallisuudesta tai tuottamuksellisuudesta. (Tietosuoja-asetus, 83–84 art.) Vaatimusten täyttäminen tuo kustannuksia rekisterinpitäjälle. Sen on muun muassa nimitettävä tietosuojavastaava, luotava prosessit tietoturvaloukkauksista ilmoittamiselle ja muutettava sopimuksiaan koskien tietojärjestelmähankintoja. (Hoppu-Mäenpää 2016; Valtiovarainministeriö 2016.)

3 TUTKIMUKSEN TAVOITE JA TARKOITUS

Tämän tutkimuksen kohteena ovat kunnat, kuntayhtymät ja maakuntien liitot (tutkittavat) rekisterinpitäjinä. Ne käsittelevät henkilötietoja suorittaessaan sekä julkis- että yksityisoikeudellisia tehtäviä ja ovat vastuussa henkilötietojen käsittelystä. Tarkoituksena on arvioida henkilötietolain ja tietosuoja-asetuksen eroja rekisterinpitäjän vaatimuksissa sekä selvittää tutkimuksen kohteena olevien nykytila suhteessa henkilötietolakiin; miten henkilötietolain vaatimukset rekisterinpitäjiä kohtaan toteutuvat. Tutkimuksen tavoitteena on saada aikaan kehittämissuosituksen. Kehittämissuosituksen pohjautuvat sekä nykytilannekuvaukseen että henkilötietolain ja tietosuoja-asetuksen väliseen arviointiin. Arviointi pohjautuu kolmeen näkökulmaan, mikä tietosuoja-asetuksessa selkeytyy, mikä täydentyy ja mikä on kokonaan uutta suhteessa henkilötietolakiin. Kehittämissuosituksista rekisterinpitäjät saavat konkreettisia apuvälineitä oman toimintansa kehittämiseen ja koulutusten suunnitteluun. Tämän pro gradu -työn tarkoituksena on saada vastaus seuraavaan tutkimuskysymykseen:

Miten rekisterinpitäjien vaatimukset muuttuvat tietosuoja-asetuksen myötä?

Tässä tutkimuksessa keskitytään kunnallisen julkishallinnon rekisterinpitäjää ja osittain henkilötietojen käsittelijöitä koskeviin vaatimuksiin. Sosiaali- ja terveydenhuoltoalat ovat tutkimuksen ulkopuolella, koska muun muassa tietosuojavastaavan nimittäminen on ollut pakollista sosiaali- ja terveydenhuollossa jo vuodesta 2007 (kts. L61/2007 ja L159/2007). Lisäksi tutkimuksen ulkopuolelle rajataan Ahvenmaa, koska siellä noudatetaan eri henkilötietolakia kuin manner-Suomessa. Tutkimuksessa ei tarkastella kaikkia tietosuoja-asetuksen määritelmiä, vaan päähuomio kiinnitetään henkilötietolain mukaisien määräysten toteuttamiseen. Tavoitteena ei ole antaa yksityiskohtaisia ohjeita siitä, mitä tietosuoja-asetuksen vaatimukset tarkoittavat käytännössä, vaan tutkimuksessa keskitytään siihen, mitä rekisterinpitäjän tulee huomioida.

4 TIETO JA TIEDONHALLINTA

Tässä luvussa kuvataan tutkimuksessa käytettävä viitekehys sekä määritellään tutkimuksen kannalta merkittävät käsitteet. Teoriat muodostavat tieteellisen tutkimuksen työkalun. Tutkimuksen teoreettinen viitekehys tarjoaa näkökulman, jonka läpi havaintoja tarkastellaan. Se määrittelee kerättävän aineiston luonteen ja sen, miten aineistoa tulee käsitellä. Toisaalta aineisto voi määritellä teoreettisen viitekehysten ja sen, millaisia metodeja voidaan käyttää. (Alasuutari 2011, 79–89.) Tutkimuksessa on määriteltävä käsitteet, ne ovat työkaluja tutkimukselle. Käsitteet kuvaavat tutkittavaa ilmiötä; ne määrittelevät, nimeävät ja antavat merkityksen tutkittavalle ilmiölle. Termit ja käsitteet sitovat tutkimuksen teoreettiseen keskusteluun. (Ronkainen, Pehkonen, Lindblom-Yläne ja Paavilainen 2011, 53.)

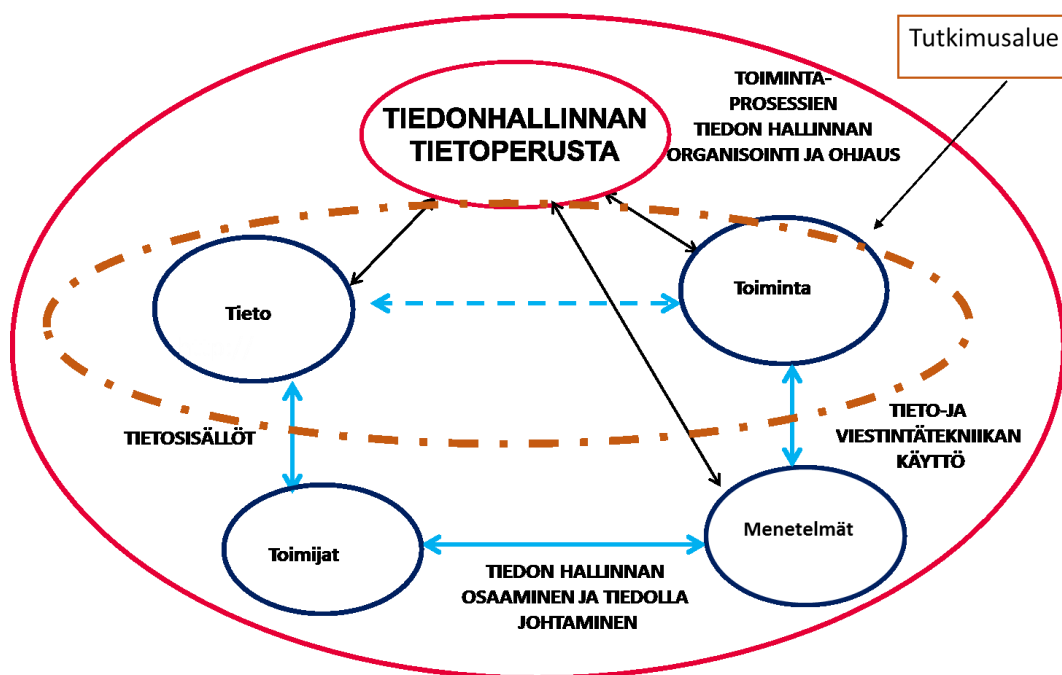
Teoreettisen viitekehysten tutkimukselle tarjoavat toisaalta sosiaali- ja terveydenhuollon tiedonhallinnan paradigma ja toisaalta tutkimuksen kannalta merkittävät käsitteet. Näiden avulla tutkimus sidotaan tiettyyn viitekehykseen, jonka läpi ilmiötä tarkastellaan. Tämän tutkimuksen keskeiset käsitteet ovat henkilötieto, yksityisyys ja rekisteri. Tutkimuksessa mielenkiinnon kohteena on henkilötieto ja miten se nivoutuu yhteen rekisterinpitäjän toiminnan kanssa.

4.1 Tiedonhallinnan paradigma tutkimuksen taustana

Tieteellisen tutkimuksen oleellinen osa on paradigma. Se kuvaa tiedeyhteisön jakamaa käsitystä tieteellisen tiedon olemuksesta ja tiedon keskeisistä kriteereistä. Paradigmalla otetaan kantaa siihen, minkälaisia ilmiöitä voidaan tutkia, millaiset kysymykset ovat tutkimuksellisesti tärkeitä ja millaiset tutkimustavat ovat hyväksytyjä. (Ronkainen ym. 2011, 26–29.) Paradigma ohjaa tieteellistä tutkimusta (Kuhn 1962, 48–51; Wray 2011).

Sosiaali- ja terveydenhuollon tiedonhallinnan (*Health and Human Services Informatics*) paradigma (Kuvio 4) koostuu neljästä ulottuvuudesta (tieto, toiminta, menetelmät ja toimijat). Tiedonhallinnan tutkimus on monitieteinen kokonaisuus, jonka taustatieteinä ovat muun muassa luonnontieteet, hallintotieteet, yhteiskuntatieteet ja terveystieteet.

Paradigmassa **tieto** on hierarkinen jatkumo datasta viisauteen. Tieto muodostaa arvoketjun, jossa verkostomaisuus ja kompleksisuus lisääntyvät, kun siirrytään datasta yhä jalostetumpaan muotoon. **Menetelmät** pitävät sisällään tietojen käsittelyyn, tallentamiseen ja välittämiseen liittyvät tekniset ja sosiaaliset toimintatavat. **Toiminta** on palvelujen suunnittelua, toteutusta, käyttöä ja arviointia. **Toimijat** ovat niitä, jotka käyttävät tai tuottavat palveluita. Tutkimusalueet muodostuvat näiden neljän **ulottuvuuden** välisissä suhteissa. Tiedon ja toiminnan välillä tutkitaan toimintaprosesseja, toiminnan ja menetelmien tutkimuskohde on tieto- ja viestintäteknikan käyttö. Osaamisen ja tiedolla johtamisen tutkiminen kuuluu menetelmien ja toimijoiden väliseen kenttään ja kun tutkitaan tietosisältöä ja tietoperustaa on kyseessä tiedon ja toimijoiden välinen suhde. (Saranto & Kuusisto-Niemi 2012.)



KUVIO 4. Sosiaali- ja terveydenhuollon tiedonhallinnan paradigma (Saranto & Kuusisto-Niemi 2012).

Tämä pro gradu -työ kuuluu tiedon ja toiminnan väliseen tutkimusalueeseen. Mielenkiinnon kohteena on, miten tietoa hallitaan, organisoidaan ja ohjataan erilaisissa toimintaprosesseissa. Henkilötietolain ja tietosuojasetuksen mukaisesti rekisterinpitäjän ja käsittelijän tulee hallita henkilötietoa, organisoida sen käyttö ja ohjata henkilötietoa

koko sen elinkaaren ajan. Henkilötietolain ja tietosuoja-asetuksen määräykset ilmenevät toimintaprosesseissa ja niiden kehittämisessä.

4.2 Käsitteet teoreettisena viitekehyksenä

Tämän tutkimuksen keskeiset käsitteet ja samalla työkalut tutkimukselle ovat henkilötietoon, yksityisyyteen ja rekisterinpitoon liittyvät käsitteet. Käsitteiden avulla voidaan asioita hahmottaa teoreettisella tasolla (Hirsjärvi, Remes & Sajavaara 2007, 142–143) ja niiden avulla tutkimustyöstä tulee tutkimus (Pohjola 2003, 61–62). Käsitteiden avulla ilmiö tulee ymmärrettäväksi (mt.). Tässä tutkimuksessa ilmiönä ovat rekisterinpitäjään liittyvät velvollisuudet henkilötietoja käsiteltäessä. Nämä velvollisuudet tulevat lain ja asetusten määräyksistä. On olennaista ymmärtää henkilötietoon, yksityisyyteen ja rekisterinpitoon liittyvät käsitteet, jotta voi ymmärtää ilmiötä.

4.2.1 Henkilötietoon liittyvät käsitteet

Tässä tutkimuksessa keskeisiä henkilötietoon liittyviä käsitteitä ovat tieto, henkilötieto, anonymisoitu ja pseudonymisoitu tieto. Suomalaisen sivistyssanakirjan mukaan **tieto** on tietämistä, tietoisuutta, todellisuuteen tai tosiasioihin perustuvaa käsitystä jostakin asiasta tai asia tai seikka, joka tiedetään. Platonin (kirjassa Niiniluoto 2003, 32) määritelmä tiedosta on, että se hyvin perusteltu tosi uskomus. Tieto on totta tai ainakin totuudenkaltaista ja sillä on perustelu tai oikeutus. Niiniluodon (1996, 58) mukaan klassisen tiedon määritelmän voi tiivistää ajatukseen, että tieto on väitelauseiden sisältämää semanttista informaatiota, joka täyttää perusteluehdon ja totuusehdon.

Niiniluodon (mt., 60) oma käsitys tiedosta edustaa kriittistä tieteellistä realismia. Siinä tieto muodostuu niistä väitteistä, joille on toistaiseksi paras perustelu. Niiniluodon (mt.) käsityksessä tiedon totuutta saatetaan epäillä ja olla epäilyssä oikeassa. Tieto paranee; se tulee totuudenkaltaiseksi, kun saadaan uutta todistusaineistoa, uusia käsitteitä tai teorioita, sillä Niiniluodon (2003, 32) mukaan kaikki inhimillinen tieto on erehtyväistä, korjattavissa ja parannettavissa. Ronkaisen kollegoineen (2011, 17) mukaan tieteen tekemisessä totuuksiin ei saa kiintyä. Tieto on perustelluin käsitys tutkittavasta asiasta. Tietty epävarmuus tiedon totuudesta on aina läsnä. Niiniluoto (1996, 60) toteaa, että tieteen

tehtävänä on korjata arkitietoon liittyvää ”ilmikuvaa” ja antaa maailmasta ”tieteellinen kuva”. Tieteessä lähestytään totuutta.

Suurla (2001, 31–32) kuvaa tiedon hierarkian rappusilla, jossa ensimmäisellä askeleella on data, toisella informaatio, kolmannella tieto, neljännellä ymmärrys ja viimeisellä viisaus. Data voi olla koodi, merkki tai signaali. Se on raaka-ainetta informaatiolle ja tiedolle. Informaatio on seuraava taso, johon liittyy jo merkitystä tai tulkintaa. Tämän jälkeen syntyy tieto, joka on ymmärrettävää ja omaksuttavaa. Suurla (mt.) käyttää tiedosta myös nimitystä tietämys silloin, kun informaatio prosessoituu osaksi ihmisen tiedollista rakennetta. Niiniluoto (1996, 61) näkee tietämyksen käytettävissä olevien tai hyväksytyjen tietojen kokonaisuudeksi. Tietämys on näin ollen laajempaa kuin tieto tai informaatio. Ymmärrys saavutetaan tiedon muokkaantuessa kokemuksissa ja viisaus on metaymmärrystä, jolla luodaan uutta (Suurla 2001, 31–33). Niiniluodon (1996, 62) mukaan tietämys, teoria ja viisaus tuovat tietoon leveyttä, järjestystä ja syvyyttä. Yksistään tiedon määrän lisääntyminen ei kuitenkaan tuo viisautta. Viisaus on asioiden laajempi yhteys ja merkitys, käsitys siitä miten tietoa hankintaan, kuinka luotettavaa tieto on sekä miten punnittua ja kokemusperäistä tieto on. Viisaus pohjautuu arvioihin hyvän elämän päämääristä.

Tässä tutkimuksessa tieto on olennaista; lakien, asetusten, sääntöjen ja erilaisten ohjeiden noudattamiseen vaaditaan tietoa. Tieto yksistään ei kuitenkaan riitä, vaan rekisterinpitäjällä ja käsittelijällä tulee olla kokemusperäistä tietämystä asioista ja niiden merkityksestä toimintaan. Tieto muokkaantuu tietämykseksi ja ymmärrykseksi ja siirtyy rekisterinpitäjän toimintaan ja toimintaprosesseihin. Kun tieto yhdistyy kokemusperäiseen toimintaan, rekisterinpitäjä ja käsittelijä pystyvät vastaamaan siitä, miten lain säännökset näkyvät toiminnassa.

Henkilötiedon käsite on keskeinen käsite ymmärtää, kun käsitellään henkilötietoja (Pitkänen ym. 2013, 40–51). Henkilötietodirektiivin 2. artiklassa (95/46/EY) määritellään henkilötiedoksi kaikenlaiset tunnistettua tai tunnistettavissa olevaa luonnollista henkilöä koskevat tiedot. Tunnistaminen voi tapahtua suoraan tai epäsuorasti. Tunnistetietoja ovat erityisesti henkilönumero tai sellaiset tunnistetiedot, joilla henkilö pystytään tunnistamaan yhden tai useamman tunnusomaisen fyysisen, fysiologisen, psyykkisen,

taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella. Henkilötietodirektiivin (95/46/EY) 26. kappaleessa määritellään, että tietosuojaperiaatteita sovellettaessa on otettava huomioon kaikki kohtuullisesti toteutettavissa olevat keinot, joita joko rekisterinpitäjä tai joku muu voi käyttää kyseisen henkilön tunnistamiseksi. Esimerkiksi ajoneuvon rekisterinumero on henkilötieto, koska henkilö voidaan kohtuullisin kustannuksin tunnistaa esimerkiksi puhelintiedustelun avulla. (Tietosuojalautakunta 2010.)

Henkilötietolain 3 §:n mukaan henkilötietoa ovat kaikki ne luonnollista henkilöä, hänen ominaisuuksiaan tai elinolosuhteitaan kuvaavat merkinnät, joista hänet tai hänen perheensä tai hänen kanssaan elävät voidaan tunnistaa. Henkilötiedon määritelmä on laaja ja tarkoittaa, että kaikki luonnollista henkilöä koskevat tiedot kuuluvat henkilötietolain piiriin. Lisäksi henkilötietoon luetaan muun muassa henkilön toiminta ammatin- ja elinkeinonharjoittajana taikka julkiseen tehtävään liittyvä tieto. Merkitystä ei ole sillä, mihin välineeseen ja millä tavalla tieto on tallennettu. Tieto voi olla esimerkiksi paperilla, tietojärjestelmässä, äänitiedostossa, valokuvana, graafisessa muodossa tai optisesti luettavissa. (Pitkänen ym. 2013, 40–51.)

Tietosuoja-asetus määrittelee henkilötiedoksi kaikki tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyvät tiedot. Tunnistaminen voi tapahtua suoraan tai epäsuorasti. Tunnistetietoja ovat nimi, henkilötunnus, sijaintitieto ja verkkotunnistetieto. Lisäksi tunnistetiedoksi katsotaan sellaiset tiedot, joista luonnollinen henkilö voidaan tunnistaa yhden tai useamman tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurisen tai sosiaalisen tekijän perusteella. (Tietosuoja-asetus, 4 art.)

Marz (1999) kiteyttää henkilötiedon käsitteen sanomalla, että henkilökohtaiseen tietoon kuuluu kaikki se informaatio, jolla voidaan tunnistaa luonnollinen henkilö. Näitä ovat muun muassa nimi, olinpaikka, mahdollinen pseudonyymi (peitenimi), sosiaalinen status tai tieto tavoista tai piirteistä, kuten esimerkiksi uniformut ja merkit. Henkilötietoja ovat esimerkiksi henkilötunnus, sormenjälki, auton rekisteritunnus, valokuva, bonuskortin tiedot, tietokoneen IP-osoite tai katuosoite. Henkilö voidaan tunnistaa tiedoista joko suoraan, kuten henkilötunnuksen avulla, tai epäsuorasti. Epäsuorasti henkilö voidaan tunnistaa yhdistämällä tieto muihin tietoihin. (Pitkänen ym. 2013, 40–47.) Esimerkiksi

”tietyn pienen kylän ainut punatukkainen nainen” on tieto, jonka perusteella henkilö on mahdollisuus tunnistaa ja on näin ollen henkilötieto.

Anonymisoidulla tiedolla tarkoitetaan sellaista henkilötietoa, josta on poistettu tunnistettavat elementit teknisillä tai muilla toimenpiteillä. Anonymisointi on lopullista eikä sitä voi peruuttaa. (Tietosuojaryhmä WP29, 2014.) Aarnio (2015) toteaa lausunnossaan, että *”henkilötietojen anonymisointi on itsessään henkilötietojen käsittelyä”*. Hän korostaa, että anonymisointi pitää tehdä niin, ettei *”yksittäinen rekisteröity ole sieltä varmuudella välillisesti tunnistettavissa edes omasta toimestaan.”* Henkilötietodirektiivin perusteella (95/46/EY, 29–30 art.) asetettu tietosuojaryhmä WP29, jonka tehtävänä on antaa lausuntoja, ohjeita ja neuvoja tietosuoja-asioissa (WP29, 2010.) Tietosuojaryhmä WP29 (2014) on lausunut, että anonymisointia ei tehdä vain kerran, vaan rekisterinpitäjän on voitava arvioida, että tiedot pysyvät tosiasiallisesti anonyymeinä. Tiedot ovat tosiasiallisesti anonyymejä vain, mikäli anonymisointi on viety tehtävätasolle asti. Esimerkiksi yrityksen keräämissä matkustustiedoissa pelkkä henkilötietojen poisto ei riitä, lisäksi on poistettava yksittäisiä matkoja koskevat tiedot. Erilaisten tietojen yhdistämisessä anonymisoitu tieto voi muuttua tunnistettavaksi; sen takia arviointia tietojen anonymisoinnin pysyvyydestä on tehtävä jatkuvasti. (mt.)

Anonymisointitekniikoihin sisältyy erilaisia riskejä. Näitä ovat erottaminen joukosta (yksilön pystyy erottamaan jostakin tiedosta), yhdistettävyyden puuttuminen (henkilö pystytään tunnistamaan yhdistämällä tietoja) ja päättely (henkilö pystytään tunnistamaan päättelyllä). Rekisterinpitäjän tulee ottaa huomioon eri tekniikoihin liittyvät riskit, ja varmistaa, että anonymisoitu henkilötieto ei missään vaiheessa saa tulla kenenkään tietoon. (mt.)

Pseudonymisoitu tieto on henkilötietoa, jota on käsitelty niin, ettei henkilötietoja voida yhdistää rekisteröityyn ilman jotain attribuuttia. Tällaisia attribuutteja ovat esimerkiksi salausavaimet ja erilaiset merkit. Kyseessä on kuitenkin henkilötietojen käsittely, koska tunnistettavuus on todennäköistä. Näin ollen rekisterinpitäjän on noudatettava henkilötietolainsäädäntöä. Ongelmia saattaa tulla, jos rekisterinpitäjä luulee pseudonymisoitua dataa anonymisoiduksi. (WP29, 2014; Aarnio 2015.) Tietosuoja-asetus määrittelee 4. artiklassa pseudonymisoinnin sellaiseksi henkilötietojen käsittelyksi, jossa henkilötietoja ei voi enää yhdistää tiettyyn rekisteröityyn ilman lisätietoja. Tämä edellyttää, että

lisätietoja säilytetään erillään rekisteröidyn tiedoista ja niihin sovelletaan sellaisia teknisiä ja organisatorisia toimenpiteitä, joilla varmistetaan, ettei henkilötietojen yhdistämistä tapahdu. Tietosuoja-asetuksen kertomusosiossa 28. kappaleessa todetaan, että pseudonymisoinnilla voidaan vähentää rekistereihin kohdistuvia riskejä sekä auttaa rekisterinpitäjiä ja henkilötietojen käsittelijöitä noudattamaan tietosuojavelvoitteitaan.

4.2.2 Yksityisyyteen liittyvät käsitteet

Yksityisyyteen liittyviä keskeisiä käsitteitä tässä tutkimuksessa ovat yksityisyys, henkilötietojen suoja ja yksityiselämän suoja. **Yksityisyys** on suomalaisen sivistyssanakirjan mukaan intiimiyttä, oikeutta yksityisyyteen. Intiimiyttä voidaan loukata ja tällöin puhutaan yksityisyyden loukkaamisesta. Yksityisyys on myös yksityiselämää. Yksityisyyden käsite pohjautuu alun perin Alan Westin (1969) määritelmään, jonka mukaan yksityisyys koostuu neljästä eri osa-alueesta. Näitä ovat henkilökohtainen yksityisyys (vapaus olla ilman toisten manipulointia), vapaus oman persoonallisuuden kehittämiseen, tarve vetäytyä omaan yksityisyyteen ja itse-arviointiin sekä sosiaalinen tarve kertoa vain osittain omista ajatuksistaan.

Yksityisyydestä säädetään Euroopan ihmisoikeussopimuksessa (63/1999) ja se on perustana Euroopan ihmisoikeuksille sekä EU:n perusoikeusasiakirjalle. (Council of Europe, 2014; Euroopan unioni 2017). Euroopan ihmisoikeussopimuksen (63/1999) 8 artiklan mukaan:

”Oikeus nauttia yksityis- ja perhe-elämän kunnioitusta

1. *Jokaisella on oikeus nauttia yksityis- ja perhe-elämäänsä, kotiinsa ja kirjeenvaihtoonsa kohdistuvaa kunnioitusta.*
2. *Viranomaiset eivät saa puuttua tämän oikeuden käyttämiseen, paitsi kun laki sen sallii ja se on välttämätöntä demokraattisessa yhteiskunnassa kansallisen ja yleisen turvallisuuden tai maan taloudellisen hyvinvoinnin vuoksi, tai epäjärjestyksen tai rikollisuuden estämiseksi, terveyden tai moraalin suojaamiseksi, tai muiden henkilöiden oikeuksien ja vapauksien turvaamiseksi.”*

Leander vs. Ruotsi tuomion jälkeen henkilötietojen suojan on katsottu kuuluvan yksityisyyden suojan alle, vaikka artikla 8. ei suoraan mainitse henkilötietojen suojaa. (European Court of Human Rights 1987; Koillinen 2012, 177; Kivi 2016).

EU:n perusoikeusasiakirjan (2012/C326/02) artiklat 6-15 määrittelevät erilaiset vapaudet. Artiklan 6 mukaisesti ”*jokaisella on oikeus vapauteen ja henkilökohtaiseen turvallisuuteen*”, 7. artiklan mukaan ”*jokaisella on oikeus siihen, että hänen yksityis- ja perhelämäänsä, kotiaan sekä viestejään kunnioitetaan*”, ja artikla 8 koskee henkilötietojen suojaa. Sen mukaisesti ”*jokaisella on oikeus henkilötietojensa suojaan, tietojen käsittelyn on oltava asianmukaista, sen on tapahduttava tiettyä tarkoitusta varten, asianomaisen henkilön suostumuksella tai laissa säädetyn oikeuttavan perusteen nojalla*”.

Tavani (2007) luokittelee yksityisyyden käsitteen neljään eri alueeseen (ei-häiritä, eristäytyminen, kontrolli, rajoittava) (kts. liite 1). Hänen mukaansa kaikki nämä yksityisyyden alueet ovat kuitenkin epätäydellisiä ja niissä on omat rajoitteensa ja ongelmansa. Tavani (2007) kuvaa Moorin vuonna 1990 ja 1997 sekä Tavani ja Moorin vuonna 2001 kehittämää yksityisyyden teoriaa nimeltään rajoitettu pääsy/rajoitettu kontrolli-teoria (*RALC, Restricted Access/Limited Control Theory.*) Siinä yksityisyyden käsite tarkoittaa, että henkilöä suojellaan muiden häirinnältä tai tietojen keräämiseltä. Tätä varten on olemassa lakeja, normeja ja määräyksiä, jotka suojelevat henkilöä. Tavani ja Moor erottelivat yksityisyyden käsitteen oikeudesta yksityisyyteen ja yksityisyyden hallintaan. Hallinta on sitä, että voi itse kontrolloida tietoja ja rajoittaa niiden käyttöä. Tavanin (2007) mukaan lait suojelevat meitä ja toisaalta voimme itse kontrolloida omia tietojamme. Marzin (1999) mukaan henkilön tulisi voida kontrolloida omia tietojaan. Yksityisyys on hänen mukaansa eri asia kuin luottamus. Luottamus on kahden tai useamman henkilön välinen asia. Molemmat tietävät henkilökohtaista tietoa, mutta sitä ei paljasteta tai se paljastetaan vain rajoitetusti. Salaisuus viittaa laajempaan tiedon suojeluun.

Suomen perustuslaissa (L731/1999: 10 §) on määritelty yksityiselämän suoja oikeutena, mutta ei sitä, mitä siihen kuuluu. Euroopan ihmisoikeustuomioistuimen oikeuskäytännön mukaan yksityiselämään katsotaan kuuluvan muun muassa henkilökohtainen identiteetti ja anonymiteetti, moraalinen ja fyysinen koskemattomuus, riittävän yksityisyyden

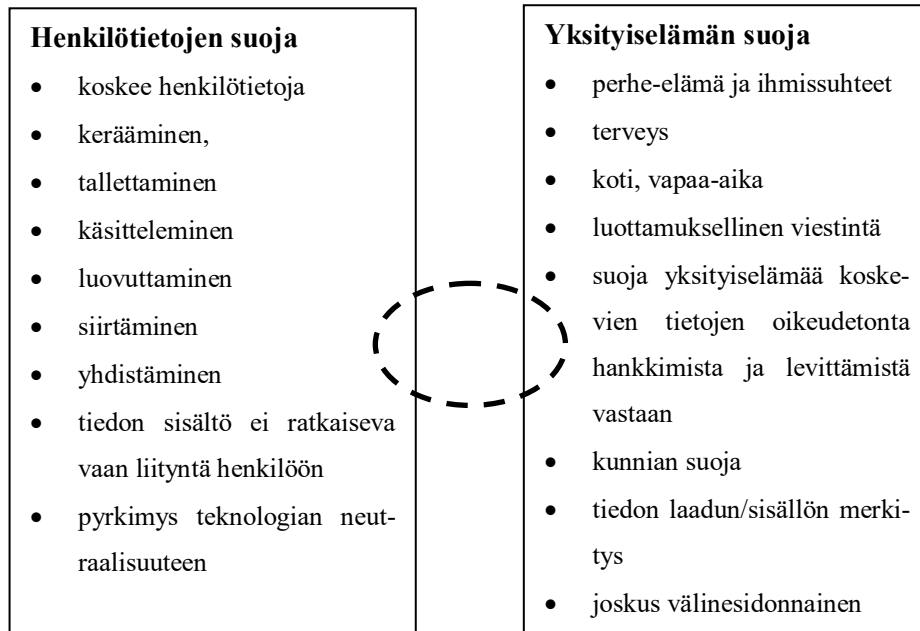
turvaava tila, oikeus henkilökohtaisiin suhteisiin sekä henkilötiedot ja sukupuoli käyttäytyminen. (Mäenpää 2016, 35.) Mladenov (2013) näkee ongelmaksi sen, ettei Euroopan ihmisoikeusneuvosto määrittele tarkasti, mitä oikeus yksityisyyteen tarkalleen tarkoittaa, vaan ainoastaan, mitä siihen kuuluu. Euroopan ihmisoikeusneuvoston (European Court of Human Rights, 2014) mukaan yksityisyys ja yksityiselämä pitävät sisällään muun muassa oikeuden muodostaa ja ylläpitää suhteita, fyysisen ja moraalisen koskemattomuuden suojan, henkilökohtaisen datan suojan, mahdollisuuden muuttaa oma nimi sekä oikeuden seksuaaliseen suuntaukseen.

Henkilötietojen suojan tarkoituksena on suojata henkilötietoja. Henkilötietolaki toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia henkilötietoja käsitellessä (L523/1999, 1 §). Tietosuoja-asetuksen 1. artiklan mukaisesti asetuksella suojellaan luonnollisten henkilöiden perusoikeuksia ja vapauksia ja erityisesti heidän oikeuttaan henkilötietojen suojaan. Suoja voi toteutua siten, että henkilö antaa suostumuksensa henkilötietojen käyttöön (kontrollointi) sekä että henkilötietojen käyttö perustuu lakiin, tehtävään, velvoitteeseen, asiakassuhteeseen, työtökijäsuhteeseen tai sopimukseen.

Tietosuoja-asetuksen 6. artiklan mukaan henkilötietojen käsittely on lainmukaista silloin, kun rekisteröity on antanut suostumuksensa, käsittely on tarpeen sopimuksen tai lakisääteisen velvoitteen noudattamiseksi tai käsittely on tarpeen rekisteröidyn tai toisen luonnollisen henkilön elintärkeiden etujen suojaamiseksi, taikka käsittely on tarpeen yleistä etua koskevan tehtävän suorittamiseksi tai julkisen vallan käyttämiseksi. Lisäksi käsittely on lainmukaista, jos käsittely on tarpeen rekisterinpitäjän tai kolmannen osapuolen oikeutettujen etujen toteuttamiseksi. Viimeistä kohtaa ei kuitenkaan sovelleta viranomaisten tehtäviin.

Pitkänen kollegoineen (2013, 24) ovat kuvanneet kuviossa 5 esitetyn mukaisesti henkilötietojen suojan ja yksityiselämän suojan suhdetta niin, että molempiin kuuluu elementtejä, joita ei kuulu toiseen ja lisäksi joitakin elementtejä, jotka ovat yhteisiä. Yksityiselämää koskevat tiedot ovat aina henkilötietoja, jos ne voidaan yhdistää tiettyyn henkilöön, mutta kaikki henkilötiedot eivät välttämättä kuulu yksityiselämän suojan alaan. (mt.) Hallituksen esitys (HE96/1998) eduskunnalle henkilötietolaiksi ja eräksi siihen

liittyviksi laeiksi mukaan yksilön suojaa ja oikeuksia kuvataan käsitteellä yksityisyyden suoja tai yksityiselämän suoja. Yksityiselämän suojaan liittyy myös muita perusoikeuksia kuten oikeus henkilökohtaiseen vapauteen, kunniaan ja yhdenvertaiseen kohteluun.



KUVIO 5. Henkilötietojen ja yksityiselämän suojan välinen suhde (Pitkänen ym. 2013, 24).

4.2.3 Rekisterinpitoon liittyvät käsitteet

Tässä tutkimuksessa rekisterinpitoon liittyviä keskeisiä käsitteitä ovat henkilötietojen käsittely, rekisterinpitäjä, käsittelijä, rekisteröity, sivullinen, henkilörekisteri ja suostumus. **Henkilötiedon käsittely** on henkilötietolain (L523/1999, 3§) mukaan henkilötietojen keräämistä, tallettamista, järjestämistä, käyttöä, siirtämistä, luovuttamista, säilyttämistä, muuttamista, yhdistämistä, suojaamista, poistamista sekä muita henkilötietoihin kohdistuvia toimenpiteitä. Käsittelyn määritelmä on laaja ja se pitää sisällään kaiken henkilötietoihin liittyvän käsittelyn. Käsitteistä siirtäminen ja luovuttaminen ovat osin päällekkäisiä. Luovuttamisessa tiedon vastaanottajasta tulee rekisterinpitäjä, kun taas siirtämisessä rekisterinpidon vastuu jää siirtäjälle. (Pitkänen ym. 2013, 52–52.)

Tietosuoja-asetuksen 4. artikla määrittelee vastaavasti henkilötietojen käsittelyn sellaiseksi toiminnaksi tai toiminnoiksi, joita kohdistetaan henkilötietoihin tai henkilötieto-

ja sisältäviin tietojoukkoihin. Käsittely voi olla automaattista tai manuaalista tietojenkäsittelyä, kuten tietojen kerääminen, tallentaminen, järjestäminen, jäsentäminen, säilyttäminen, muokkaaminen tai muuttaminen. Lisäksi käsittely voi olla hakua, kyselyä, käyttöä, tietojen luovuttamista siirtämällä, levittämällä tai asettamalla ne muutoin saataville, tietojen yhteensovittamista tai yhdistämistä, rajoittamista, poistamista tai tuhoamista.

Rekisterinpitäjä on henkilötietolain 3§:n mukaan yksi tai useampi henkilö, yhteisö, laitos tai säätiö, jonka käyttöä varten henkilökisteri perustetaan. Rekisterinpitäjällä on oikeus määrätä henkilökisterin käytöstä tai hänen tehtäväkseen on lailla säädetty rekisterinpito. Rekisterinpitäjän tulee huolehtia siitä, että rekisteröidyn oikeudet toteutuvat. Tietosuoja-asetuksen 4. artiklan mukainen rekisterinpitäjä on luonnollinen tai oikeushenkilö, viranomainen, virasto tai muu elin, joka yksin tai yhdessä määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot. Myös tietosuoja-asetuksessa rekisterinpitäjän yksi päävelvollisuus on toteuttaa rekisteröidyn oikeuksia. Tietosuoja-asetuksessa rekisterinpitäjää ei sidota henkilökisterin käsitteeseen. Henkilötietolain 3 §:n mukaan käsittelijä käsittelee henkilötietoja rekisterinpitäjän lukuun. Käsittelijä on tietosuoja-asetuksessa 4. artiklan mukaan sellainen luonnollinen tai oikeushenkilö, viranomainen, virasto tai muu elin, joka käsittelee henkilötietoja rekisterinpitäjän lukuun.

Rekisteröity on henkilö, jota henkilötieto koskee henkilötietolain 3 §:n mukaan. Tietosuoja-asetuksen 4. artiklan mukainen rekisteröity on sellainen luonnollinen henkilö, joka voidaan tunnistaa suoraan tai epäsuorasti erityisten tunnistetietojen (nimen, henkilötunnuksen, sijaintitiedon, verkkotunnistetietojen, fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän) perusteella. **Sivullinen** on muu henkilö, yhteisö, laitos tai säätiö kuin rekisteröity, rekisterinpitäjä, henkilötietojen käsittelijä tai henkilötietoja kahden viimeksi mainitun lukuun käsittelevää (HeTiL 3 §). Tietosuoja-asetuksen 4. artiklassa sivullinen on määritelty kolmantena osapuolena. Kolmas osapuoli on sellainen luonnollinen henkilö tai oikeushenkilö, viranomainen, virasto tai muu toimielin, joka ei käsittele henkilötietoja rekisterinpitäjän välittömän vastuun alaisena.

Henkilörekisteri on henkilötietolain 3 §:n mukaan henkilötietoja sisältävä tietojoukko, jotka käyttötarkoituksensa vuoksi kuuluvat yhteen. Näitä tietoja voidaan käsitellä osin tai kokonaan automaattisen tietojenkäsittelyn avulla tai ne on järjestetty kortistoksi, luetteloksi tai näihin verrattavalla tavalla siten, että tiettyä henkilöä koskevat tiedot voidaan löytää helposti ja kohtuuttomitta kustannuksitta. Pitkänen kollegoineen (2013, 53) esittää, että henkilötietojen käsittelyyn käytetty tekniikka ei ratkaise, onko kyseessä henkilörekisteri vai ei, vaan se, onko tiedot järjestetty tai saatavissa helposti järjestykseen. Manuaaliset järjestämättömät tiedot eivät muodosta henkilörekisteriä. Hallituksen esityksen (HE96/1998) mukaan henkilörekisteri on niin sanottu looginen rekisteri, mikä tarkoittaa sitä, että samaan rekisteriin kuuluvat kaikki ne tiedot, joita käytetään samassa käyttöyhteydessä riippumatta siitä, miten ja mihin ne on tallennettu. Lyhytaikaiset tiedostot ja tallenteiden eri sukupolvet eivät ole eri henkilörekistereitä silloin, kun ne ovat rekisterinpitäjän hallussa ja niitä käytetään rekisterille määriteltyihin käyttötarkoituksiin. Erilaiset päätökset, muistiot, luettelot ja kirjeet eivät muodosta henkilörekisteriä, vaikka niissä olisi henkilötietoja, jos niitä ei tallenneta erikseen tietojenkäsittelyjärjestelmään.

Tietosuoja-asetuksen 4. artiklan mukaan rekisterin muodostaa mikä tahansa jäsenelty henkilötietoja sisältävä tietojoukko, josta tiedot ovat saatavilla tietyin perustein. Tietojoukko voi olla keskitetty, hajautettu tai toiminnallisin tai maantieteellisen perustein jaettu. Tietosuoja-asetuksen kertomusosiossa 15. kappaleessa on maininta, että henkilöiden suojeleu koskee henkilötietojen automaattista käsittelyä sekä niiden manuaalista käsittelyä, jos henkilötiedot sisältyvät tai ne on tarkoitus sisällyttää rekisteriin. Ne asiakirjat tai asiakirjakokoelmat kansilehtineen, joita ei ole järjestetty tiettyjen perusteiden mukaisesti, eivät sisälly tietosuoja-asetuksen piiriin.

Suostumus on henkilötietolain 3 §:n mukaan kaikenlainen vapaaehtoinen, yksilöity ja tietoinen tahdonilmaisu, jolla rekisteröity hyväksyy henkilötietojensa käsittelyn. Tietosuoja-asetus määrittelee 4. artiklassa suostumuksen olevan mikä tahansa vapaaehtoinen, yksilöity, tietoinen ja yksiselitteinen tahdonilmaisu, jolla rekisteröity hyväksyy henkilötietojensa käsittelyn antamalla suostumusta ilmaisevan lausuman tai toteuttamalla selkeästi suostumusta ilmaisevan toimen.

5 TUTKIMUKSEN AINEISTOT JA ANALYYSIMENETELMÄT

Tässä luvussa kuvataan tutkimuksessa käytetyt aineistot ja niihin liittyvät eri analysointimenetelmät. Analysointimenetelminä käytettiin sekä määrällisiä että laadullisia menetelmiä. Käytetyt menetelmät olivat sisällönanalyysi, sisällön erittely, tilastollisten määreiden kuvaaminen sekä arviointi. Ensimmäisessä kappaleessa (5.1) kuvataan aineistot ja viimeisissä kappaleissa kuvataan käytetyt analysointimenetelmät (5.2, 5.3) ja perustelut (5.4) niiden käytölle.

Tutkimuksen vaiheet voidaan jakaa tutkimuksen suunnitteluun, tietojen analysointiin, johtopäätösten tekoon ja tulosten esittämiseen. (Pietilä 1973, 264). Laadullisen tutkimuksen aineistoa voidaan hankkia haastatteluilla, kyselyillä, havainnoilla tai erilaisista dokumenteista. (Hirsjärvi & Hurme 2001, 144.) Määrällinen tutkimus vastaa kysymyksiin kuinka paljon ja miten usein; tietoa tarkastellaan numeerisesti. Määrällisessä tutkimuksessa käytetään kysely-, haastattelu- ja havainnointilomakkeita. (Vilka 2007, 13–14.)

5.1 Tutkimuksen aineistot

Ensimmäinen aineisto muodostui henkilötietolaista ja siihen liittyvät hallituksen esityksestä (HE96/1998) sekä tietosuoja-asetuksesta ja siihen liittyvästä kertomusosiosta. Henkilötietolaki koostuu 11 luvusta, jotka jakaantuvat 51 pykälään. Tietosuoja-asetus koostuu 11 luvusta ja niihin liittyy 99 artiklaa. Tietosuoja-asetuksen kertomusosio sisältää 173 kappaletta ja se vastaa hallituksen esitystä perusteluineen. Taulukossa 1 on kuvattu henkilötietolain ja tietosuoja-asetuksen rakenteet kokonaiskuvan hahmottamiseksi.

Toinen aineisto muodostui henkilötietolain ja tietosuoja-asetuksen arviointiaineistosta ja arvioinnista tehdystä yhteenvedosta. Vertailu henkilötietolain ja tietosuoja-asetuksen välillä tehtiin käymällä läpi henkilötietolain pykälä ja verrattiin niitä tietosuoja-asetuksen vastaaviin artikloihin. Joihinkin henkilötietolain pykäliin saattoi kohdistua useampi tietosuoja-asetuksen artikla. Toisaalta taas tietosuoja-asetuksen joihinkin artikloihin, kuten oletusarvoista tietosuojaa käsittelevään artiklaan, ei löytynyt vastinetta henkilötietolaissa. Arviointi on kuvattu taulukossa liitteessä 2 ja siihen liittyvä kooste

on liitteessä 3. Liitteen 2 ensimmäisessä sarakkeessa on kirjattu otsikot henkilötietolain pykälistä ja tietosuoja-asetuksen artikloista. Toisessa sarakkeessa on kuvattu henkilötietolain kyseinen pykälä. Pykälä pyrittiin ilmaisemaan lyhyesti ja selkeästi. Joitakin pykäläitä jouduttiin kirjoittamaan lähes kokonaisuudessaan ymmärrettävyyden parantamiseksi. Kolmannessa sarakkeessa on kuvattu tietosuoja-asetuksen artikkelit henkilötietolain mukaisessa järjestyksessä. Tietosuoja-asetuksen artikloiden kirjoittamisessa noudatettiin samaa periaatetta kuin henkilötietolain pykälien kanssa. Artiklat pyrittiin kirjoittamaan lyhyesti ja selkeästi. Viimeisessä sarakkeessa arvioitiin henkilötietolain ja tietosuoja-asetuksen eroja.

TAULUKKO 1. Henkilötietolain ja tietosuoja-asetuksen rakenteet

Henkilötietolain (L523/1999) rakenne		Tietosuoja-asetuksen (2016/679) rakenne	
1 Luku	Yleiset säännökset (§ 1-4)	I Luku	Yleiset säännökset (1-4 art.)
2 Luku	Henkilötietojen käsittelyä koskevat yleiset periaatteet (§ 5-10)	II Luku	Periaatteet (5-11 art.)
3 Luku	Arkaluonteiset tiedot ja henkilötunnus (§11-13)	III Luku	Rekisteröidyn oikeudet (12-23 art.)
4 Luku	Henkilötietojen käsittely erityisiä tarkoituksia varten (§ 14-19)	IV Luku	Rekisterinpitäjä ja henkilötietojen käsittelijä (24- 43 art.)
5 Luku	Henkilötietojen käsittely erityisiä tarkoituksia varten (§ 22-23)	V Luku	Henkilötietojen siirrot kolmansiin maihin tai kansainvälisille järjestöille (44-50 art.)
6 Luku	Rekisteröidyn oikeudet (§ 24-31)	VI Luku	Riippumattomat valvontaviranomaiset (51-59 art.)
7 Luku	Tietoturvallisuus ja tietojen säilytys (§ 32- 35)	VII Luku	Yhteistyö ja yhdenmukaisuus (60-76 art.)
8 Luku	Ilmoitus tietosuojavaltuutetulle (§ 36- 37)	VIII Luku	Oikeussuojakeinot, vastuu ja seuraamukset (77-84 art.)
9 Luku	Henkilötietojen käsittelyn ohjaus ja valvonta (§ 38-44)	IX Luku	Tietojenkäsittelyyn liittyviä erityistilanteita koskevat säännökset (85-91 art.)
10 Luku	Erinäiset säännökset (§ 47-49)	X Luku	Delegoidut säädökset ja täytäntöönpanosäännökset (92-93 art.)
11 Luku	Voimaantulo- ja siirtymäsäännökset (§ 50-51)	XI Luku	Loppusäännökset (94-99 art.)

Arviointi tehtiin kolmen eri kriteerin perusteella: onko tietosuoja-asetus selkeyttänyt, täydentänyt vai tuonut uutta rekisterinpitäjän vaatimuksiin verrattuna henkilötietolakiin. Lisäksi sarakkeessa on huomioitu mahdollinen erityislainsäädäntö sekä se, milloin henkilötietolaissa on tarkemmat määrittelyt. Arviointia ei kuitenkaan tehty erityislainsäädännön osalta sen suuren määrän takia. (Liite 2 ja 3.)

Kolmantena aineistona oli tutkittaville tehty kysely ja vastauksiin pohjautuva analyysi. Kyselyn kohteena olivat rekisterinpidosta vastaavat kunnalliset julkishallinnon organisaatiot: peruskunnat (n=295), kuntayhtymät (n=55) ja maakuntien liitot (n=18). Kuntayhtymät koostuivat koulutuskuntayhtymistä ja muista kuntayhtymistä. Kysely lähetettiin 368 organisaatioon. Kyselyyn saattoivat vastata organisaatioiden eri toimialat yhdessä tai erikseen, esimerkiksi suurissa kaupungeissa tekninen toimiala ja opetustoimi, joten tutkimukseen saattoi tulla useampi vastaus samasta organisaatiosta. Kyselyyn sai vastata täysin anonyymisti. Tutkimuksen ulkopuolelle rajattiin sosiaali- ja terveydenhoitoala, sairaanhoitopiirit ja Ahvenmaa. Sosiaali- ja terveydenhuolto rajattiin pois, koska muun muassa tietosuojavastaavan nimittäminen on ollut pakollista siellä jo vuodesta 2007. Ahvenmaa rajattiin pois, koska Ahvenmaalla noudatetaan eri lainsäädäntöä henkilötietojen käsittelyssä kuin manner-Suomessa. Kysymysten teemat koostuivat henkilötietolain kohdista ja kysymykset ryhmiteltiin taulukossa 2 kuvatun mukaisesti.

TAULUKKO 2. Kyselylomakkeen ryhmittely

Teema	Kysymykset
Taustatiedot	1-5
Henkilötietojen käsittelyä koskevat yleiset periaatteet	6-11
Rekisteröidyn oikeudet	12-13
Rekisteriseloste	14-16
Tietosuojavastaava	17-18
Tietoturva ja riskienhallinta	19
Valmistautuminen tietosuoja-asetukseen	20-26

Teemat valittiin niistä henkilötietolain kohdista, jotka kohdistuvat ensisijaisesti rekisterinpitäjän velvollisuuksiin: mitä rekisterinpitäjän tulee tietää, jotta voi huolehtia rekisteröidyn oikeuksista ja rekisterinpitäjän valmistautumista tietosuoja-asetukseen. Lupa kyselyn lähettämiseen saatiin Kuntaliiton tutkimuspäälliköltä Marianne Pekola-Sjöblomilta. Kyselylomake (liite 5) tehtiin webropol-kyselynä ja lähetettiin tutkittavien organisaatioiden kirjaamoiden sähköpostiin. Sähköpostiosoitteet saatiin Kuntaliiton asiakasrekisteristä. Jollei kyseisellä organisaatiolla ollut kirjaamon sähköpostia, kysely lähetettiin hallinnosta vastaavalle johtajalle. Nimet pro gradu-työn tekijä haki organisaatioiden nettisivuilta. Kyselylomake testattiin Kuntaliiton asiantuntijoilla ja kommentteja pyydettiin julkishallinnon asiantuntijoista koostuvalta asiantuntijaryhmältä. Kysely-

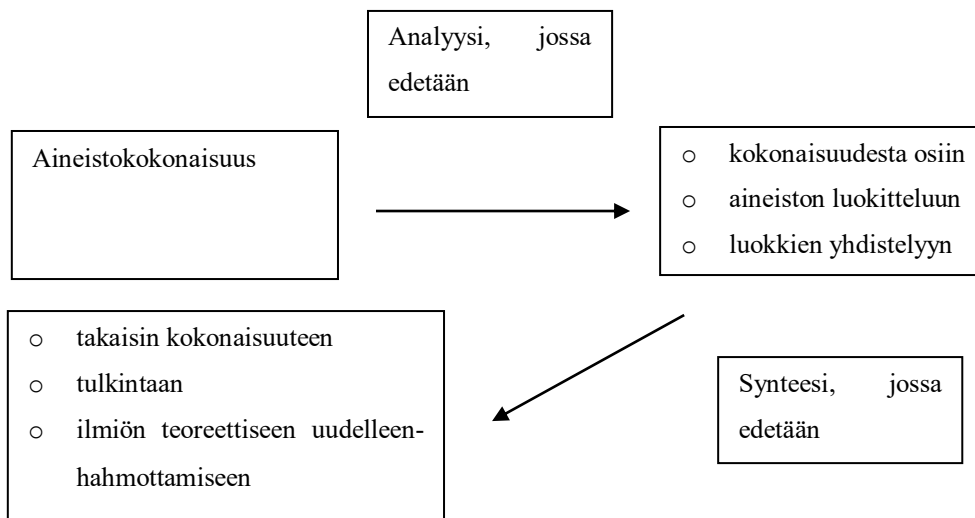
lomaketta muokattiin testausten jälkeen ja käännettiin ruotsin kielelle. Saatteena olevassa sähköpostissa ohjeistettiin kyselyyn vastaamiseen ja siihen, kenelle kysely kohdistetaan. Kysely pyydettiin kohdistamaan keskushallinnon esimiehelle tai henkilölle, joka tietää henkilötietojen suojan toteuttamiskäytännöistä organisaatiossa. Nämä voivat toimia eri nimikkeillä, kuten kunnanjohtaja, johtaja, hallintojohtaja, talousjohtaja, asiakirjahallinnosta ja arkistotoimesta vastaava johtaja tai toimitusjohtaja. Kysely tehtiin helmikuussa 2017. Aikaa vastaamiselle annettiin kaksi viikkoa, jonka jälkeen lähetettiin muistutuskirje, jossa annettiin vielä viikko lisäaikaa. Vastaukset ohjautuivat webropol-ohjelmaan analysoitavaksi.

5.2 Analyysimenetelmänä sisällönanalyysi ja sisällön erittely

Perusanalyysimenetelmänä laadullisessa tutkimuksessa voidaan käyttää **sisällönanalyysiä**. Analyysi toimii kirjoitettujen, kuultujen tai nähtyjen aineistojen kevyenä teoreettisen viitekehysten ja analysointitapana. Tavoitteena on järjestää aineisto tiiviisti ja selkeästi niin, että aineiston tietosisältö ei katoa. (Tuomi & Sarajärvi 2009, 103–108; Hirsjärvi & Hurme 2001, 144.) Sisällönanalyysia voidaan tehdä aineistolähteisesti, teorialähtöisesti tai teoriaohjaavasti. Menetelmän valinta ohjaa viitekehystä, aineiston hankintaa, aineiston analyysia ja raportointia. (Tuomi & Sarajärvi 2009, 99.) Aineistolähtöisessä analyysissä tutkimusaineisto muodostaa teoreettisen kokonaisuuden ja analyysi tehdään aineiston perusteella. Teoria liittyy aineistolähtöisessä analyysissä siihen, miten analyysi toteutetaan. Tuomi ja Sarajärvi (2009, 96) nostavat esiin kysymyksen siitä, voidaanko tutkimusta toteuttaa puhtaasti aineistolähtöisesti. Heidän mukaansa ei ole olemassa ”puhtaita” havaintoja, vaan tutkijan käyttämät käsitteet, tutkimusasetelma ja menetelmät vaikuttavat tuloksiin.

Aineistolähtöisen analyysin puutteita korvaa teoriaohjaava analyysi. Siinä viitekehystenä toimii metodologia ja se mitä tutkittavasta ilmiöstä jo tiedetään. Aineistoa voidaan kerätä vapaasti. Analyysivaiheessa edetään ensin aineistopohjaisesti, mutta tutkija pystyy myös käyttämään valmiita malleja ja etenemään analyysissään luovasti. Kolmas analyysimuoto on teorialähtöinen analyysi. Se pohjautuu tiettyyn teoriaan, malliin tai auktoriteetin esittämään ajatteluun, eli siihen, mitä tutkittavasta ilmiöstä tiedetään. Voidaan testata esimerkiksi aikaisempaa tietoa uudessa kontekstissa. Analyysia ohjaa aikai-

semmin luotu kehys. (mt., 91–100.) Sisällönanalyysissä tunnistetaan ne asiat, joista ollaan kiinnostuneita ja jotka vastaavat tutkimusongelmaan. Tunnistamisen jälkeen kiinnostavat asiat ryhmitellään ja annetaan ryhmille nimi. Eri ryhmiä tai kategorioita voi olla useita, sekä ala- että ylätasoon kategorioita. Tavoitteena on luoda uusi kokonaisuus. (Tuomi & Sarajärvi 2009, 95–100.) Hirsjärvi ja Hurme (2001, 144) ovat kuvanneet analyysin käsittelyvaiheet prosessina. Prosessi alkaa analyysin erittelystä, jonka jälkeen aineisto luokitellaan ja lopulta muodostetaan kokonaisuus tutkittavasta ilmiöstä. Kyseinen prosessi on kuvattu tarkemmin kuviossa 6.



KUVIO 6. Analyysistä synteisiin (Hirsjärvi & Hurme 2001, 144)

Analyysi voidaan jakaa myös sen mukaan, miten havainnot tai tulkinnot tehdään. Analyysi voi olla induktiivista (yksittäisestä yleiseen) tai deduktiiviseen (yleisestä yksittäiseen) analyysiin. (Tuomi & Sarajärvi 2009, 95.) Deduktiivisessa näkökulmassa testataan teoriaa ja sen pohjalta tehtyä hypoteesia. Tarkoitus on selittää, ennustaa ja ymmärtää ilmiötä muuttujien avulla. (Creswell 1994, 88.) Induktiivisessa analyysissä tarkoituksena on kuvailla, ymmärtää, kehittää ja löytää; luokat syntyvät tutkimuksen aikana (mt., 58). Tuomen ja Sarajärven (2009, 95) mukaan jako induktiiviseen ja deduktiiviseen analyysiin ei ole riittävä, eikä puhtaan induktiivinen analyysi ole välttämättä mahdollista. Hirsjärvi ja Hurme (2001, 136) kutsuvat kolmatta tapaa abduktiiviseksi päättelyksi. Siinä käytetään apuna teoreettisia johtideoita, joita pyritään todentamaan aineistosta. Alasuutari (1993, 23) puhuu havaintojen pelkistämisestä ja arvoituksen ratkaisemisesta. Havaintojen pelkistämisessä aineistoa tarkastellaan tietystä näkökulmasta ja

karsitaan havaintomäärää yhdistämällä. Tuloksena on yhteinen piirre tai sääntö, joka kuvaa esimerkkinä tai näytteenä samaa ilmiötä. Arvoituksen ratkaiseminen on abduktiivista päättelyä, missä tehdään tulkintoja tuotettujen johtolankojen ja käytettävissä olevien vihjeiden pohjalta.

Hirsjärvi kollegoineen (2007, 188–190) pitävät **kyselytutkimusta** hyvänä menetelmänä saada tietoa standardoidusti, laajasti ja samalla tavalla kaikilta vastaajilta. Kyselyssä on heikkoutensa, jotka tutkijan on huomioitava. Näitä ovat muun muassa seuraavat: kuinka hyvin kyselylomake on tehty, kuinka huolellisesti kyselyyn on vastattu, onko kysymykset ymmärretty oikein, ovatko kysymykset selkeitä, ja ovatko tutkittavat perehtyneet kyseiseen alueeseen, sekä saadaanko kattava vastausprosentti. Ronkaisen kollegoineen (2011, 83–84) mukaan kyselytutkimuksella pyritään kuvaamaan ja tulkitsemaan ilmiötä, niiden yhteyksiä ja vaikutussuhteita. Tarkoituksena on tiivistää kielelliset merkitykset luvuiksi ja analysoida niitä tilastollisesti tai matemaattisesti. Kyselylomakkeen kysymykset muodostuvat ilmiön eri osioista. Tutkittaville voidaan esittää myös avoimia kysymyksiä, joilla selvennetään merkitystä.

Sisällön erittely on tutkimustekniikka, jossa kuvaillaan kommunikaatiota objektiivisesti, systemaattisesti ja määrällisesti. (Berelson 1971, 14–18; Pietilä 1973, 51.) Tutkimuksessa keskitytään siihen mitä sanotaan, eikä niinkään siihen, miksi sanotaan (Berelson 1971, 16). Pietilän mukaan (1973, 51) sisällön erittely liittyy käsitteellisesti siihen tutkimuksen vaiheeseen, jossa kerätään tietoa tutkittavasta dokumenttisisällöstä tai sen ulkopuolisesta ilmiöstä. Tuomi ja Sarajärvi (2009, 106) erottavat sisällönanalyysin ja sisällön erittelyn toisistaan siten, että sisällönanalyysissa kuvataan dokumenttien sisältöä sanallisesti. Sisällön erittelyssä tarkoituksena on kuvata kvantitatiivisesti tekstin sisältöä. Voidaan esimerkiksi kertoa, kuinka moni vastaaja oli jotakin mieltä kysyttävästä asiasta. Tutkimusmenetelmänä sisällön erittelyä käytetään Pietilän (1973, 52–53) mukaan sellaisissa tutkimuksissa, joissa joko tilastollisesti tai sanallisesti pyritään kuvailemaan dokumenttien sisältöä tai niitä ulkopuolisia ilmiöitä, joita sisällön ajatellaan ilmaisevan. Eskolan (1968, 107) mukaan sisällön erittelyllä voidaan tutkia yksinkertaisesti kommunikaation sisältöä. Sisällön erittelyä analyysimenetelmänä voidaan käyttää kaikissa sellaisissa tutkimuksissa, joissa joko tilastollisesti tai sanallisesti kuvaillaan sisäl-

töä sinänsä ja niitä ulkopuolisia ilmiöitä, joita sisällön ajatellaan ilmaisevan (Pietilä 1973, 52–53).

Eskola (mt., 108–111) kuvaa kirjassaan Berelsonin vuonna 1952 esittelemät kolme sisällön erittelyn luokkaa. Ensimmäisen luokan muodostavat ne tutkimukset, joissa ainoastaan kuvataan kommunikaation sisältöä, muotoon liittyviä piirteitä ja luotettavuutta. Toisessa luokassa tehdään päätelmiä kommunikaation tuottajista ja kolmannessa luokassa kommunikaation vastaanottajista ja vaikutuksista. Jos tutkimuksen tarkoituksena on vain kuvata tekstiä, saattavat tulokset Eskolan (mt., 106) mukaan jäädä yksinkertaisiksi ja mielenkiinnottomiksi. Hän erottelee kommunikaation kahteen tasoon, ekspressiiviseen ja instrumentaaliseen. Ekspressiivinen ilmaisee välittömästi puhujan tunteita ja instrumentaalinen heijastaa tutkittavan pyrkimyksiä. Tässä pro gradu -työssä käytettyjä menetelmiä kuvataan kappaleessa 5.4.

5.3 Analyysimenetelmänä arviointi

Sanakirjan mukaan **arviointi** on jonkin asian arvoa tai ansiota. Arviointi ja tutkimus ovat eri asioita; arvioinnissa asetetaan arvo, tutkimuksessa kuvataan, selitetään tai ymmärretään. (Robson 2001, 23–26.) Sinkkosen ja Kinnusen (1994, 32–37) mukaan arviointi on havainnoitavan kohteen arvottamista. Kohteen ominaisuuksia verrataan valittuihin arvottamiskriteereihin. Kriteerit voivat olla muun muassa erilaiset standardit ja tavoitteet, jotka on johdettu arvoista. Tavoitteet ja standardit asetetaan etukäteen ja niitä arvioidaan suhteessa toimintaan. Arvot vaikuttavat näin kriteereihin. Keskeistä arvioinnissa on muodostaa arviointikriteereitä ja mittareita sekä mitata ja arvioida saatua tietoa (Stakes 2001). Arviointikysymykset vaikuttavat arvioinnin tarkoitukseen, käytettävään teoriaan ja menetelmiin sekä aineiston hankintastrategiaan (Robson 2001, 122–124; Virtanen 2007, 156).

Chelimskyn (1997, 1-25) mukaan arviointiin vaikuttavat voimakkaasti globaalit poliittiset voimat, uusi teknologia ja maailman tilanne. Arvioinnilla on tärkeä rooli osoittaa, kuinka on onnistuttu tai epäonnistuttu. Arvioinnilla voidaan tuoda ilmi epäkohtia ja kehittää toimintaa. Eräsaaren (1999, 147–148) mukaan arvioinnilla pyritään muokkaamaan jotain hyödyllisempää, uskottavampaa ja menestyvämpää. Hän tuo esiin arvioin-

nin kehämäisyyden. Arviointi aktivoi ihmisiä ja asioita muuntautumaan ja muuttumaan uusiin olosuhteisiin ja samalla kehittämään ajattelutapojaan ja näkemyksiään. Arviointi sisältää myös institutionaalisesti ehdollistavan ohjauksen. Toimijoiden vastuut ja tulokset selkeytyvät ja toimijarooli vahvistuu. Arvioinnin avulla voidaan tuoda keskusteluun uusia asioita.

Arviointi voidaan jakaa kolmeen erilaiseen muotoon. Vastuullisuusarvioinnissa korostuvat tulokset ja arvo ja arvioinnin kohteena ovat kustannukset ja tehokkuus. Puhutaan myös tilivelvollisuudesta. Tietotuotantoarvioinnissa tarkoituksena on arvioida julkisia ongelmia, ohjelmia, prosesseja sekä kehittää uusia metodeja. Kolmas arvioinnin muoto on kehittämisarviointi. Sen tarkoituksena on vahvistaa ja kehittää toimintaa arvioinnin perusteella. (Chelimsky 1997, 21.) Scriven (1991, 63, 150) jakaa arvioinnin formatiiviseen ja summatiiviseen arviointiin. Formattiivinen arviointi tehdään kehittämisen aikana, useimmiten organisaation tai ohjelman sisällä, ja arvioinnin tekijä voi olla organisaation tai ohjelman sisäinen tai ulkopuolinen henkilö. Lähtökohta on se, että arviointi tapahtuu, kun toimet ovat vielä käynnissä. Summatiivisessa arvioinnissa arvioidaan, miten jokin asia, esimerkiksi ohjelma, on onnistunut. Scriven (1991, 63) kuvaa näiden kahden arvioinnin välistä eroa Bob Stakesin lausumalla ” *Kun kokki maistaa keittoa on kyseessä formatiivinen arviointi; kun syöjä maistaa keittoa on kyseessä summatiivinen arviointi.* ”

Muitakin malleja, lähestymistapoja, paradigmoja tai otteita arviointiin ja arviointitutkimuksessa on kuvattu. Sinkkonen ja Kinnunen (1994, 77) ovat jaotelleet arvioinnin peruslähestymistavat kahdeksaan erilaiseen luokkaan ja vertailevat luokkien piirteitä keskenään. Luokat ovat standardiperusteiset, harkintaan perustuvat, tavoiteperusteiset, systeemianalyttiset (operaatio- ja kustannushyötyanalyysit), päätöksentekijään tai tiedonkäyttäjään liittyvät, tavoitteista riippumattomat, tapaustutkimus-lähestymistavat ja asiantuntija-arviointiin perustuvat. Standardi- ja normiperusteista arviointitapaa kutsutaan myös kuuliaisuus- tai luotettavuusarvioinniksi. Tarkoituksena on verrata toimintatapoja asetettuihin ja yleensä dokumentoituihin standardeihin tai normeihin. Arvioinnilla on myös kontrolloiva tarkoitus: voidaan arvioida, kuinka huolellisesti jotakin säännöstöä, esimerkiksi lakia, noudatetaan. (Vuorela 1990, 34–35.) Laillisuuden arvioinnilla halutaan arvioida sitä, ovatko olosuhteet tai toimenpiteet normien mukaiset sekä saada selville mahdolliset poikkeamat ennalta hyväksytyistä, sovitusta laatuvaatimuksista tai

ylemmän päätöksentekijän arvioista, tarkoituksista tai päätöksistä. (Ahonen 1985, 12–13; Sinkkonen ym. 1994, 80.) Seuraavassa kappaleessa 5.4. kuvataan valitun arviointimenetelmän käyttöä aineistossa.

5.4 Analyysimenetelmien valinta

Tässä pro gradu -työssä on käytetty kolmea eri analyysimenetelmää. Erilaisten menetelmien käytöllä (triangulaatiolla) saadaan monipuolisempia, tarkempia ja toisiaan täydentäviä tuloksia (Ronkainen ym. 2011, 47). Henkilötietolain ja tietosuoja-asetuksen aineistojen osalta analyysimenetelminä olivat sekä sisällönanalyysi että arviointi. Sisällönanalyysissä aineisto ryhmiteltiin eri otsikoiden mukaisesti, jotta saatiin hajotettua aineisto kokonaisuudesta osiin ja takaisin kokonaisuuteen Hirsjärven ja Hurmeen (2001, 144) kuvauksen mukaisesti. Analyysissa käytettiin induktiivista aineistolähtöistä päättelyä, missä edettiin yksittäisestä yleiseen. Arvioinnin avulla selvitettiin tietosuoja-asetuksen ja henkilötietolain välisiä eroavaisuuksia. Arviointikriteerinä oli se, miten henkilötietolain vaatimukset rekisterinpitäjälle eroavat tietosuoja-asetuksen vaatimuksista. Henkilötietolain ja tietosuoja-asetuksen arvioinnin arviointimenetelmä oli normiperusteinen arviointitapa. Arvioinnilla oli kontrolloiva ja keskustelua herättävä tarkoitus. Menetelmä oli luonteeltaan formatiivinen; arviointia tehtiin tilanteessa, missä kaikki tietosuoja-asetuksen käytännöt eivät ole vielä selvillä. Arviointia tehtiin kolmen eri osan alueen avulla; arvioitiin, mitkä asiat selkeytyivät, mitkä täydentyivät ja mitkä olivat kokonaan uutta tietosuoja-asetuksessa.

Rekisterinpitäjien (tutkittavien) lähtötilanteen selvittämiseksi tehtiin kysely. Nykytilan tietoa tarvitaan, jotta voidaan suunnitella tarvittavat kehittämistoimet. Kyselytutkimuksen vastausten analysoinnissa käytettiin sisällön erittelyä. Vastaukset kuvailtiin sekä tilastollisesti että sanallisesti. Tarkoituksena oli kuvailla sitä, mikä on rekisterinpitäjien lähtötilanne suhteessa henkilötietolakiin, sekä miten rekisterinpitäjät ovat valmistautuneet tulevaan tietosuoja-asetukseen. Mielenkiinnon kohteena oli se, mitä tutkittavat sanoivat ja mikä oli kommunikation sisältö, muoto ja luotettavuus. Kommunikation taso oli ekspressiivistä; vastaukset kuvasivat tutkittavien käsityksiä. Aineisto käsiteltiin SPSS 20 tilastointiohjelmalla sekä webropol 2.0 -kyselyohjelmassa olevalla tilastointiohjelmistolla

6 TUTKIMUSTULOKSET JA YHTEENVETO

Tässä luvussa kuvataan tutkimuksen tulokset. Ensimmäisissä kappaleissa (6.1–6.3) käydään läpi henkilötietolain ja tietosuoja-asetuksen välisen arvioinnin tulokset kolmen osa-alueen kautta. Nämä alueet ovat: miten tietosuoja-asetuksen vaatimukset rekisterinpitäjälle selkiytyvät, miten ne täydentyvät sekä mitkä ovat uutta verrattuna henkilötietolakiin. Lopuksi esitetään yhteenveto (6.4) tietosuoja-asetuksen mukaisista rekisterinpitäjän vaatimuksista. Tämän jälkeen käydään läpi kyselytutkimuksen tulokset (6.5) ja kuvataan rekisterinpitäjien nykytilanne. Sen jälkeen verrataan arvioinnin kautta saatuja tuloksia nykytilanteeseen (6.6). Vertailun avulla saadaan muodostettua kehittämissuosituksia rekisterinpitäjille: mitä rekisterinpitäjän tulee ottaa huomioon, jotta tietosuoja-asetuksen vaatimukset tulevat täytetyksi. Kehittämissuosituksia jaetaan välittömästi tehtäviin ja päivitettäviin asioihin. Kehittämissuosituksia on kuvattu liitteessä 6.

6.1 Tietosuoja-asetus selkeyttää

Tietosuoja-asetuksen selkeyttämisellä tarkoitetaan, että tietosuoja-asetuksen kohdat ovat vastaavat tai selventävät tiettyä rekisterinpitäjään kohdistuvaa vaatimusta verrattuna henkilötietolakiin. Tietosuoja-asetus selkeyttää lainsäädäntöä siten, että asetusta koskee kaikkia jäsenvaltioita sekä unionin alueella tapahtuvaa henkilötietojen käsittelyä. Rajauksena toimialaan on unionin toimialaan kuulumaton lainsäädäntö, kuten ulko- ja turvallisuuspolitiikan soveltamisalaan kuuluva toiminta. Tietosuoja-asetusta ei sovelleta luonnollisen henkilön suorittamaan henkilötietojen käsittelyyn. (1-2 art.) Tietosuoja-asetus selkeyttää ohjeistusta henkilötietojen käsittelyn lainmukaisuuteen (6 art.) ja rekisteröidyn vastustamisoikeuteen (21 art.) koskien henkilötietojen käsittelyä suoramarkkinoinnissa, tieteellisessä tai historiallisessa tutkimustarkoituksessa tai tilastollista tarkoitusta varten.

6.2 Tietosuoja-asetus täydentää

Tietosuoja-asetuksen täydentävillä osioilla tarkoitetaan tilanteita, jolloin tietosuoja-asetus täydentää henkilötietolain määräyksiä. Säädökset eivät ole uusia, mutta tuovat

sellaisia täydennyksiä, joihin rekisterinpitäjän on varauduttava. Tietosuoja-asetuksessa on useita sellaisia käsitteitä, joita ei ole henkilötietolaissa. Näitä ovat muun muassa profilointi, pseudonymisointi, geneettiset tiedot ja biometriset tiedot. (4 art.) Täydennykset tuovat mukanaan vaatimuksia, joilla kuvataan uuden tekniikan tuomia mahdollisuuksia. Rekisterinpitäjän kannalta tietosuoja-asetus tuo mukanaan henkilötietojen yleisen periaatteiden noudattamisen, osoitusvelvollisuuden ja toiminnan läpinäkyvyyden (5 art.). Rekisterinpitäjän on noudatettava henkilötietojen käsittelyssä tietosuoja-asetuksen mukaan, samoin kuin henkilötietolaissa, lainmukaisuutta, kohtuullisuutta, käyttötarkoituksidonnaisuutta, tietojen minimointia ja täsmällisyyttä niin, että tiedot säilyvät eheinä ja luottamuksellisena.

Rekisterinpitäjän tulee huomioida tietosuoja-asetuksen laajennus koskien erityisiä henkilötietoryhmiä (9 art.). Käsittelykiellon piiriin on lisätty geneettisten ja biometrinen tietojen käsittely henkilön yksiselitteistä tunnistamista varten. Sosiaalihuolto ei määritellä tietosuoja-asetuksen 9. artiklassa (erityisiä henkilötietoryhmiä koskeva käsittely), mutta sosiaalihuolto mainitaan käsittelykiellon poikkeuksissa. Henkilötietolaki on joltain osin tarkempi arkaluonteisten tietojen käsittelyssä. Laki pitää muun muassa sisällään määräykset poistaa arkaluonteiset tiedot, kun niiden käyttämiselle ei ole perustetta. Toisaalta taas tietosuoja-asetuksen 5. artiklassa säädetään tietojen minimoinnista ja säilytyksen rajoittamisesta. Suostumuksen (4 art. ja 7 art.) osalta tietosuoja-asetus tuo mukanaan osoitusvelvollisuuden suostumuksen olemassaolosta. Lisäksi suostumuksen sisältö on määritelty nykyistä tarkemmin tietosuoja-asetuksessa.

Rekisterinpitäjällä on velvollisuus informoida (12 art.) rekisteröityä henkilötietojen käsittelystä sekä siitä, miten rekisteröity voi tarkastaa tietonsa, rekisteröidyn oikeudesta tietojen oikaisemiseen, rekisteröidyn oikeudesta tulla joissakin tapauksessa unohdetuksi, rekisteröidyn oikeudesta käsittelyn rajoittamiseen, rekisteröidyn oikeudesta henkilötietojen oikaisuun tai poistoon, rekisteröidyn oikeudesta siirtää tietoja järjestelmästä toiseen, rekisteröidyn oikeudesta vastustaa käsittelyä sekä rekisteröidyn oikeudesta tietää automatisoiduista yksittäispäätöksistä, profiloinnista ja tietoturvaloukkauksista. Täydentävää informoinnin osalta henkilötietolakiin nähden on se, että rekisterinpitäjällä on velvollisuus tunnistaa rekisteröity. Rekisteröityyn kohdistuva informointi on esitettävä tiiviisti ja läpinäkyvästi sekä ilmaistava selkeällä ja yksinkertaisella kielellä. Tiedot on

toimitettava kirjallisesti tai sähköisessä muodossa. Tiedot on toimitettava, kun henkilötietoja kerätään rekisteröidyltä itseltään (13 art.) tai kun henkilötietoja ei ole saatu rekisteröidyltä itseltään. Tietosuoja-asetuksen artikloissa 13 ja 14 on tarkemmin määritelty, mitä tietoja rekisteröidylle on ilmoitettava.

Tietosuoja-asetus täydentää rekisteröidyn oikeuksia. Liitteessä 4 on määritelty ne artiklojen 14–17 mukaiset rekisteröidyn oikeudet, jotka täydentyvät. Lisäksi tietosuoja-asetus täydentää automatisoituja yksittäispäätöksiä mukaan lukien profilointi (22 art.). Profilointia saa tehdä vain, jos päätös on välttämätön rekisteröidyn ja rekisterinpitäjän välisen sopimuksen tekemistä tai täytäntöönpanoa varten ja se perustuu lainsäädäntöön ja nimenomaiseen suostumukseen. Tietosuoja-asetuksella täydennetään myös rajoituksia (23 art.): unionin oikeudessa tai lainsäädännössä voidaan lainsäädäntötoimenpiteillä rajoittaa rekisteröidyn oikeuksia koskien tietoturvaloukkauksista ilmoittamista ja henkilötietojen käsittelyä koskevia periaatteita. Rajoituksia voidaan tehdä kansallisen turvallisuuden, puolustuksen ja yleisen turvallisuuden takaamiseksi.

Tietosuoja-asetus täydentää rekisterinpitäjän vastuuta toteuttaa tarvittavat tekniset ja organisatoriset toimenpiteet, jolla voidaan varmistaa ja osoittaa, että rekisterinpitäjä noudattaa asetusta: rekisterinpitäjällä on osoitusvelvollisuus (24 art.). Tietosuoja-asetus määrittelee henkilötietojen käsittelijän (4 art.) sekä henkilötietojen käsittelijän vastuun (28 art.). Henkilötietojen käsittelijällä tulee olla riittävät suojatoimet asianmukaisten teknisten ja organisatoristen toimien täytäntöönpanemiseksi, niin että henkilötietojen käsittely täyttää tietosuoja-asetuksen vaatimukset. Henkilötietojen käsittelijä saa käsitellä henkilötietoja vain rekisterinpitäjän kirjallisella luvalla, hänen on tiedotettava suunnitelluista muutoksista ja käsittely on määriteltävä sopimuksella. Rekisterinpitäjältä vaaditaan kattava sopimus henkilötietojen käsittelijän kanssa sekä hyvä ohjeistus. Henkilötietojen käsittelijän pitää toimia rekisterinpitäjän ohjeiden mukaisesti. Tietosuoja-asetus korostaa rekisterinpitäjän ohjausvelvollisuutta (29 art.). Valvontaviranomainen voi hyväksyä vakiosopimuslausekkeita (28 art.), joita voidaan käyttää rekisterinpitäjän ja henkilötietojen käsittelijän välissä sopimuksissa.

Henkilötietolain 10. pykälässä on määritelty rekisterinpitäjän velvollisuudesta laatia rekisteriseloste henkilörekistereistä sekä mitä rekisteriselosteesta on ilmentävä. Tieto-

suoja-asetuksessa rekisterinpitäjän ja tarvittaessa rekisterinpitäjän edustajan velvollisuus on pitää selostetta käsittelytoimista (30 art.). Seloste ei ole rekisterikohtainen, vaan se kuvastaa rekisteröityjen ryhmiä ja henkilötietoryhmiä. Uutena asiana selosteessa on, että siihen pitää sisällyttää myös tietosuojavastaavan yhteystiedot, mahdollisen yhteisrekisterinpitäjän nimi, tietoryhmien poistamisen suunnitellut määräajat sekä tekniset ja organisatoriset turvatoimet henkilötietojen käsittelylle. Uutta on myös se, että seloste on oltava sekä sähköisessä että kirjallisessa muodossa. Lisäksi henkilötietojen käsittelijän ja tarvittaessa henkilötietojen käsittelijän edustajan on ylläpidettävä selostetta kaikista rekisterinpitäjien lukuun suoritettavista käsittelytoimista ja pyydettyä esitettävä se valvontaviranomaiselle.

Tietosuoja-asetuksessa on myös määrittelyt henkilötietojen siirrolle Euroopan unionin ulkopuolelle (44–50 art.). Henkilötietojen siirto on mahdollista, jos rekisterinpitäjä tai henkilötietojen käsittelijä toteuttaa asianmukaiset suojatoimet ja rekisteröityjen saatavilla on täytäntöönpanokelpoisia suojatoimia ja tehokkaita oikeussuojakeinoja. Komissio julkaisee luetteloa turvallista alueista sekä alueista, jotka eivät ole turvallisia. Tietosuoja-asetus täydentää henkilötietolakea käytäntönsäännöissä (40 art.). Käytäntönsäännöt koskevat EU:n jäsenvaltioita. EU:n tietosuojaneuvosto käsittelee jäsenvaltioiden käytäntönsääntöjä valvontaviranomaisen esityksestä. Henkilötietojen ohjaus ja valvonta täydentyvät Euroopan unionin tasoisella ohjauksella. Kukin maa nimittää valvontaviranomaisen (51 art.), joka valvoo tietosuoja-asetuksen noudattamista alueellaan ja tekee yhteistyötä muiden jäsenvaltioiden valvontaviranomaisten kanssa. Tarvittaessa valvontaviranomainen vie asioita EU:n tietosuojaneuvoston (68 art.) käsiteltäväksi. Tietosuoja-asetuksen 31. artiklassa säädetään rekisterinpitäjän ja henkilötietojen käsittelijän tai niiden edustajien velvollisuudesta tehdä yhteistyötä valvontaviranomaisen kanssa. Henkilötietojen siirrosta arkistoon tietosuoja-asetus täydentää niin ikään rekisterinpitäjän velvoitteita. Asetus painottaa teknisiä ja organisatorisia toimenpiteitä, joita rekisterinpitäjän on noudatettava (89 art.).

6.3 Tietosuoja-asetus tuo uutta

Kolmantena jaottelukriteerinä henkilötietolain ja tietosuoja-asetuksen vertailussa oli arvioida, mitä uutta tietosuoja-asetus tuo rekisterinpitäjän velvollisuuksiin. Tietosuoja-

asetus tuo uutta lapsen suostumuksen ehtoihin koskien tietoyhteiskunnan palveluita (8 art.). Jäsenvaltiot voivat säätää asetuksen määrittelemästä 16 vuoden ikää alemmasta ikärajusta. Asetuksen mukaan tietoyhteiskunnan palveluihin tarvitaan vanhempainvastuunkantajan suostumus alle 16-vuotiaan lasten osalta. Tietoyhteiskunnan palveluita ovat kaikki etäpalveluina annettavat sähköiset palvelut, joita toimitetaan henkilökohtaisesti pyynnöstä ja joista tavallisesti maksetaan korvaus (95/46/EY).

Uutta on myös rekisterinpitäjän velvollisuus tunnistaa rekisteröity sekä velvollisuus ilmoittaa rekisteröidylle, mikäli rekisterinpitäjä ei pysty tunnistamaan rekisteröityä (11 art.). Asetus tuo uutta rekisteröidyn oikeuksiin. Näitä ovat rekisteröidyn oikeus käsittelyn rajoittamiseen (18 art.), henkilötietojen oikaisua tai poistoa tai käsittelyn rajoitusta koskeva ilmoitusvelvollisuus rekisteröidylle (19 art.), rekisteröidyn oikeus siirtää tiedot järjestelmästä toiseen (20 art.) ja vastustamisoikeus (21 art.). Liitteessä 4 on ryhmiteltyinä tarkemmin ne rekisteröidyn oikeudet, joihin tietosuoja-asetus tuo uutta.

Uutta tietosuoja-asetuksessa on mahdollisuus toimia yhteisrekisterinpitäjänä. Yhteisrekisterinpitotilanne syntyy, kun vähintään kaksi rekisterinpitäjää määrittää yhdessä henkilötietojen käsittelyn tarkoitukset ja keinot. Yhteisrekisterinpitäjien tulee sopia vastuualueista, rooleista ja suhteista rekisteröityihin. (26 art.) Tietosuoja-asetus tuo uutena vaatimuksen sisäänrakennetusta ja oletusarvoisesta tietosuojasta (25 art.). Rekisterinpitäjän on käsittelytapoja määriteltessään ja henkilötietojen käsittelyn yhteydessä toteutettava tehokkaasti tietosuojaperiaatteita, kuten tietojen minimointia, sekä huolehdittava asianmukaisista teknisistä ja organisatorisista toimenpiteistä. Lisäksi uutta tietosuoja-asetuksessa on henkilötietojen käsittelyyn liittyvä vaikutustenarviointi (35 art.) sekä ennakkokuuleminen (36 art.). Kun rekisterinpitäjä ottaa käyttöön uutta teknologiaa ja jos sitä käytettäessä luonnollisen henkilön oikeuksille ja vapauksille muodostuu korkea riski, on rekisterinpitäjän tehtävä vaikutustenarviointi. Rekisterinpitäjän on kuultava ennen käsittelyä valvontaviranomaista ja valvontaviranomainen tulee julkaista luettelo niistä käsittelytoimien tyypeistä, joiden suhteen vaikutustenarviointi on tehtävä. (35 ja 36 art.)

Uutta on sertifiointimenettely. Rekisterinpitäjiä kannustetaan ottamaan käyttöön sertifiointimekanismeja, tietosuojasinettejä ja -merkkejä. Sertifioinnilla voidaan osoittaa, että

toimitaan tietosuoja-asetuksen määräämällä tavalla. (42 art.) Uutta on myös se, että rekisterinpitäjien ja henkilötietojen käsittelijöiden on toimittava riskiperusteisesti (32 art.). Heidän tulee osoittaa, että he noudattavat tietosuoja-asetukseen liittyviä toimintaperiaatteita sekä hallinnollisesti että teknisesti. Heidän on näytettävä toteen, että toiminnan jatkuvuus on turvattu eri olosuhteissa. Lisäksi rekisterinpitäjien ja henkilötietojen käsittelijöiden tulee huolehtia, että ne luonnolliset henkilöt, joilla on pääsy henkilötietoihin, toimivat ohjeiden mukaisesti. (32 art.) Rekisterinpitäjä ja henkilötietojen käsittelijä voivat ilmaista tämän osoitusvelvollisuuden esimerkiksi käyttämällä sertifioituja järjestelmiä tai käyttämällä valvontaviranomaisella vahvistettuja käytäntöjä. (32 art.)

Lisäksi rekisterinpitäjän tulee ilmoittaa tietoturvaloukkauksista valvontaviranomaiselle ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 72 tunnin kuluessa, mikäli loukkauksesta ei todennäköisesti aiheudu riskiä luonnollisten henkilöiden oikeuksiin ja vapauksiin (33 art.). Myös henkilötietojen käsittelijän tulee ilmoittaa rekisterinpitäjälle tietoturvaloukkauksista ilman aiheetonta viivytystä (33 art.). Tietoturvaloukkauksista on ilmoitettava rekisteröidylle, mikäli tietoturvaloukkaus aiheuttaa korkean riskin luonnolliselle henkilölle. Ilmoitusta ei kuitenkaan tarvitse tehdä, jos se vaatii kohtuutonta väivä ja jos rekisterinpitäjä on toteuttanut suojaimet riskin välttämiseksi. (34 art.)

Tietosuoja-asetus tuo uutena vaatimuksen nimittää tietosuojavastaava, määrittellä hänen asemansa ja tehtävänsä sekä ilmoittaa tietosuojavastaavan tiedot valvontaviranomaiselle. Tietosuojavastaava voi olla konsernin tai viranomaisten yhteinen ja lisäksi tietosuojavastaava voi hoitaa työtään palvelusopimuksella. (37–39 art.)

Tietosuoja-asetuksen 82. artiklassa säädetään vastuusta ja oikeudesta korvauksen saamiseen. Kukin rekisterinpitäjä on vastuussa vahingosta, joka on aiheutunut asetuksen rikkomisesta. Vastuu on myös henkilötietojen käsittelijällä; hänen tulee noudattaa asetusta ja rekisterinpitäjän ohjeita. Uutta on valvontaviranomaisen mahdollisuus määrätä hallinnollisia sakkoja, joiden määrä vaihtelee kahdesta neljään prosenttiin kokonaisliiketoiminnasta tai enintään 10–20 miljoonaa. Määrän vaihtelu riippuu muun muassa siitä, mitä asetuksen artiklaa rikkomus koskee. (83 ja 84 art.)

6.4 Yhteenveto tietosuoja-asetuksen vaatimuksista rekisterinpitäjälle

Yhteenveto tietosuoja-asetuksen vaatimuksista rekisterinpitäjän velvollisuuksille on esitetty kuviossa 7. Yhteenveto muodostettiin mukaillen Pitkäsen kollegioinen (2013, 309) tekemää mallia henkilötietojen käsittelystä elinkaaren eri vaiheissa.



KUVIO 7. Tietosuoja-asetuksen vaatimukset rekisterinpitäjälle (soveltaen Pitkänen ym. 2013, 309)

Mallissa kuvataan, mitä rekisterinpitäjän on tehtävä ennen kuin hän aloittaa henkilötietojen käsittelemisen, miten hänen tulee toimia käsittelyn aikana sekä mitä asioita on huomioitava käsittelyn päätyttyä. Kaikissa henkilötietojen elinkaaren vaiheissa rekiste-

rinpitäjän on toimittava asetuksen mukaisesti ja osoitettava toimintatapansa hallinnollisesti ja teknisesti, tiedettävä asetuksen soveltamisalue ja asetuksessa kuvatut määritelmät, kuten henkilötiedon käsite. Lisäksi rekisterinpitäjän on toimittava riskilähtöisesti, ennakoivasti ja läpinäkyvästi. Tietosuoja-asetus korostaa rekisterinpitäjän ohjausvelvollisuutta. Rekisterinpitäjän on myös nimitettävä tietosuojavastaava ja määriteltävä hänen tehtävänsä.

6.5 Kyselytutkimuksen tulokset

Tässä kappaleessa käydään läpi kyselytutkimuksen tulokset aihealueittain. Ensimmäiset viisi kysymystä käsittelivät tutkittavien taustamuuttujia. Seuraavat kysymykset käsittelivät henkilötietojen käsittelyn yleisiä periaatteita, kysymykset 6-11. Tämän jälkeen rekisteröidyn oikeudet, kysymykset 12-13, rekisteriseloste, kysymykset 14-16, tietosuojavastaavaan liittyvät kysymykset 17-18, tietoturva ja riskienhallinta kysymys 19 ja lopuksi valmistautuminen EU-tietosuoja-asetukseen, kysymykset 20-26. (Liite 5).

6.5.1 Taustakysymykset

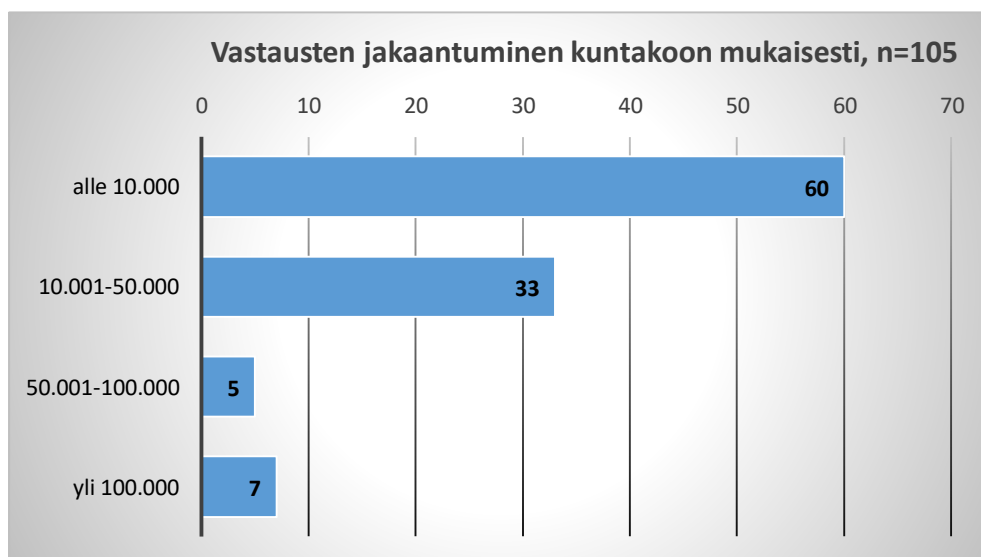
Kyselytutkimus lähetettiin 368 organisaatioon: peruskuntiin (n=295), kuntayhtymiin (n=55) ja maakuntien liittoihin (n=18). Vastauksia saatiin 138 kappaletta. Vastauksista poistettiin kaksi vastausta. Vaikka kysely oli tehty anonyymisti, eräs kunta ja kuntayhtymä olivat vastanneet kyselyyn kahteen kertaan ja tämä näkyi kirjoitetuissa kommentteissa. Vastajiin otettiin yhteyttä ja pyydettiin lupa toisen vastauksen poistamiseen. Näin ollen tutkimuksessa käytettyjä vastauksia oli 136 kappaletta. Vastausprosentti peruskuntien osalta oli 36 prosenttia (n=106), (pienet kunnat 30 %, keski-suuret kunnat 42 %, suuret kunnat 60 %) kuntayhtymien osalta vastausprosentti 36 (n=20) ja maakuntien liittojen 50 prosenttia (n=9), yksi vastaaja oli valinnut organisaatioksi muu ja määritellyt sen opetustoimeksi. Sen takia kuntien vastauksissa vaihtelee vastaajien lukumäärä (n=105) ja (n=106).

Kokonaisvastausaste oli 37 prosenttia. Vastauksista 117 kappaletta koski koko kunnan, kuntayhtymän tai maakunnan toimialaa tai yksikköä ja 19 vastausta koski vain tiettyä toimialaa. Muiksi toimialoiksi tai yksiköiksi vastaajat olivat ilmoittaneet hallinnon, kes-

kushallinnon, hallinnon- ja talouden, asiakirjahallinnon, kulttuurin- ja vapaa-ajan, lomituspalveluiden, sivistystoimen, palkanlaskennan, ICT-palveluiden, opetustoimen, koulutuskuntayhtymän ja museon.

Peruskuntien (n=106) vastausten jakautuminen asukaslukumäärän mukaisesti on kuvattu taulukossa 3. Suurin osa kunnista oli pieniä alle 10.000 asukkaan kuntia. Kyselyyn oli mahdollista vastata kunnan eri toimialojen, joten yksi kunta saattoi vastata kyselyyn useamman kerran. Jatkossa analyysissä käytetään kuntien osalta ryhmittelyä pienet kunnat alle 10.000 asukasta (n=60), keskisuuret kunnat 10.001–50.000 asukasta (n=33) ja viimeiset kaksi ryhmää yhdistettiin yli 50.000 asukkaan kunniksi (n=12).

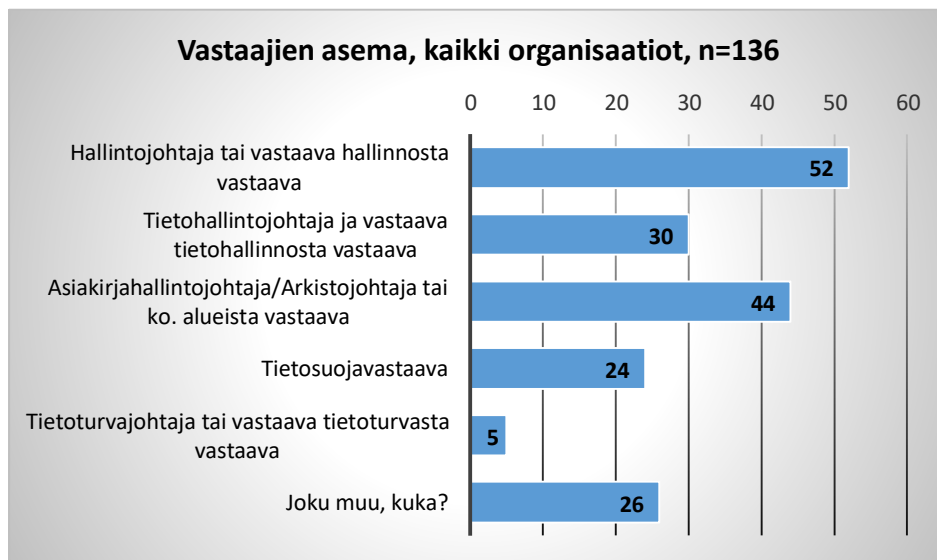
TAULUKKO 3. Vastausten jakautuminen kuntakoon mukaisesti (kpl)



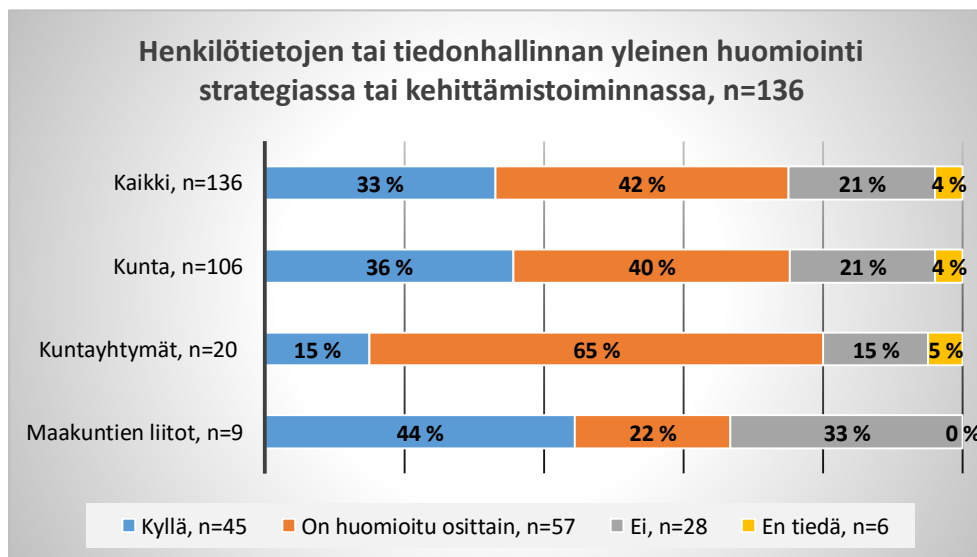
Vastaajien asemien (n=136) jakautuminen kuvataan taulukossa 4. Kysymykseen saattoi valita useamman vaihtoehdon. Suurimman vastaajaryhmän (n=52) muodostivat hallintojohtaja tai hallinnosta vastaava. Pienin edustus vastaajista (n=5) olivat tietoturvajohdajat tai vastaavat tietoturvasta vastaavat. Vastaajista (n=26) ilmoitti ryhmäkseen jonkin muun. Nämä 26 vastaajaa ilmoittivat nimikkeikseen hallintoon liittyvät (hallinnon toimialajohtaja, hallintosihteeri, toimistosihteeri, asianhallintasihteeri, suunnittelija, keskusarkistonhoitaja, arkistonhoitaja), henkilöstöhallintoon liittyvät (henkilöstöjohtaja, -päällikkö, -lakimies, -suunnittelija ja -sihteeri sekä palvelusuhdepäällikkö), IT-hallintoon liittyvät (tietohallintopäällikkö, it-vastaava, järjestelmäsuunnittelija, tietotek-

niikkaihminen, se ainoa IT-kaveri koko puljussa), taloushallintoon liittyvät (talousjohtaja maksatusasiantuntija) sekä muita kuten kehitysjohtaja, tulosityksikön johtaja ja lomituspalvelujohtaja.

TAULUKKO 4. Vastaajien asema kaikki organisaatiot (kpl)



TAULUKKO 5. Henkilötietojen tai tiedonhallinnan yleinen huomiointi strategiassa tai kehittämistoiminnassa



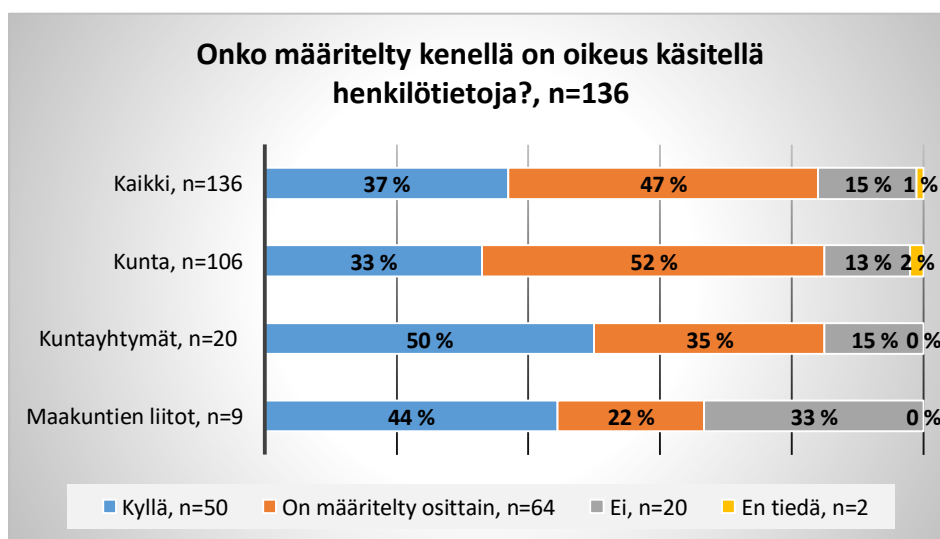
Taulukosta 5 ilmenee, että kaikista vastaajista suurin osa (75 %) ilmoitti, että henkilötietojen käsittely tai tiedonhallinta yleisesti oli huomioitu strategiassa tai kehittämistoiminnassa kokonaan tai osittain. Kunnissa henkilötietojen käsittely tai tiedonhallinta oli

huomioitu strategiassa tai kehittämistoiminnassa joko kokonaan tai osittain 76 %:lla. Kuntavertailussa pienissä kunnissa henkilötietojen käsittely tai tiedonhallinta oli huomioitu strategiassa tai kehittämistoiminnassa 67 %, keskikokoisissa kunnissa 84 % ja suurissa kunnissa 92 %:lla. Maakuntien liittojen osalta 66 % vastaajista ilmoitti, että henkilötietojen käsittely oli huomioitu joko kokonaan tai osittain strategiassa tai kehittämistoiminnassa. Vastaava luku kuntayhtymillä oli 80 %.

6.5.2 Henkilötietojen käsittelyä koskevat yleiset periaatteet

Henkilötietojen käsittelyä koskevien yleisten periaatteiden osalta kysymykset käsittelevät sitä, kenellä oli oikeus käsitellä henkilötietoja, oliko ohjeistusta henkilötietojen, henkilötunnuksen ja suostumuksen käsittelystä sekä asiakirjallisen tiedon säilyttämisen periaatteista. Lisäksi haluttiin selvittää, miten oli ohjeistettu tietojärjestelmätoimittajia ja ostopalveluita henkilötietojen käytöstä ja lopuksi oliko henkilötietojen käyttötarkoitus selvillä ja miten huolehdittiin arkaluonteisten henkilötietojen käsittelystä.

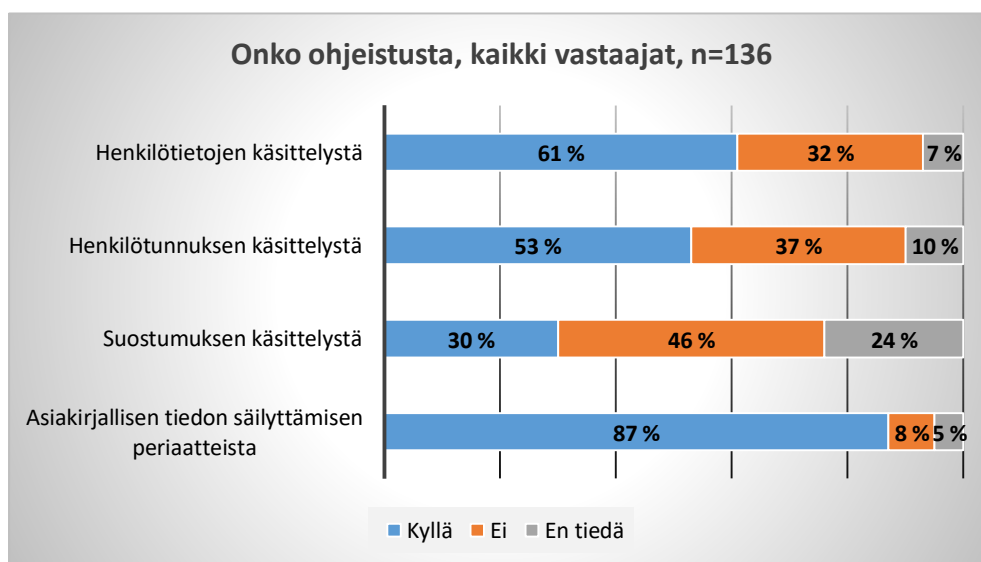
TAULUKKO 6. Onko määritelty kenellä on oikeus käsitellä henkilötietoja?



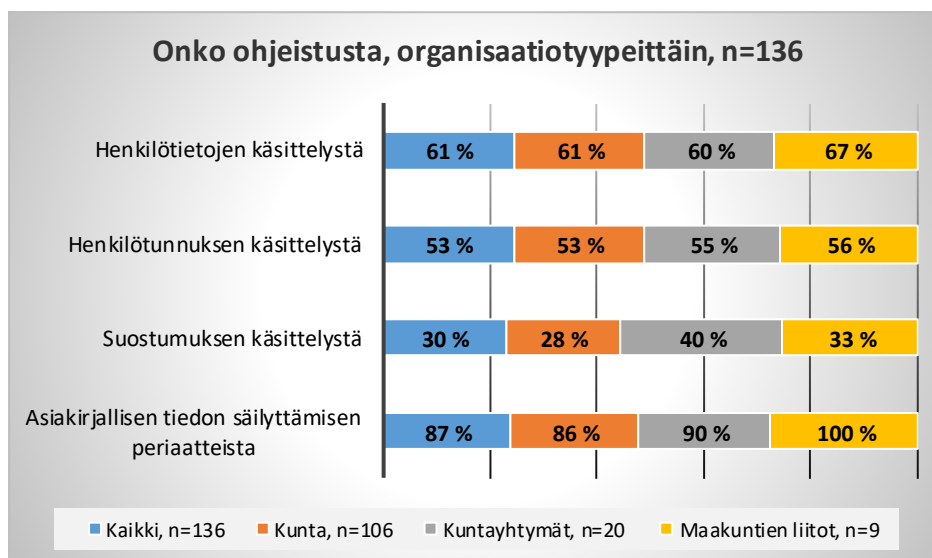
Taulukossa 6 näkyy kaikkien organisaatioiden osalta, että 84 % (kunnat 85 %, kuntayhtymät 85 %, maakuntien liitot 66 %) vastaajista ilmoitti, että organisaatiossa on määritelty joko kokonaan tai osittain kenellä on oikeus käsitellä henkilötietoja. Kuntavertailussa vastaavasti luvut olivat: pienet kunnat 82 %, keskisuuret 88 % ja suuret kunnat 92

%. Taulukosta 7 ilmenee, että kaikista organisaatiosta löytyi ohjeistusta henkilötietojen käsittelystä (61 %), henkilötunnuksen käsittelystä (53 %) ja asiakirjallisen tiedon säilyttämisen periaatteista (87 %). Heikointa oli ohjeistus koskien suostumuksen käsittelyä, 70 %:lla vastaajista ei ollut ohjeistusta tai eivät tieneet ohjeistuksen olemassaolosta.

TAULUKKO 7. Kaikkien vastaajien vastaukset koskien organisaation ohjeistusta



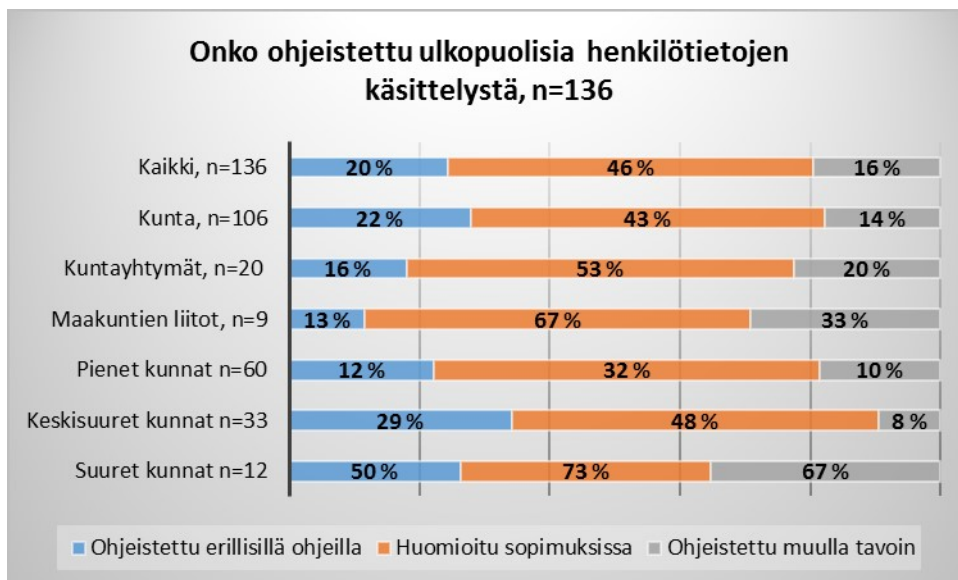
TAULUKKO 8. Ohjeistuksen olemassaolo eri organisaatiotyypeittäin



Taulukossa 8 esitetään ohjeistuksen olemassaolo eri organisaatiotyypeittäin, parhaiten oli ohjeistettu asiakirjallisen tiedon säilyttämisen periaatteet, prosenttiluvut olivat välillä 87–100. Henkilötietojen käsittelystä oli ohjeistusta 60–67%:lla. Henkilötunnuksen käsittelystä ohjeistusta oli 53–56 %:lla. Heikointa oli ohjeistettu suostumuksen käsittelyä,

prosenttiluvut olivat välillä 28–40. Lisäksi haluttiin selvittää millä tavoin organisaatiot olivat ohjeistaneet tietojärjestelmätoimittajia ja ulkopuolisia henkilötietojen käsittelijöitä, esimerkiksi ostopalveluita henkilötietojen käytössä. (Taulukko 9.)

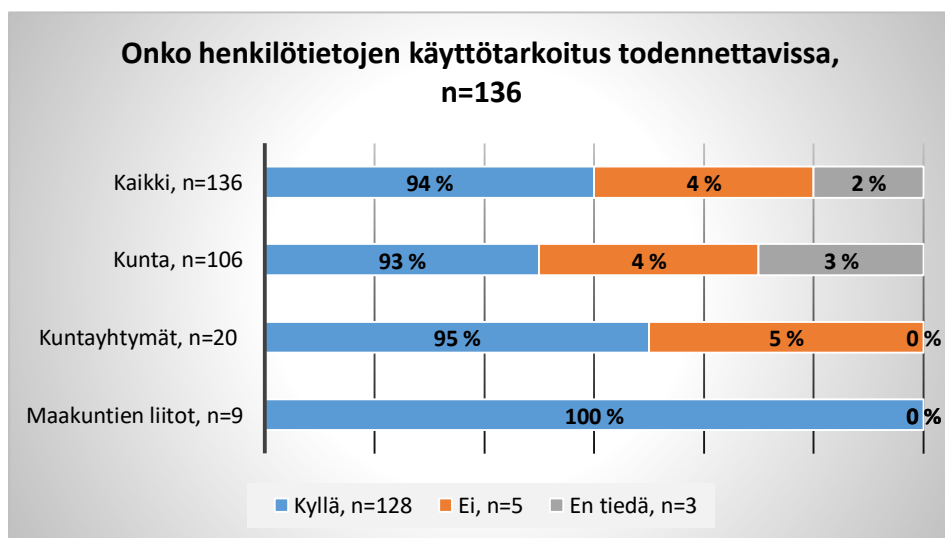
TAULUKKO 9. Ulkopuolisten ohjeistus henkilötietojen käsittelystä



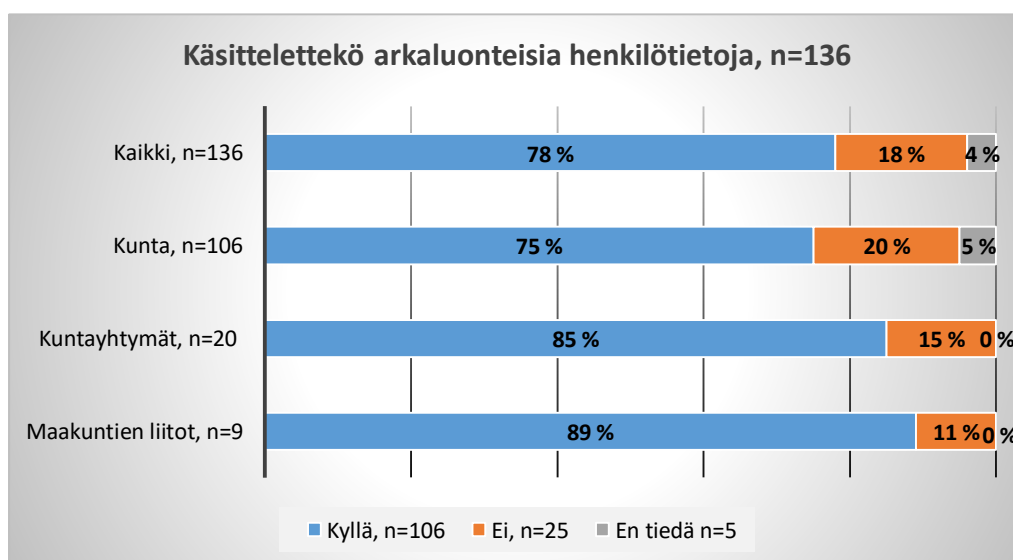
Taulukosta 9 käy ilmi, että erillisiä ohjeita ulkopuolisille oli vain 20 %:lla, 46 % vastaajista olivat huomioineet henkilötietojen käsittelyn sopimuksissa ja 16 % muulla tavoin. Korkeimmat prosenttiluvut kaikissa ryhmissä sai ulkopuolisten henkilötietojen ohjeistus sopimuksilla. Kuntien välisessä vertailussa suuret kunnat olivat huomioineet ulkopuoliset henkilötietojen käsittelijät sopimuksissa 73 %:sti.

Kysymys koskien henkilötietojen tarkoituksen todentamista oli vastaajien mukaan hyvin hoidossa, 94 % kaikista vastaajista ilmoitti, että pystyivät todentamaan henkilötietojen käyttötarkoituksen. (Taulukko 10). Tulos oli samansuuntainen eri organisaatiotyypeillä ja eri kuntaryhmissä. Seuraavat kysymykset käsittelivät arkaluonteisia henkilötietoja.

TAULUKKO 10. Henkilötietojen käyttötarkoitus



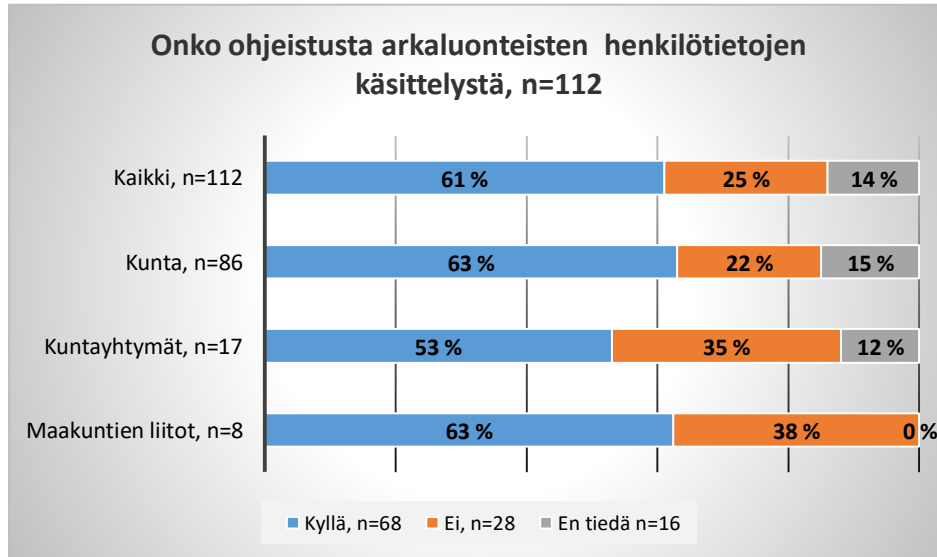
TAULUKKO 11. Käsitteletkö arkaluonteisia henkilötietoja



Tutkittavilta kysyttiin käsittelevätkö he arkaluonteisia henkilötietoja (Taulukko 11) ja jos he käsittelevät, niin onko heillä ohjeistusta arkaluonteisten henkilötietojen käsitte-

lyyn (Taulukko 12). Kaikista organisaatioista 78 %:ssa käsiteltiin arkaluonteisia henkilötietoja (Taulukko 11) ja 61 %:ssa organisaatioista (Taulukko 12) oli myös ohjeistus arkaluonteisten henkilötietojen käsittelystä.

TAULUKKO 12. Onko ohjeistusta arkaluonteisten henkilötietojen käsittelystä



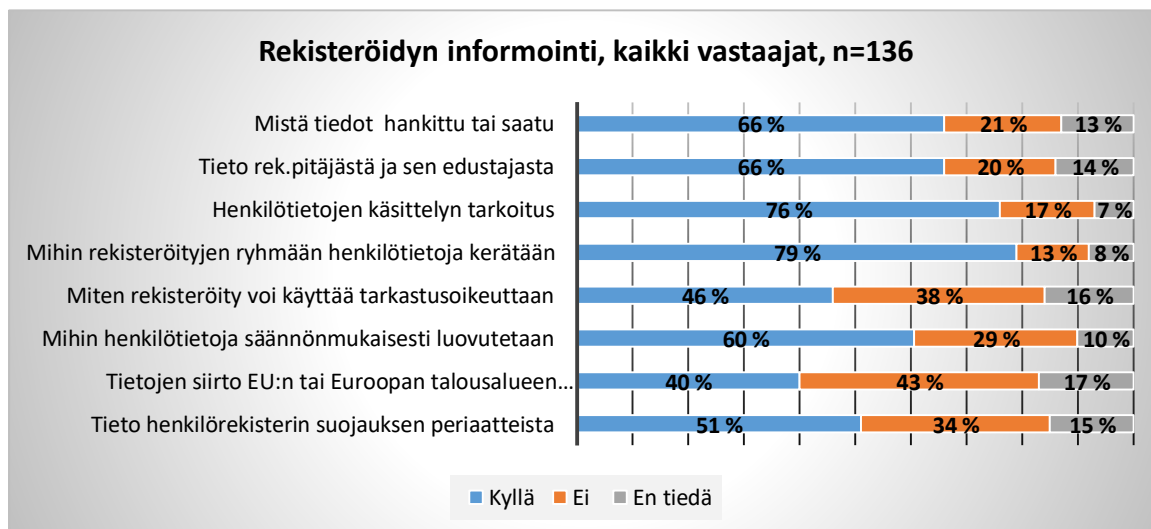
Kuntien välisissä vertailuissa arkaluonteisia henkilötietoja käsiteltiin pienissä kunnissa 75 %, keskisuurissa 67 % ja suurissa kunnissa 100 %. Arkaluonteisten henkilötietojen käsittelyn ohjeistus oli pienissä kunnissa 55 % ja keskisuurissa kunnissa 58 %. Suurissa kunnissa oli 100 % ohjeistus arkaluonteisten henkilötietojen käsittelystä.

6.5.3 Rekisteröidyn oikeudet

Rekisteröidyn oikeuksiin liittyvät kysymykset koskivat sitä, miten rekisterinpitäjä hoiti velvollisuuksiaan rekisteröityjä kohtaan. Taulukossa 13 on kaikkien organisaatioiden vastaukset. Parhaiten rekisteröityä informoitiin siitä, mihin rekisteröityjen ryhmään henkilö kuului, prosenttiluku oli 79. Toiseksi ja kolmanneksi isoimman prosenttiluvun saivat ne, mistä rekisteröidyn tiedot oli hankittu tai saatu sekä tieto rekisterinpitäjästä ja sen mahdollisesta edustajasta. Molemmissa informointi suoritettiin 66 % tapauksista. Heikoiten informoitiin sitä, siirretäänkö tietoja EU:n tai Euroopan talousalueen puolelle; prosenttiluku oli 40 %.

Lisäksi rekisteröidyn oikeudesta käyttää tarkastusoikeuttaan informoi vain 46 % vastaajista. (Taulukko 13.)

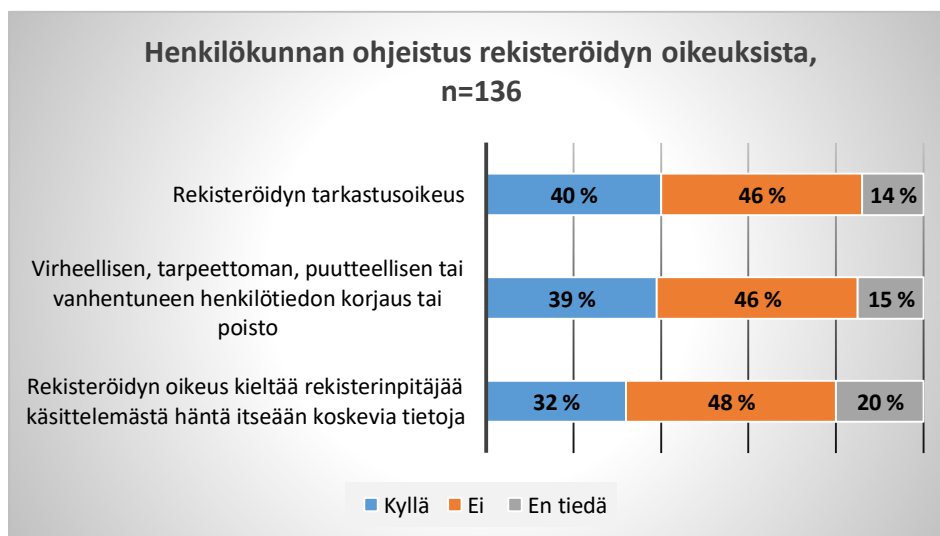
TAULUKKO 13. Kaikki vastaajat rekisteröidyn informoinnista



Kuntayhtymissä vaihteluväli rekisteröinnin informoinnissa oli 50–90 % välillä. Heikoiten informoitiin sitä, siirretäänkö tietoja EU:n tai Euroopan talousalueen ulkopuolelle (50 %), parhaiten informoitiin henkilötietojen käsittelyn tarkoituksesta (90 %) ja mihin rekisteröityjen ryhmään henkilötietoja kerättiin (90 %). Maakuntien liitoilla vaihteluväli oli 11–100 %, heikoiten informoitiin rekisteröityä siitä, miten hän voi käyttää tarkastusoikeutta (11 %) ja parhaiten mihin rekisteröityjen ryhmään tietoa kerättiin (100 %). Keskiarvo informoinnin osalta maakuntien liitoilla oli 53 %. Kuntien osalta vaihteluväli informoinnin osalta oli 41–75 %. Heikoiten oli informoitu tietojen siirrosta EU:n tai Euroopan talousalueen ulkopuolelle ja parhaiten siitä, mihin rekisteröityjen ryhmään henkilötietoja kerättiin. Pienissä kunnissa informoinnin keskiarvo oli 53 %, keskisuurissa 61 % ja suurissa kunnissa 79 %.

Taulukosta 14 ilmenee, miten organisaatioissa oli ohjeistettu henkilökuntaa rekisteröidyn oikeuksista. Rekisteröidyn oikeuksista oli ohjeistusta 32-40%:lla organisaatioista siten, että tarkastusoikeus oli parhaiten ohjeistettu.

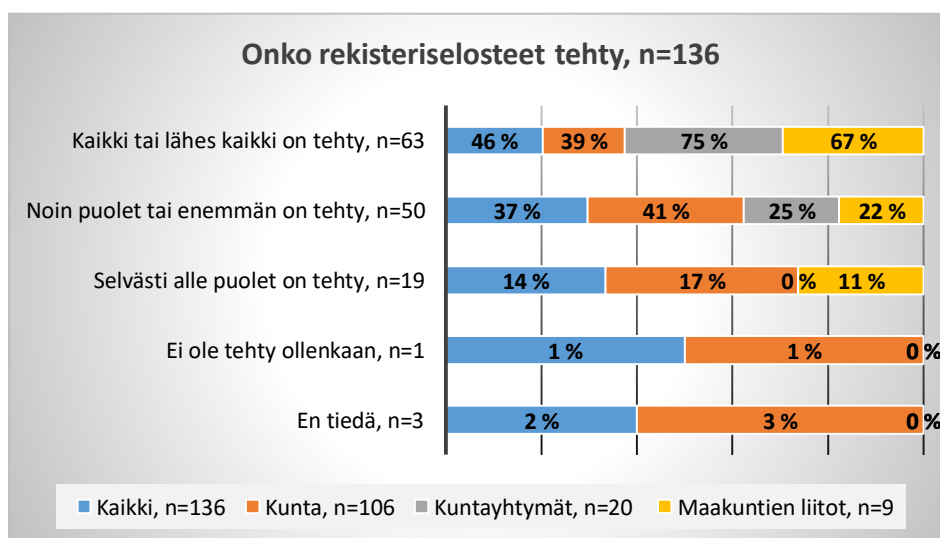
TAULUKKO 14. Kaikki vastaajat organisaation ohjeistuksesta



6.5.4 Rekisteriseloste

Kysymykset 14–16 koskivat rekisteriselosteen olemassaoloa, oliko rekistereille määriteltä yhteyshenkilö ja olivatko rekisteriselosteet rekisteröityjen saatavilla. (Taulukko 15.)

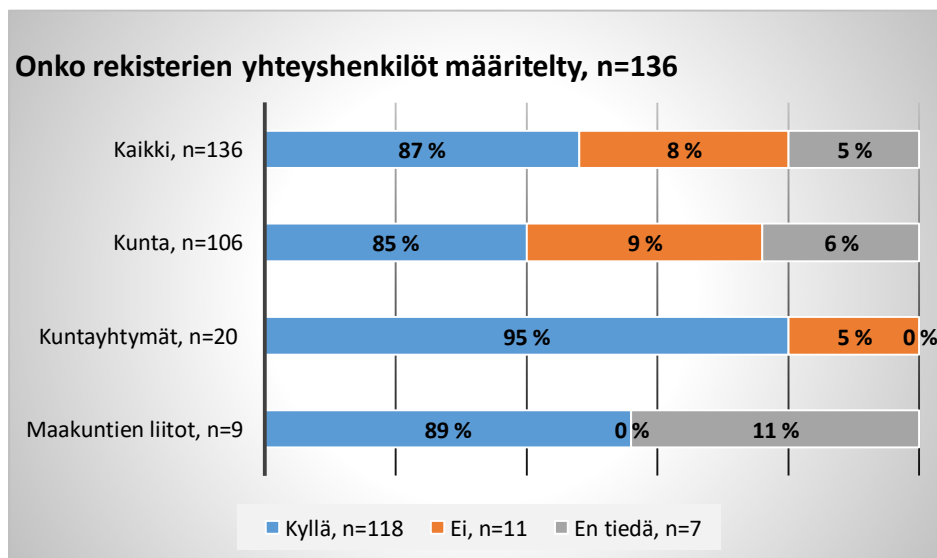
TAULUKKO 15. Onko rekisteriselosteet tehty



Kaikista organisaatioista rekisteriselosteet oli tehty kokonaan tai yli puolet 83 %:lla vastaajista. Kuntien vastaava luku oli 80 %, kuntayhtymien prosenttiluku oli 100 ja

maakuntien liitoissa 89 %. Kuntien välisissä vertailuissa pienissä kunnissa prosenttiluku oli 71 %, keskisuurissa kunnissa 84 % ja isoissa kunnissa 100 %. (Taulukko 15).

TAULUKKO 16. Onko rekisterien yhteyshenkilö määritelty



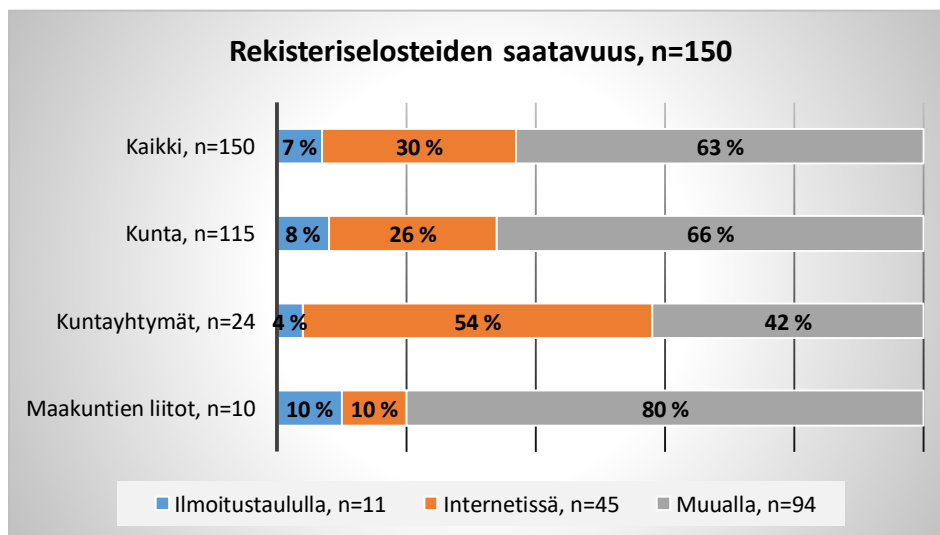
Myös rekisterien yhteyshenkilöt oli hyvin määritelty organisaatioissa. Taulukon 16 mukaan kaikkien vastaajien osalta rekistereiden yhteyshenkilö oli määritelty 87 %:lla, (kunnat 85 %, kuntayhtymät 95 %, maakuntien liitot 89 %). Kuntien välisessä vertailussa pienten kuntien luku oli 78 %, keskisuurten kuntien 91 % ja suurten kuntien 100 %.

Seuraava kysymys käsitteli sitä, olivatko rekisteriselosteet rekisteröityjen saatavilla. Tähän kysymykseen oli mahdollista valita monta vaihtoehtoa. Vastauksia tuli kaikkiaan 150 kappaletta. Suurin osa vastaajista 63 % (kunnat 66 %, kuntayhtymä 42 % ja maakuntien liitot 80 %) ilmoittivat, että rekisteriselosteet olivat saatavilla muualla kuin internetissä tai ilmoitustauluilla. Toiseksi suosituin tapa oli se, että rekisteriselosteet olivat internetissä, kaikissa organisaatioissa luku oli 30 %, kunnissa 26 %, kuntayhtymissä 54 % ja maakuntien liitoissa 10 %. Vähiten käytetty menetelmä oli laittaa rekisteriselosteet ilmoitustaululle (7 %). (Taulukko 17).

Kuntien välisessä vertailussa pienillä kunnilla suosituin oli ilmoittaa muualla 76 %, internetissä 15 % ja ilmoitustaululla 10 %. Keskisuurissa kunnissa suosituin oli muualla 65 %, ilmoitustaululla 3 % ja internetissä 33 %. Suurissa kunnissa suosituin tapa laittaa

rekisteriselosteet rekisteröityjen saataville oli internet 56 %, muualla 31 % ja vähiten ilmoitustauluille 13 %.

TAULUKKO 17. Ovatko rekisteriselosteet rekisteröityjen saatavilla



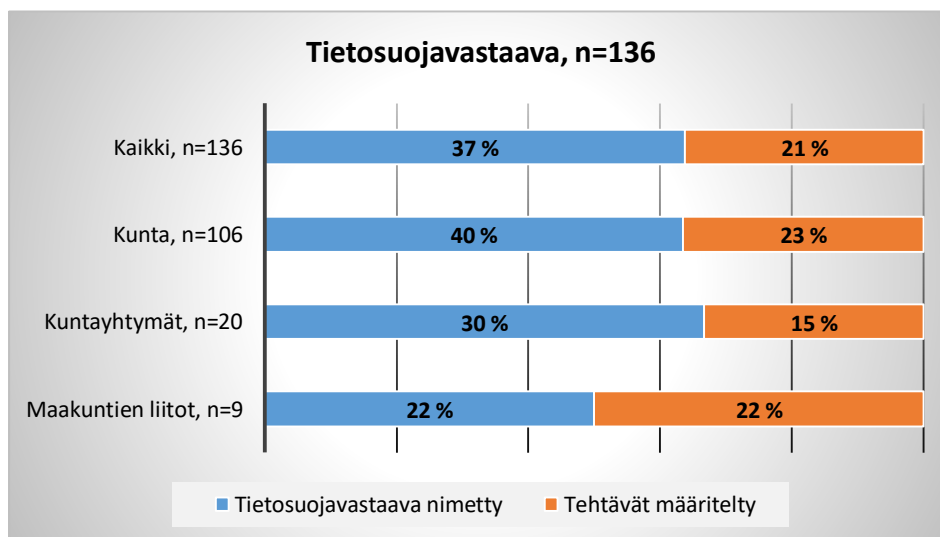
Vastaajia pyydettiin kertomaan mikä tämä muu tapa oli, jolla he laittavat rekisteriselosteet rekisteröityjen saataville. Vastauksia tuli kaikkiaan 86 kappaletta. Näistä vastauksista kävi ilmi, että suurin osa (32 kpl) ilmoitti, että rekisteriselosteet löytyvät kirjaimosta, neuvonnasta, asiakaspalvelupisteessä, tietopalvelussa, infopisteessä, palvelupisteessä tai asianhallintasihteerin työhuoneessa. Muita paikkoja rekisteriselosteelle olivat eri toimipisteet (13 kpl), arkistonhoitajan hallussa (9 kpl), intranet (9 kpl) ja asianhallintajärjestelmät (4 kpl). Yhdeksän vastaajaa ilmoitti, että rekisteriselosteet sai pyydettäessä tai johtajalta kysyttäessä. Loput vastaajat ilmoittivat, että rekisteriselosteet olivat vasta suunnitteilla, erilaisissa kansioissa, www-sivuilla tai ilmoitustaululla oli tieto, mistä rekisteriselosteet löytyvät.

6.5.5 Tietosuojavastaava

Tietosuojavastaavan nimeämistä ja tehtävänkuvasta käsiteltiin kysymyksissä 17–18. Taulukosta 18 ilmenee, että kaikkien organisaatioiden osalta tietosuojavastaava oli nimetty 37 %:lla ja tehtävät määritelty 21 % organisaatioista. Vertailuissa organisaatioiden välillä vastaavat luvut olivat: kuntayhtymistä 30 % ilmoittivat, että tietosuojavas-

taava oli nimitetty ja tehtävät oli määritelty 15 %:lla. Maakuntien liittojen osalta vastaavat luvut olivat 22 % ja 23 %. Kuntien välisessä vertailussa tietosuojavastaava oli nimetty seuraavasti: pienet kunnat 32 %, keskisuuret kunnat 46 %, suuret kunnat 58 % ja tehtävät määritelty: pienet kunnat 12 %, keskisuuret kunnat 30 %, suuret kunnat 50 %.

TAULUKKO 18. Tietosuojavastaava on nimetty ja tehtävät määritelty



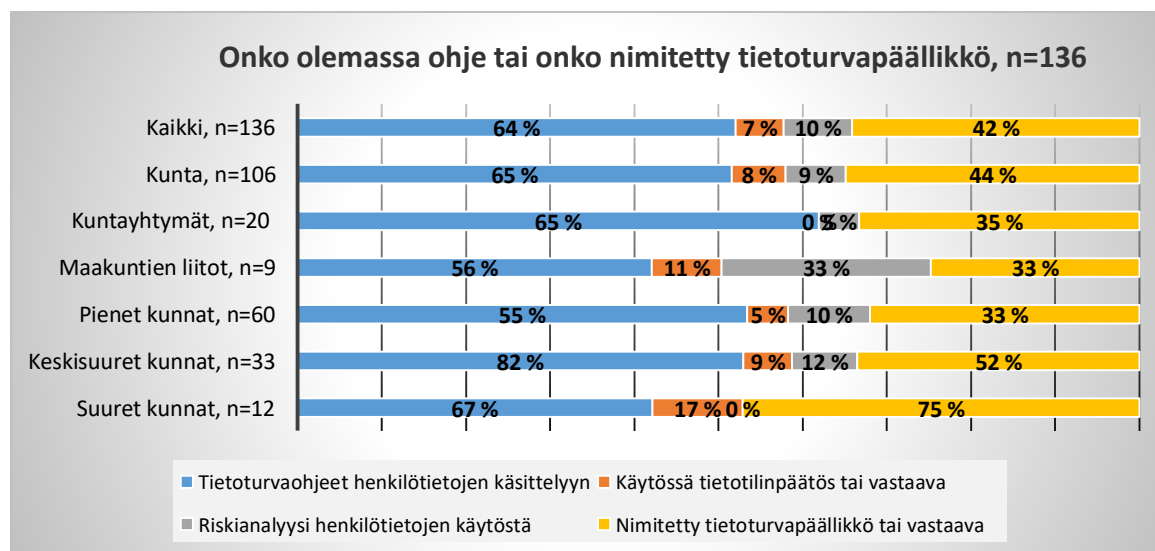
Kysymykseen siitä, missä tietosuojavastaavan tehtävät oli määritelty, tuli yhteensä 36 vastausta. Suurin osa vastaajista ilmoitti, että tietosuojavastaavan tehtävät oli määritelty tehtäväkuvauksessa, kymmenen vastaajaa ilmoitti, että asia oli vasta valmistelussa tai rekrytointi meneillään. Kahdeksan ilmoitti, että tehtävät oli määritelty johtosäännössä, kaupunginhallituksessa tai hallintosäännössä. Loput viisi ilmoitti, että tietosuojavastaavan tehtävät oli määritelty tietoturvasuunnitelmissa tai tietoturvapoliitikassa.

6.5.6 Tietoturva ja riskienhallinta

Kysymys numero 19 käsitteli tietoturvaa ja riskienhallintaa. Kaikista organisaatioista tietoturvaohjeet olivat käytössä 64 %:lla, tietotilinpäätös 7 %:lla, riskianalyysi 10 %:lla ja tietoturvapäällikkö tai vastaava oli nimitetty 42 %:lla. Kuntien välisessä vertailussa tietoturvaohjeet löytyivät seuraavasti: kaikki kunnat 65 %, pienet kunnat 55 %, keskisuuret 82 % ja suuret kunnat 67 %. Kuntayhtymissä tietoturvaohjeet oli tehty 65 %:lla ja maakuntien liitoissa 56 %:lla. Tietotilinpäätös tai vastaava oli tehty kaikissa kunnissa 8

% (pienet kunnat 5 %, keskisuuret 9 %, suuret kunnat 17 %), kuntayhtymissä 0 % ja maakuntien liitoissa 11 %. Riskianalyysi oli tehty kaikissa kunnissa 9 % (pienet kunnat 10 %, keskisuuret 12 %, suuret kunnat 0 %), kuntayhtymät 5 % ja maakuntien liitot 11 %.

TAULUKKO 19. Onko olemassa ohje tai onko nimitetty tietoturvapääällikkö



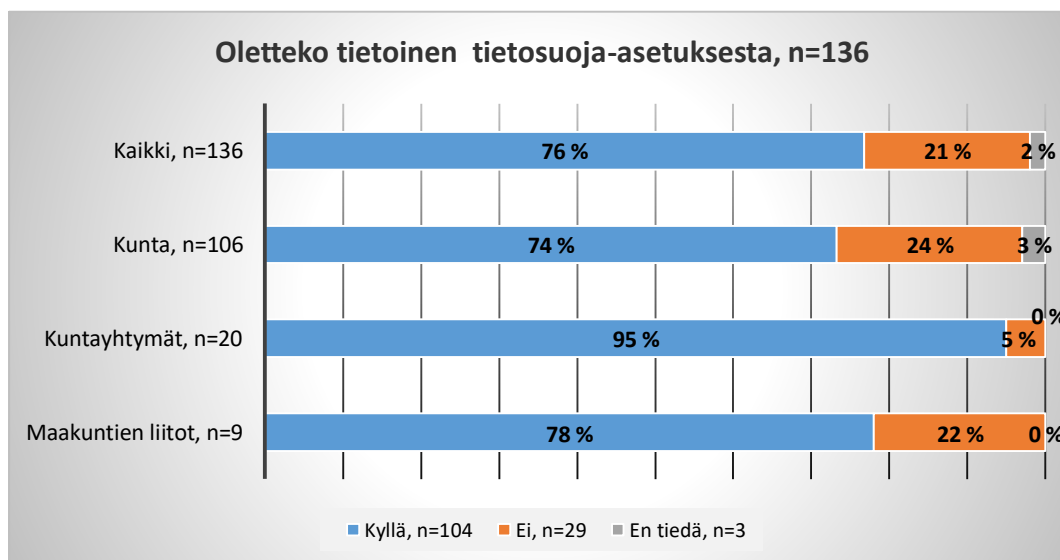
Tietoturvapääällikkö tai vastaava oli nimitetty kaikissa kunnissa 44 %:lla (pienet kunnat 33 %, keskisuuret 52 %, suuret kunnat 75 %). Kuntayhtymillä tietoturvapääällikkö oli nimitetty 35 %:lla ja maakuntien liitoissa 3 %:lla.

6.5.7 Valmistautuminen tietosuoja-asetukseen

Viimeiset kuusi kysymystä käsittelevät sitä, miten rekisterinpitäjät olivat valmistautuneet tulevaan tietosuoja-asetukseen. Taulukossa 20 kuvataan sitä, ovatko eri organisaatiot saaneet tai hankkineet tietoa tulevasta tietosuoja-asetuksesta. Kaikista organisaatioista 76 % oli saanut tai hankkinut tietoa tulevasta tietosuoja-asetuksesta. Paras tilanne oli kuntayhtymillä, vastaajista jopa 95 % oli tietoinen tulevasta muutoksesta. Organisaatioilta myös kysyttiin, mistä he olivat saaneet tai hankkineet tietoa koskien tietosuoja-asetusta. Suurin osa vastaajista ilmoitti, että tietoa oli saatu internetistä, koulutustilaisuuksista, sähköpostilla, Kuntaliitosta, valtiovarainministeriöstä, oikeusministeriöstä, tietosuojavaltuutetun sivustolta ja myös eri yhteistyötahoilta. Muutama vastaaja ilmoitti,

että he olivat lukeneet tietosuoja-asetuksen virallisesta lehdestä. 61 % kaikista vastaajista myös tiesivät, minkälaisia muutoksia on tulossa (kunnat 58 %, kuntayhtymät 90 %, maakuntien liitot 44 %).

TAULUKKO 20. Oletteko tietoinen tietosuoja-asetuksesta



Kuntia vertailtaessa pienissä kunnissa tiedettiin, että muutoksia on tulossa 43 %:a vastauksista, keskisuurissa 76 % ja suurissa kunnissa 85 %. Vastauksia siihen, mitä nämä muutokset tulevat olemaan tuli paljon. Vastaukset jakautuivat seuraaviin ryhmiin: tietosuojavastaava, rekisterinpitäjän velvollisuudet, rekisteröidyn oikeudet, muutoksia sopimukseen, ohjeisiin, dokumentointiin, muutoksia toimintapainiin ja prosesseihin, sanktiot ja rekisteriselosteet. Esimerkiksi eräs vastaaja kirjoitti seuraavasti kysyttäessä mitä muutoksia on tulossa:

”tietosuojavastaavan nimeäminen, korvausvastuu, sopimukset henkilötietojen käsittelystä, ilmoitusvelvollisuus henkilötietojen tietoturvaloukkauksista, hallinnolliset sakot, varmistettava riittävän tietosuoja taso henkilötietojen siirroissa EU:n/ETA:n ulkopuolelle”

Vastauksista tuli myös osittain esiin se, että kaikki ei ole vielä selvää.

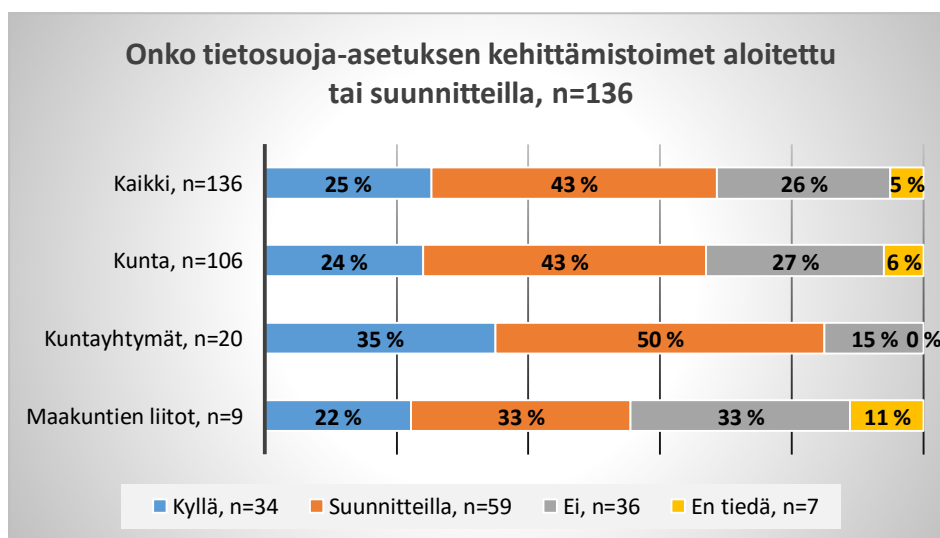
”Asiat ovat vielä tarkentumatta, mutta muutoksia tiedetään olevan tulossa”

Esille tuli myös, että muutos aiheuttaa paljon työtä kunnissa ja asia vaatii tietoisuuden lisäämistä. Eräs vastaajista ilmoitti, että muutoksista on mahdotonta tehdä listausta.

”Vi är medvetna om förändringarna. Ej möjligt att lista upp i detta fält”.

Seuraavaksi kysyttiin, kuinka organisaatiot olivat valmistautuneet tietosuoja-asetukseen tuloon. Oliko kehittämistoimet aloitettu, suunnitteilla vai eikö mitään ollut vielä tehty.

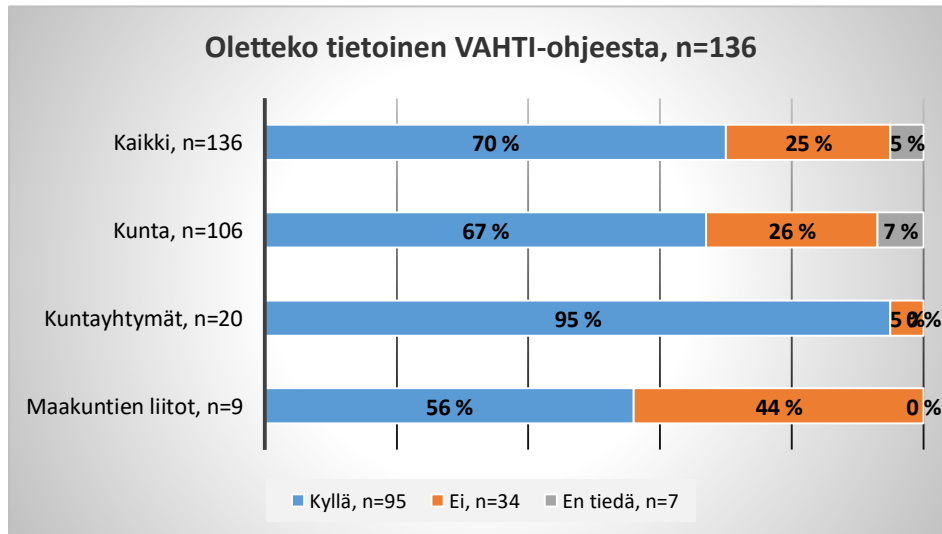
TAULUKKO 21. Tietosuoja-asetuksen kehittämistoimet aloitettu tai suunnitteilla



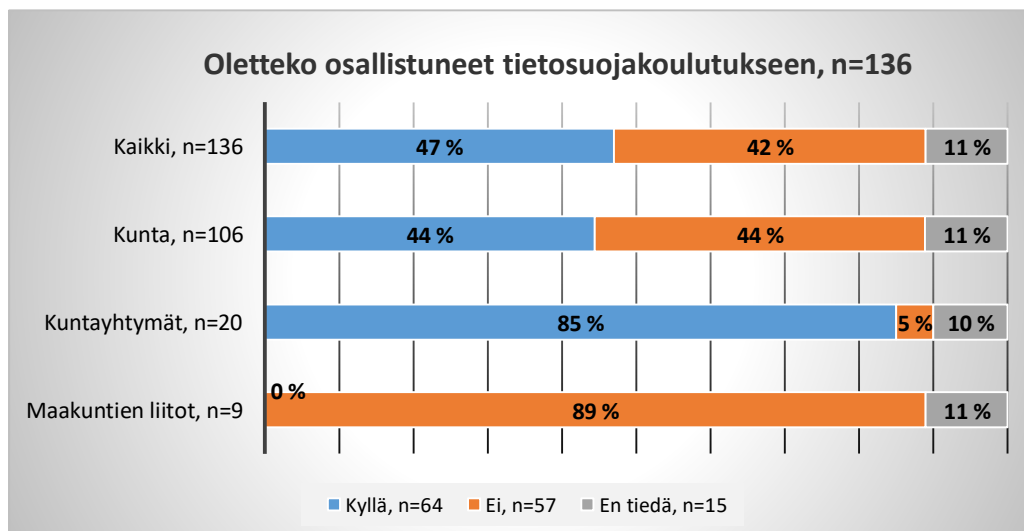
Taulukosta 21 ilmenee, että kaikissa organisaatioissa kehittämistoimet oli aloitettu tai suunnitteilla 68 %:lla. Kunnissa vastaava luku oli 67 %, kuntayhtymissä 85 % ja maakuntien liitoissa 55 %. Kuntien välisessä vertailussa vastaavat luvut olivat pienissä kunnissa 60 %, keskisuurissa 69 % ja suurissa kunnissa 100 %. Kuitenkin kaikista vastaajista 26 % ei ollut vielä tehnyt mitään.

Vastaajilta kysyttiin myös ovatko he lukeneet tietosuoja-asetuksen ohjeeksi tehtyä valtiovarainministeriön julkaisemaa VAHTI-ohjetta. (Taulukko 22). Ohje oli hyvin tiedoissa organisaatioissa. Kaikista organisaatioista VAHTI-ohjeeseen oli tutustunut 70 % organisaatioista. Kunnissa luku oli 65 %, kuntayhtymissä 95 % ja maakuntien liitoissa 56 %.

TAULUKKO 22. Oletteko tietoinen VAHTI-ohjeesta



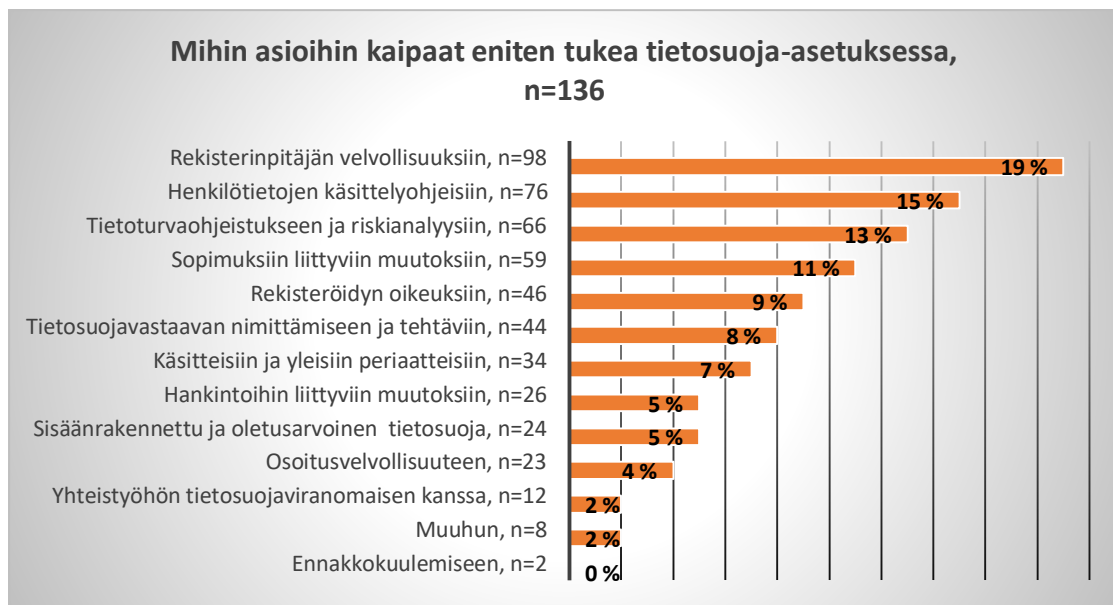
TAULUKKO 23. Oletteko osallistuneet tietosuojakoulutukseen



Lisäksi haluttiin tietää organisaatioiden osallistumisesta tietosuojakoulutukseen. Taulukosta 23 käy ilmi, että kaikista vastaajista vajaa puolet (47 %) ilmoitti osallistuneensa

koulukseen. Kuntien osuus oli 44 % ja kuntayhtymien 85 %. Maakuntien liitoissa ei ole osallistuttu ollenkaan tietosuojakoulutuksiin tai ainakaan kyseiset vastaajat eivät olleet siitä tietoisia. Kuntien välissä vertailuissa pienissä kunnissa osallistumisprosentti koulutuksiin oli 35 %, keskisuurissa 52 % ja suurissa kunnissa 75 %. Tutkimuksella haluttiin myös selvittää, minkälaisiin asioihin vastaajat kaipaavat tukea tulevassa tietosuoja-asetus uudistuksessa. (Taulukko 24).

TAULUKKO 24. Mihin asioihin kaipaavat eniten tukea tietosuoja-asetuksessa



Vastaajat saivat valita neljä tärkeintä asiaa. Eniten haluttiin tukea rekisterinpitäjän velvollisuuksiin (19 %), toiseksi henkilötietojen käsittelyohjeisiin (15 %), kolmanneksi tietoturvaohjeistukseen ja riskianalyyseihin (13 %) ja neljänneksi sopimukseen liittyviin muutoksiin (11 %). Mutta myös muut alueet saivat tasaisesti kannatusta. Tukea kaivattiin muun muassa käsitteisiin, yleisiin periaatteisiin, rekisteröidyn oikeuksiin, hankintoihin ja osoitusvelvollisuuksiin. Lopuksi vastaajat saivat ilmoittaa, mihin muuhun he halusivat tukea. Vastaajat ilmoittivat haluavansa konkreettisia, lyhyitä ohjeita ja malleja muun muassa tietotilinpäätökseen ja miten tarvittavat tietojärjestelmämuutokset saadaan aikaan. Tietoja kaivattiin siitä, miten julkisuuslaki ja asiakirjahallinto kytkeytyvät tietosuoja-asetukseen ja arkistoitujen henkilötietojen käsittelyyn. Toivottiin myös ruotsinkielistä koulutusta.

Kyselyn viimeisessä kysymyksessä annettiin vastaajille mahdollisuus kommentoida tietosuoja-asetukseen liittyviä asioita. Vastaukset käsittelivät seuraavia aihe-alueita: asia (tietosuoja-asetus) on uusi, lainsäädäntö on vielä vaiheessa, muitakin muutoksia on tulossa paljon ja uudistus vaatii paljon resursseja. Vastaajat toivoivat yhteisiä toimintamalleja ja asiakirjamalleja, muun muassa yhteistä tietosuojaseloste-mallia sekä nykytilan kuvausta ja miten päästään tavoitteisiin. Eräs vastaaja toivoi tukea sähköisen asiointiin liittyviin kysymyksiin. Eräs vastaaja kirjoitti asenteesta tietosuojaan seuraavasti:

”xxx kunnassa tietosuojaan on aina suhtauduttu vakavasti. Vaikka kirjallisia ohjeita ei vielä ole rekisteriselostetta enempää, asioista on tiedotettu ja ohjeistettu työntekijöitä sekä rekisteröityä suullisesti.”

6.6 Yhteenveto arviointitutkimuksen ja kyselytutkimuksen tuloksista

Tässä kappaleessa tehdään yhteenveto arviointitutkimuksen ja kyselytutkimuksen tuloksista tiedon elinkaarimallin mukaisesti: toimenpiteet ennen käsittelyn aloittamista, toimenpiteet henkilötietojen käsittelyn aikana ja toimenpiteet käsittelyn perusteen lakattua ja ylläpitovaihe. Arviointitutkimuksessa tehtyä yhteenvetoa tietosuoja-asetuksen vaatimuksista rekisterinpitäjille on täydennetty kyselytutkimuksen tulosten perusteella. Yhteenveto perustuu kaikkien kyselytutkimukseen organisaatioiden (kunnat, kuntayhtymät, maakuntien liitot) vastauksiin. Tason määrittämiseen käytettiin seuraavaa tasotaulukkoa:

0-40 %	◆	punainen, heikko tai uusi asia, vaatii välitöntä kehittämistä
40-80 %	■	keltainen, tyydyttävä, vaatii kehittämistä
80-100 %	●	vihreä, hyvä, vaatii päivitystä

Punaisen värin saavat asiat vaativat välitöntä kehittämistä tai ovat uusia asioita tietosuoja-asetuksessa, keltaiset ovat tyydyttävässä kunnossa ja vaativat kehittämistä, vihreiden osalta asioita suositellaan päivitettäväksi vastaamaan tietosuoja-asetusta.

6.6.1 Toimenpiteet ennen henkilötietojen käsittelyn aloittamista

Rekisterinpitäjän vastuulla on tietosuoja-asetuksen 24. artiklan mukaan toteuttaa tarvittavat tekniset ja organisatoriset toimenpiteet, joilla voidaan varmistaa ja osoittaa, että henkilötietojen käsittelyssä noudatetaan tietosuoja-asetusta. Rekisterinpitäjän on toimeenpantava henkilötietojen käsittelyä koskevat toimintaperiaatteet. Näitä toimintaperiaatteita voi osoittaa muun muassa käytäntösäännöillä (40 art.) ja sertifiointilla (42 art.) Kyselyn mukaan organisaatioissa oli huomioitu tyydyttävästi (75 %) henkilötietojen käsittely ja tiedonhallinta yleisesti strategiassa tai kehittämistoiminnassa. Kuitenkin, jos tietyn tyyppinen, esimerkiksi uusi teknologia aiheuttaa suuren riskin rekisteröidyn oikeuksille ja vapauksille on rekisterinpitäjän suoritettava tietosuojaa koskeva vaikutustenarviointi (35 art.) ja siihen liittyvä valvontaviranomaisen ennakkokuuleminen (36 art.). Näin ollen organisaatioissa punaisella olevia asioita on selvittää, tarvitaanko vaikutustenarviointia ja ennakkokuulemisia sekä ottaa käyttöön mahdollisuuksien mukaan käytänteitä ja sertifikaatteja. (Taulukko 25.)

Henkilötietojen lainmukaisen käsittelyn periaatteet ja käsittelyn kannalta tarpeellista tietoa käsitellään tietosuoja-asetuksessa 5. artiklassa. Henkilötietolaissa samat vaateet on säädetty pykälissä 5-7. Henkilötietolain mukaan rekisterinpitäjällä on huolellisuusvelvoite, suunnitteluelvoite ja henkilötietoja saa kerätä vain määriteltyyn käyttötarkoitukseen. Kyselyn mukaan käyttötarkoitus oli organisaatioissa hyvällä tasolla (95 %). Tässä kyselyssä kysyttiin organisaatioilta suunnittelusta (mainittu edellä) ja käyttötarkoitussidonnaisuudesta, mutta muita tietosuoja-asetuksessa mainittuja henkilötietojen käsittelyä koskevat periaatteita ei kysytty. Näitä ovat: lainmukaisuus, kohtuullisuus, läpinäkyvyys, tietojen minimointi, täsmällisyys, säilytyksen rajoittaminen, eheys ja luottamuksellisuus. (Taulukko 25.)

Organisaatioissa oli hyvällä tasolla se, kenellä on oikeus käsitellä henkilötietoja. 84 % vastaajista ilmoitti, että henkilötietojen käsittelyoikeudet on määritelty kokonaan tai osittain. Tietosuoja-asetuksessa 28. artiklassa käsitellään henkilötietojen käsittelijän velvollisuuksia sekä miten rekisterinpitäjän on ohjeistettava henkilötietojen käsittelijää sopimuksella ja ohjeilla (28 art.). Henkilötietojen käsittelyyn liittyvä ohjeistuksen vaihteluväli oli 30–87 %. Heikolla tasolla oli ohjeistus suostumuksen käsittelystä (30 %).

Tyydyttävällä tasolla oli ohjeistus koskien henkilötietojen (61 %), henkilötunnuksen (53 %) ja arkaluonteisten tietojen käsittelyä (61 %). Hyvällä tasolla oli ohjeistus koskien asiakirjallisen tiedon säilyttämisen periaatteita (87 %). Heikkoa oli myös ulkopuolisten tietojärjestelmätoimittajien ja ulkopuolisten ostopalveluiden ohjeistus. Eri tapojen ohjeistuksen vaihteluväli oli 16–46 %. Heikolla tasolla oli ohjeistus erillisillä ohjeilla (20 %) ja muulla tavalla (16 %). Tyydyttävällä tasolla oli sopimuksissa huomiodut ohjeet (46 %). Uutena asiana tietosuoja-asetuksessa on mahdollisuus yhteisrekisterinpitoon (26 art.) Jos organisaatio ottaa käyttöön yhteisrekisterin pidon toisen rekisterinpitäjän kanssa, on tästä tehtävä sopimus tai vastaava läpinäkyvä dokumentti. Lisäksi rekisterinpitäjä voi ottaa käyttöön vakiosopimuslausekkeitä rekisterinpitäjän ja henkilötietojen käsittelijän välisiin sopimuksiin (28 art.). Yhteisrekisterinpito ja vakiosopimuslausekkeet on merkitty punaisella, eli kehittämiskohteiksi, jos asiat ovat ajankohtaisia organisaatioissa. (Taulukko 25.)

Tietosuoja-asetuksen 25. artiklan vaatimus sisäänrakennetusta ja oletusarvoisesta tietosuojasta on uusi asia rekisterinpitäjälle. Rekisterinpitäjällä on osoitusvelvollisuus siitä, että henkilötietojen käsittelyä koskevia periaatteita noudatetaan. Periaatteet on määritelty erikseen artiklassa 5. Taulukossa 25 tämä alue on merkitty punaisella, eli välittömästi kehitettäväksi. (Taulukko 25.)

Henkilötietolain nojalla tehtävät rekisteriselosteet oli tehty tyydyttävästi (46 %) ja rekistereiden yhteyshenkilöt henkilöt oli määritelty hyvin (87 %). Sen sijaan hajontaa tuli siihen, olivatko rekisteriselosteet rekisteröityjen saatavilla. Vastaajista 7 % piti niitä ilmoitustaululla, 30 % internetissä ja 63 % jossain muualla. Tietosuoja-asetuksen (30 art.) vaatimus siitä, että selosteen on oltava sekä kirjallinen että sähköinen ei tällä hetkellä toteudu, jos rekisteriselosteet ovat pääosin muualla kuin internetissä. Nämä jossain muualla-vastaukset sisälsivät muun muassa sisäiseen käyttöön tarkoitetun intranetin, eri toimipisteet, tietojärjestelmät tai rekisteriselosteet olivat eri henkilöiden takana ja ne sai erikseen pyydettyä. Tietosuoja-asetuksen (30 art.) vaatimus selosteiden tekemisestä koskien käsittelytoimia on säädetty myös rekisterinpitäjän lukuun toimivalle henkilötietojen käsittelijälle ja lisäksi seloste sisältää uusia asioita, kuten vaatimuksen tietosuoja-

vastaavan yhteystietojen ilmoittamisesta ja eri tietoryhmien poistamisen suunnitelluista määräajoista. (Taulukko 25.)

TAULUKKO 25. Toimenpiteet ennen henkilötietojen käsittelyn aloittamista

Tietosuoja-asetus	Kysely	Lähtötilannetilanne
Ennakkokuuleminen ja vaikutustenarviointi Käytännösäännöt ja sertifiointimenettely Rekisterinpitäjän vastuu Henkilötietojen käsittelyn ja tiedonhallinnan kytkeminen strategiaan ja kehittämis-toimintaan	75 %	<ul style="list-style-type: none"> ◆ Uusi asia: tekniset ja organisatoriset toimenpiteet (käytännösäännöt, sertifiointi), vaikutustenarviointi ja ennakkokuuleminen ■ Suunnitelmallisuus (huomioitu strategiassa tai kehittämistoiminnassa)
Lainmukaisen käsittelyn periaatteet ja käsittelyn kannalta tarpeellinen tieto, osoitusvelvollisuus	94 %	<ul style="list-style-type: none"> ● Käyttötarkoitus ◆ Ei kysytty: lainmukaisuus, kohtuullisuus, läpinäkyvyys, tietojen minimointi, täsmällisyys, säilytyksen rajoittaminen, eheys, luottamuksellisuus.
Käyttäjien oikeudet määrittely	84 %	<ul style="list-style-type: none"> ● Käyttöoikeudet
Suostumusmenettely Ohjeistus henkilötietojen käsittelijöille Erityiset henkilötietoryhmät (arkaluonteiset) Hävittämisajat ja käytännöt	30 % 61 % ¹ , 53 % ² 61 % 87 %	<ul style="list-style-type: none"> ◆ Suostumus ■ Ohjeistus henkilötietojen¹ ja -tunnusten² käsittelystä ■ Arkaluonteisten henkilötietojen käsittelyohjeet ● Asiakirjallisen tiedon säilyttämisen periaatteet
Vakiosopimuslausekkeet Hankinnat ja sopimukset Yhteisrekisteri Ohjeistus ulkopuolisille }	20 % ¹ , 16 % ² 46 %	<ul style="list-style-type: none"> ◆ Uusi asia: sopimus yhteisrekisterinpidosta ja Ei kysytty: vakiosopimuslausekkeet, huomiointi hankinnoissa ◆ Erilliset ohjeet¹, muu tapa ohjeistaa² ■ Ohjeistus sopimuksessa
Sisäänrakennettu ja oletusarvoinen tietosuojavaatimus		<ul style="list-style-type: none"> ◆ Uusi asia: sisäänrakennettu ja oletusarvoinen tietosuoja henkilötietojen käsittelyä koskevien periaatteiden mukaiseksi
Seloste käsittelytoimista ja niiden saatavuus	7 % ¹ ilm. taulu 30 % ¹ internet 63 % ¹ jossain muualla 46 % 87 %	<ul style="list-style-type: none"> ◆ Rekisteriselosteiden saatavuus¹ ◆ Uudet vaatimukset rekisteriselosteelle (säilytysajat, tietosuojavastaava, ulkopuoliset henkilötietojen käsittelijät, kirjallinen + sähkö.) ■ Rekisteriselosteet tehty ● Rekistereiden yhteyshenkilö määritelty
Tietosuojavastaava	37 % ¹ , 21 % ²	<ul style="list-style-type: none"> ◆ Uusi asia: tietosuojavastaavan nimitys¹ ja tehtävien määrittely²
Tietoturva ja riskienhallinta Riskilähtöisyys	7 % ¹ , 10 % ² 42 % 64 %	<ul style="list-style-type: none"> ◆ Tietotilin päätös¹, riskianalyysi² ■ Tietoturvapäällikkö tai vastaava ■ Tietoturvaohjeet

Selosteen uudet asiat, muoto ja sisältö sekä vaatimus myös henkilötietojen käsittelijöille on merkitty punaisella, eli välittömiksi kehittämiskohteiksi. Sinänsä organisaatioilla oli

hyvällä tasolla asiakirjallisten tietojen säilyttämisen periaatteet; nämä tiedot on jatkossa löydettävä myös tietosuoja-asetuksen mukaisesta selosteesta. (Taulukko 25.)

Tietosuojavastaava tulee pakollisesti kaikille organisaatiolle vasta tietosuoja-asetuksessa (37 art.). Kaikista organisaatioista 37 % ilmoitti, että tietosuojavastaava on nimetty ja tehtävät määritelty 21 %:lla, joten tilanne on heikko ja merkitty punaisella. Tietosuoja-asetus painottaa tietoturvan huomioonottamista henkilötietojen käsittelyssä sekä ennakoivaa riskienhallintaa (32 art.). Tietoturvaohjeita organisaatioista löytyi tyydyttävästi, 64 %:lla. Sen sijaan tietotilinpäätös oli käytössä vain 7 %:lla, samoin myös riskianalyysi oli heikosti käytössä, vain 10 %, vaihteluväli oli 0-33 %. Tietoturvapäällikkö tai vastaava löytyi tyydyttävästi organisaatioista, luku oli 42 %, mutta vaihteluväli oli iso, 3-75 %. Paras tilanne oli suurissa kunnissa. (Taulukko 25.)

TAULUKKO 26. Toimenpiteet henkilötietojen käsittelyn aikana

Tietosuoja-asetus	Kysely	Lähtötilannetilanne
Tietojen saanti ja luovutusten hallinnointi	40 %	◆ Luovutus EU:n tai Euroopan talousalueen ulkopuolelle
Rekisteröidyn tunnistaminen ja informointi oikeuksien toteuttamisesta	46 % ¹ , 51 % ² , 60% ³ , 66% ⁴ , 66% ⁵ , 76% ⁶ , 79 % ⁷	■ Tarkastusoikeuden käyttö ¹ , suojauksen periaatteet ² , tietojen luovutus ³ , mistä tiedot hankittu tai saatu ⁴ , tiedot rekisterinpitäjältä ⁵ , käsittelyn tarkoitus ⁶ , mihin rekisteröityjen ryhmään tietoja kerätään ⁷
Ohjeistus ja ylläpito rekisteröidyn oikeuksista	32 % ¹ , 39 % ² , 40 % ³	◆ Rekisteröidyn oikeus kieltää ¹ , korjata tai poistaa ² ja tarkistaa omia tietojaan ³ ◆ Uusi asia: uudet rekisteröidyn oikeudet (rajoittaminen, siirto, vastustaminen)
Menettelytavat ja ilmoitukset tietoturvaloukkauksista		◆ Uusi asia: ilmoitukset tietoturvaloukkauksista

Rekisterinpitäjän velvollisuuksiin kuuluu muun muassa informoida rekisteröityä hänen oikeuksistaan ja miten hän voi oikeuksiaan käyttää. Tulosten mukaan heikoiten informoitiin rekisteröityä siitä, luovutetaanko tietoja EU:n tai Euroopan talousalueen ulkopuolelle (40 %). (Taulukko 26). Tyydyttävällä tasolla oli se, miten rekisteröity voi käyttää tarkastusoikeuttaan (46 %), henkilörekisterin suojauksen periaatteet (51 %), mihin henkilötietoja säännönmukaisesti luovutetaan (60 %), mistä rekisteröidyn tiedot on hankittu tai saatu sekä tieto rekisterinpitäjältä ja sen mahdollisesta edustajasta (66 %). Li-

säksi tyydyttävällä tasolla oli henkilötietojen käsittelyn tarkoitus (76 %) ja mihin rekisteröityjen ryhmään henkilötietoja kerätään (79 %). Tietosuoja-asetuksessa rekisteröidyn oikeuksia käsitellään artikloissa 12–14. Tietosuoja-asetus täydentää rekisteröidyn oikeuksia suhteessa henkilötietolakiin muun muassa painottamalla informointia sekä rekisterinpitäjän velvollisuutta tunnistaa rekisteröity. (Taulukko 26.)

Rekisterinpitäjän tulee myös ohjeistaa henkilötietojen käsittelijöitä siitä, kuinka rekisteröity voi käyttää oikeuksiaan. Organisaatioissa ohjeistus oli heikkoa, vaihteluväli oli 32–40 %. Ohjeistus rekisteröidyn oikeudesta kieltää käsittelemästä omia tietojaan oli olemassa 32 %:lla. Ohjeistus siitä, kuinka virheellinen, tarpeeton, puutteellinen tai vanhentunut henkilötieto korjataan tai poistetaan, oli olemassa 39 %:lla. Ohjeistus siitä, kuinka rekisteröity voi tarkistaa omat tietonsa, oli olemassa 40 %:lla. Tietosuoja-asetuksessa rekisteröidyn oikeuksia säädellään artikloissa 15–23. Uusina oikeuksina on rekisteröidyn oikeus käsittelyn rajoittamiseen (18 art.), oikeus siirtää tiedot järjestelmästä toiseen (20 art.) ja vastustamisoikeus (21 art.). Uutena asiana tietosuoja-asetuksessa on myös velvollisuus ilmoittaa tietoturvaloukkauksista sekä valvontaviranomaisille että joissakin tapauksissa myös rekisteröidyille, näistä säädetään artikloissa 33–34. Nämä uudet oikeudet on merkitty taulukkoon punaisella, eli välittömiksi kehittämiskohteiksi. (Taulukko 26.)

Henkilötietojen elinkaaren viimeisessä vaiheessa on suunniteltava toimenpiteet käsittelyn perusteen lakattua ja ylläpitovaihe. Tietosuoja-asetuksen 5 artiklassa säädetään yleisistä käsittelyä koskevista periaatteista, sen mukaan henkilötietoja on säilytettävä muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan kuin on tarpeen tietojenkäsittelyn tarkoitusten toteuttamista varten. Henkilötietoja voidaan kuitenkin säilyttää pidempiä aikoja, jos henkilötietoja käsitellään ainoastaan yleisen edun mukaisia arkistointitarkoituksia taikka tieteellisiä tai historiallisia tutkimustarkoituksia tai tilastollisia tarkoituksia varten. Edellytyksenä on huolehtia käsittelyn turvallisuudesta (32 art.) sekä huomioida tietosuoja-asetuksen artikla 89 koskien arkistointia, tutkimusta ja tilastointia. (Taulukko 27.)

Kyselyn mukaan organisaatioissa on hyvällä tasolla asiakirjallisen tiedon säilyttämisen periaatteet 87 %. Näiden periaatteiden tulee ilmetä myös käytännössä. Uutena kehitettä-

vänä asia on tietosuoja-asetuksessa 25, 32 ja 40 artikloissa mainitut tietojen pseudonymisointi ja salaus. (Taulukko 27.)

TAULUKKO 27. Toimenpiteet käsittelyn perusteen lakattua ja ylläpitovaihe

Tietosuoja-asetus	Kysely	Lähtötilannetilanne
Tietojen siirto, hävitys, tarpeettoman tiedon poisto ja pseudonymisointi Tietojen käyttö arkistointiin, tieteelliseen tai historialliseen tutkimukseen tai tilastollisiin tarkoituksiin	87 %	<ul style="list-style-type: none"> ◆ Uusi asia: tietojen pseudonymisointi ja salaus ● Asiakirjallisen tiedon säilyttämisen periaatteet
Tietosuojan kehittäminen, tiedon hankkiminen ja kouluttautuminen	25 % 47 % 70 % ¹ , 76 % ²	<ul style="list-style-type: none"> ◆ Kehittämistoimet aloitettu ■ Osallistuttu koulutuksiin ■ Tieto VAHTI-ohjeesta¹ ja tietosuoja-asetuksesta²

Tietosuoja-asetuksen 24. artiklassa koskien rekisterinpitäjän vastuulla on toteuttaa tarvittavat tekniset ja organisatoriset toimenpiteet, joilla voidaan varmistaa ja osoittaa, että henkilötietojen käsittelyssä noudatetaan asetusta. Toimenpiteitä on tarkistettava ja päivitettävä tarvittaessa. Tämä edellyttää kehittämistoimia ja tietoa tietosuoja-asetuksen vaatimuksista. Heikosti eli vain 25 % organisaatioista olivat aloittaneet kehittämistoimet. Suunnitteilla kehittämistoimet olivat 43 %:lla vastaajista, mutta kolmasosa vastaajista sitä mieltä, ettei mitään ole vielä tehty tai ei ainakaan ole tiedossa, että jotain olisi aloitettu. (Taulukko 27.)

Tietosuojakoulutuksiin oli osallistuttu vaihtelevasti eri organisaatioissa. Keskimäärin vajaa puolet (47 %) oli käynyt koulutuksissa, mutta toisaalta yli puolet ei ollut osallistunut tai ei ainakaan tiennyt, että koulutuksiin olisi omasta organisaatioista osallistuttu. Kuntayhtymissä prosenttiluku oli suurin (85 %), mutta maakuntien liitoissa ei koulutuksiin ole osallistuttu ollenkaan tai ei ainakaan ollut tiedossa. Tietosuoja-asetuksen tulo oli tyydyttävästi tiedossa, prosenttiluku oli 76. Tietoa tietosuoja-asetuksesta oli hankittu perinteisesti osallistumalla koulutuksiin, lukemalla tietoa internetistä tai saamalla kohdistettua sähköpostia. Vähemmän oli luettu itse asetusta ja seurattu ministeriöiden sivustoja, poikkeuksena tietosuojavaaluttetun sivusto. Lisäksi Kuntaliiton nettisivustoja oli käyty lukemassa. Valtiovarainministeriön julkaisema VAHTI-ohje EU-tietosuojan ko-

konaisuudistuksesta oli tyydyttävästi (70 %) vastaajilla tiedossa. Kuntayhtymistä miltei kaikki olivat tietoisia ohjeesta. (Taulukko 27.)

Tukea vastaajat halusivat eniten rekisterinpitäjän velvollisuuksiin, tietoturva-asioihin ja henkilötietojen käsittelyohjeisiin. Huomattavaa on, että myös käsitteet ja yleiset periaatteet ja niistä kouluttaminen koettiin tärkeiksi. Vastaajat olivat tietoisia, että muutoksia tulee ja osittain myös siitä, millaisia muutoksia. Samalla oltiin huolissaan siitä, että menossa on niin paljon muutakin ja nämä asiat tuntuvat vaikeilta. Kaivattiin konkreettisia ja yksinkertaisia ohjeita ja malleja.

6.6.2 Rekisterinpitäjään kohdistuvat kehittämistoimet

Tässä kappaleessa kuvataan kehittämissuosituksen tietosuoja-asetusten vaatimusten ja nykytilakuvauksen perusteella. Kehittämissuosituksen on jaettu välitöntä kehittämistä vaativiin toimenpiteisiin, joihin kuuluvat tietosuoja-asetuksesta tulevat uudet asiat ja organisaatioiden nykytilanteen mukaan heikoiten noudatetut asiat. Toinen jako on tehty kehitettäviin ja päivitettäviin asioihin. Ne ovat asioita, joita tulee kehittää, jotta organisaatiot pääsevät tietosuoja-asetukseen vaatimuksiin. Liitteessä 6 on kuvattu asiat nämä ryhmiteltynä.

Organisaatioissa on välittömästi aloitettava kehittämistoimet tietosuoja-asetuksen valmistautumiseen, käytävä läpi asetuksen uudet käsitteet ja niiden merkitykset ja tietosuoja-asetuksen soveltamisala. Tietosuoja-asetus painottaa etukäiteistä suunnittelua ja riskianalyysien tekemistä. Tutkimuksen mukaan riskianalyysejä ei juurikaan organisaatioissa käytetä. Rekisterinpitäjän tulee luoda toimintatavat tietoturvaloukkauksille ja otettava käyttöön esimerkiksi tietotilinpäätös, missä voi osoittaa kuinka asiat toimivat organisaatiossa. Rekisterinpitäjällä on osoitusvelvollisuus siitä, että hän noudattaa tietosuoja-asetusta. Uusia asioita ovat myös vaikutustenarviointi ja ennakkokuuleminen, näitten käyttöönottoa tulee miettiä, mikäli ottaa käyttöön sellaista uutta teknologiaa, joka aiheuttaa korkean riskin henkilötietojen käytölle. Lisäksi tulevaisuudessa kehitetään yhteisiä käytäntöjä, menettelytapoja ja sertifioituja järjestelmiä, joita rekisterinpitäjä voi ottaa käyttöön.

Rekisterinpitäjän on välittömästi nimitettävä tietosuojavastaava ja määriteltävä hänen tehtävänsä. Näin tietosuojavastaava ehtii kouluttautua ja toimia neuvonantajana tietosuojaan liittyvissä asioissa. Rekisterinpitäjien on käytävä läpi lainmukaisen käsittelyn periaatteet ja se, miten ne näkyvät hallinnollisissa ja teknisissä toimintatavoissa. Vaikka tutkimuksen mukaan henkilötietojen käsittely ja yleinen tiedonhallinta oli huomioitu strategiassa tai kehittämistoiminnassa, se ei välttämättä kuitenkaan riitä osoittamaan, että tarvittavat tekniset ja organisatoriset toimenpiteet ovat tehty. Tietosuoja-asetuksen resitaalissa 78. sanotaan, että oikeus tietosuojaan on otettava huomioon tuotteita, palveluita ja sovelluksia kehittäessä. Tähän kuuluu myös tietosuoja-asetuksen vaatimus sisäänrakennetusta ja oletusarvoisesta tietosuojasta prosesseissa ja tietojärjestelmissä.

Tietosuoja-asetuksen vaatimukset on huomioitava hankinnoissa ja sopimuksissa. Jonkin verran sopimuksissa oli huomioitu tietosuoja-asetuksen mukaisia asioita, mutta sopimukset on päivitettävä tietosuoja-asetuksen mukaisesti. Muun muassa 28. artiklassa määritellään, että sopimuksen tai muun asiakirjan on oltava kirjallinen, mukaan lukien sähköinen asiakirja, ja että rekisterinpitäjän on myös ohjeistettava ulkopuolisia henkilötietojen käsittelijöitä henkilötietojen käsittelyssä. Ohjeistuksella ja sopimuksilla rekisterinpitäjä ohjeistaa henkilötietojen käsittelijän toimimaan vastuullisesti. Avuksi sopimuksiin voi ottaa käyttöön vakiosopimuslausekkeita. Lisäksi tietosuoja-asetuksen vaatimukset on huomioitava tietojärjestelmähankinnoissa.

Lisäksi rekisterinpitäjän on huolehdittava rekisteröidyn oikeuksien turvaamisesta ja informoinnista. Tietosuoja-asetus painottaa läpinäkyvää, helposti ymmärrettävää ja saatavilla olevaa informointia. Informoitavat tiedot tulee olla tiiviisti esitetyssä muodossa. Informoinnissa on käytettävä selkeää ja yksinkertaista kieltä, varsinkin kun informointi tehdään lapsille (12 art.). Rekisterinpitäjän tulee huolehtia, että selosteet käsittelytoimista ovat saatavilla kirjallisesti ja sähköisesti. Seloste on pyydettyessä toimitettava myös valvontaviranomaiselle. Pelkkä selosteen käyttö ei kuitenkaan riitä, vaan rekisterinpitäjän on kehitettävä informointimenettelyä. Välittömästi kehittämistä vaativat myös ohjeistus suostumusten käytöstä sekä luovutukset ja siirrot EU:n ja Euroopan talousalueen ulkopuolelle. Pilvipalveluiden lisääntyessä rekisterinpitäjä voi tahattomasti tulla luovuttaneeksi henkilötietoja EU:n ulkopuolelle.

Uusia asioita tietosuoja-asetuksessa on mahdollisuus yhteisrekisterinpitoon. Nämä menettelytavat rekisterinpitäjän tulee selvittää. Lisäksi rekisterinpitäjän on tietosuoja-asetuksen artiklan 31. mukaan tehtävä yhteistyötä valvontaviranomaisen kanssa.

Kehittämistä tai päivittämistä vaativia asioita organisaatiossa ovat sellaiset, mitkä ovat jo osittain käytössä, mutta edellyttävät tietosuoja-asetuksen vaatimuksien huomioonotamista. Näitä ovat ohjeistus henkilötietojen ja tunnusten käsittelystä. Organisaatioissa oli ohjeistusta saatavilla, mutta ohjeistukset vaativat kehittämistä. Lisäksi päivitystä kaipaavat erityisesti erityisiä henkilötietoryhmiä (henkilötietolaissa arkaluonteiset tiedot) koskevat ohjeistukset. Käyttöoikeudet oli hyvin määritelty, niiden osalta riittää päivitys.

Rekisterinpitäjän tulee tehdä ja päivittää rekisteriselosteet (Tietosuoja-asetuksessa selosteet käsittelytoimista). Tutkimuksen mukaan selosteet oli tehty tyydyttävästi ja rekistereille oli määritelty yhteyshenkilöt, mutta ongelmia oli niiden saatavuudessa. Koska tietosuoja-asetus painottaa riskilähtöisyyttä, niin rekisterinpitäjän tulisi nimittää tietoturvapäällikkö tai vastaava tietoturva-asioista vastaava ja päivitettävä tietoturvaohjeet. Henkilötietojen käsittelyä koskevia asioita käsitellään tietosuoja-asetuksen 5. artiklassa. Yhtenä periaatteena on muun muassa tietojen minimointi. Rekisterinpitäjän tulisi päivittää asiakirjallisen tiedon säilyttämisen periaatteet ja huomioida ne käytännössä. Lopuksi rekisterinpitäjän tulisi kouluttautua ja perehtyä tietosuoja-asetukseen liittyviin ohjeistuksiin.

7 JOHTOPÄÄTÖKSET JA POHDINTA

Tässä luvussa tehdään johtopäätökset tutkimustuloksista. Lisäksi pohditaan tutkimuksen luotettavuutta, tutkimusmenetelmien valintaa, analyysia ja käsitellään eettisiä kysymyksiä. Lopuksi esitetään jatkotutkimusaiheita.

7.1 Johtopäätökset

Tässä pro gradu -työssä tarkoituksena oli vastata kysymykseen siitä, miten rekisterinpitäjiin kohdistuvat vaatimukset muuttuvat tietosuoja-asetuksen myötä. Tutkimuskysymystä lähestyttiin kahdesta näkökulmasta. Ensimmäiseksi arvioitiin henkilötietolain ja tietosuoja-asetuksen eroja rekisterinpitäjiin kohdistuvien vaatimusten näkökulmista. Tähän käytettiin standardiperusteista arviointia. Arviointikriteerinä oli, miten henkilötietolain vaatimukset rekisterinpitäjälle eroavat tietosuoja-asetuksen vaatimuksista. Arvioinnin tuloksena saatiin yhteenveto julkisen sektorin rekisterinpitäjään kohdistuvista vaatimuksista. Toisena näkökulmana oli selvittää rekisterinpitäjien henkilötietolain noudattamisen lähtötilanne. Lähtötilanteesta ja arvioinnin yhteenvedosta muodostettiin kehittämissuosituksen (liite 6).

Vastaavanlaista tutkimusta henkilötietolain noudattamisesta ei ollut aikaisemmin tehty. Tutkimuksen tulos on näin ollen mielenkiintoinen. Suunniteltaessa tietosuoja-asetukseen liittyviä kehittämistoimia, on hyödyllistä tietää, mihin asioihin on kiinnitettävä huomiota. Näitä asioita ovat muun muassa henkilötietojen ohjeistuksen ajantasaisuus, henkilötietojen käsittelijöille, tietosuojavastaavan nimeäminen ja rekisteröidyn informointi ja oikeuksien turvaaminen. Useissa keskusteluissa tietosuojavaltuutetun toimiston edustajien kanssa tuli esiin se, että esimerkiksi henkilötietoon liittyvät käsitteet ovat heikosti tiedossa. Tässä tutkimuksessa ei kysytty käsitteiden ymmärtämisestä, mutta se, että 7 % kaipaa niihin tukea tietosuoja-asetuksen osalta, saattaa osoittaa, että käsitteet eivät kaikilta osin ole hallussa.

Rekisterinpitäjiin kohdistuvat vaatimukset tulevat lisääntymään, osin entiset vaatimukset selkiintyvät, osin täydentyvät ja tietosuoja-asetus tuo myös uusia vaatimuksia. Väli-

töntä kehittämistä vaativat alueet ovat tietosuoja-asetuksen uudet asiat kuten vaatimus sisäänrakennetusta ja oletusarvoisesta tietosuojasta, riskilähtöisyyden huomiointi, tietoturvaloukkausmenettelyt, tietojen pseudonymisointi ja salaus sekä osoitusvelvollisuus. Rekisterinpitäjän on osoitettava, että henkilötietojen käsittelyä koskevia periaatteita noudatetaan. Tietosuoja-asetus painottaa rekisterinpitäjän ohjausvelvollisuutta, läpinäkyvää ja avointa informointia sekä riskien tunnistamista.

Yksittäisinä asioina ja välittöminä kehittämiskohteina nousivat esiin suostumusmenettelyn kehittäminen, tietosuojavastaavan nimitys ja tehtävän määrittely, ohjeistus henkilötietojen käsittelijöille, myös ulkopuolisille, rekisteriselosteiden saatavuus, menettelytavat luovutuksissa EU:n ja Euroopan talousalueen ulkopuolelle sekä yleinen tietosuoja-asetukseen valmistautuminen. Tutkimuksesta kävi ilmi, että rekisteriselosteet oli tehty ja yhteyshenkilöt oli määritelty, mutta rekisteriselosteiden saatavuus asiakkaille ei ollut hoidossa. Jollei asiakas tiedä, minkälaisia rekistereitä on olemassa, niin miten hän voi tarkistaa niistä omat tietonsa. Koska tietosuoja-asetus painottaa informoinnin merkitystä, on organisaatioissa kiinnitettävä enemmän huomioita muun muassa rekisteriselosteiden, tietosuoja-asetuksessa seloste käsittelytoimista, saatavuuteen. Jatkossa rekisterinpitäjien on näytettävä pyydettäessä selosteet käsittelytoimista myös valvontaviranomaiselle. Myös tietojen luovuttamiseen liittyvät asiat ovat myös ilmeinen kehittämiskohde. Pilvipalveluiden lisääntyessä rekisterinpitäjä saattaa tahtomattamaan tulla luovuttaneeksi tietoaan EU:n ulkopuolelle, jos palvelin sijaitsee EU:n ulkopuolella.

Organisaatioissa oli tyydyttävästi tai hyvin huomioitu jonkinasteinen suunnitelmallisuus henkilötietojen käytössä, henkilötietojen käyttötarkoitukset, asiakirjallisen tiedon säilyttämisen periaatteet, rekisteriselosteet ja rekistereiden yhteyshenkilöt. Lisäksi yksittäisiä rekisteröidyn oikeuksia kuten tarkastusoikeuden käyttö, tietojen hankinta, tiedot rekisterinpitäjästä ja tieto siitä mihin rekisteröityjen ryhmään henkilötietoja kerätään, oli hyvin tai tyydyttävästi hoidettu. Asiat vaativat kuitenkin kehittämistä tai vähintäänkin päivittämistä. Kehittämistä tarvitaan myös sopimuksissa, niin että niissä huomioidaan henkilötietojen käsittelyyn liittyvät velvollisuudet. Lisäksi ohjeistusta tarvitaan erityisiä henkilöryhmiä koskevissa käytännöissä.

Kyselystä nousi esiin se, että kyselyyn vastaajien nimekkeitä oli useita ja että, eniten vastauksia antoivat hallinnosta ja asiakirjahallinnosta vastaavat. Tämä saattaa kuvastaa sitä, että henkilötietojen käsittelyn liittyvät vastuut ovat jakautuneet eri toimijoille. Samansuuntaista tulosta antoi myös kysymys siitä, onko henkilötietojen käsittelyä tai tiedonhallintaa yleisesti huomioitu strategiassa tai kehittämistoiminnassa. Neljännestä vastaajista ilmoitti, ettei kyseisiä asioita ole huomioitu tai, että he eivät ainakaan tiedä siitä. Pitäisikö tarkemmin määritellä tai ohjeistaa, kenelle kuuluisi kokonaisvastuu henkilötietojen käsittelystä? Tietosuoja-asetus myös lisää henkilötietojen käsittelyyn liittyvien riskien tunnistamista. Kyselyn vastaajista vain 5 henkilöä ilmoitti asemakseen tietoturvaohjeita tai tietoturva-asetaava. Tämä ei ehkä kuitenkaan yksistään selitä sitä, että riskianalyysyjä oli tehty heikosti, sillä vastaajat olivat kuitenkin tietoisia siitä, että esimerkiksi tietoturvaohjeet oli tehty. Tietosuoja-asetus asettaakin rekisterinpitäjät tilanteeseen, missä henkilötietoihin liittyviin mahdollisiin riskeihin on jatkossa varauduttava ennakkolta.

Huomiota herätti myös se, että 26 % vastaajista ilmoitti, ettei ole aloittanut tietosuoja-asetuksen vaatimia kehittämistoimia ja 5 % ilmoitti, ettei ole tietoinen, onko kehittämistoimia aloitettu. Tulevat isot uudistukset kuten sote-maakuntaudistus vievät voimavaroja ja resursseja kunnilta, maakuntien liitoilta ja kuntayhtymiltä, niin ettei aikaa välttämättä riitä muihin isoihin muutoksiin. Vastaajat myös ilmoittivat, että kokonaisuutena tietosuoja-asetus on heille vielä selkiintymätön ja he odottavat valtiovallan sääntelyä kansalliseen liikkumavaraan ja muuta tietoa. Tietosuoja-asetusta sovelletaan 25.5.2018 lukien ja menossa on vuonna 2016 alkanut siirtymäkausi. Koska tietosuoja-asetus tulee asettamaan uusia velvoitteita entisten lisäksi, on kehittämistoimien aloittamisella kiire. Uutena asiana on muun muassa tietosuojavastaavan nimittäminen. Vain 37 % vastaajista oli nimittänyt tietosuojavastaavan ja vain 21 % oli määritellyt hänen tehtävänsä. Tietosuojavastaavan rooli on toimia neuvonantajana ja tietosuoja-asioiden asiantuntijana. Työ vaatii erityisosaamista, joten olisi tärkeää nimittää tietosuojavastaava, jotta hän ehtii koulututtua.

Kokonaisuutena rekisterinpitäjien nykytilanne perustuen henkilötietolakiin oli tyydyttävällä tasolla. Tietyt asiat olivat hyvin hoidossa, toiset taas kaipaavat nopeaa kehittämistä. Taulukoissa 25, 26 ja 27 on liikennevaloilla kuvattu nykytilannetta sekä myös tieto-

suoja-asetuksesta tulevia vaatimuksia. Tarkoituksena on antaa rekisterinpitäjälle nopea kokonaissilmäys tilanteesta. Tietosuoja-asetus tuo mukanaan myös hallinnollisten sakkojen uhan ja velvollisuuden ilmoittaa tietoturvaloukkauksista 72 tunnin kuluessa tapahtuneesta. Hallinnolliset sakot saattavat olla jopa 10–20 miljoonaa euroa. Positiivista tutkimuksessa oli, että organisaatioilla oli tietoa sekä tietosuoja-asetuksesta että valtiovaraministeriön tekemästä VAHTI-ohjeesta. Lisäksi kouluksiin oli osallistuttu tyydyttävästi. Eniten tukea tietosuoja-asetukseen kaivattiin rekisterinpitäjän velvollisuuksiin, henkilötietojen käsittelyohjeisiin, tietoturvaan ja riskienhallintaan liittyviin asioihin sekä sopimushallintaan. Toiveena oli saada yhteisiä malleja ja konkreettisia käytänteitä.

7.2 Tutkimuksen luotettavuus

Tutkimuksen luotettavuutta voidaan arvioida sekä validiteetin (tutkitaan sitä mitä on luvattu) että reliabiliteetin (tutkimustulosten toistettavuus) mukaisesti. Mainitut arviointitavat eivät kuitenkaan sellaisenaan sovellu laadullisen tutkimuksen luotettavuuden arviointiin. Laadullisista tutkimusta arvioidaan kokonaisuutena, jossa tutkimuksen sisäinen johdonmukaisuus on keskeisellä sijalla. Kokonaisuuteen sisältyvät tutkimuksen kohde ja tarkoitus, tutkijan sitoumukset, aineiston keruu ja analyysi sekä tutkimuksen raportointi (Tuomi & Sarajärvi 2009, 134–141.)

Tässä pro gradu -työssä tutkimusmenetelminä käytettiin arviointia, sisällönanalyysia ja sisällön erittelyä. Eri menetelmien käytöllä pyrittiin löytämään jokaiselle tutkimusalueelle sille soveltuvin menetelmä ja parantamaan tätä kautta luotettavuutta. Eri tutkimusmenetelmien triangulaation tarkoituksena on saada enemmän ymmärrystä tutkittavasta asiasta, laajentaa ja täydentää näkökulmaa (Creswell 1994, 173–178.) Sisällönanalyysi ja arviointitutkimuksen osuus pyrittiin tekemään niin tarkasti ja huolellisesti kuin mahdollista. Eräsaari (1999, 148) toteaa kuitenkin, että arviointi on aina kontekstisidonnaista. Aina voidaan tehdä tai ymmärtää toisin ja tulokset ovat väliaikaisia ja ehdollisia. Haasteena ja luotettavuutta vähentävänä tässä pro gradu -työssä oli se, että tietosuoja-asetusta sovelletaan toukokuusta 2018 lukien. Kansalliset liikkumavarat eivät ole vielä tiedossa, eikä tietosuoja-asetukseen liittyviä käytäntöjä ole syntynyt.

Tutkijan arviointi siitä, mitkä kohdat henkilötietolaissa vastaavat tietosuoja-asetuksen tiettyjä kohtia perustuivat tutkijan näkemyksiin. Arviointia tehtiin kolmen eri näkökulman kautta: mikä osio täydentyy, mikä tuo lisää ja mikä on kokonaan uutta. Kyseisen kolmen kysymyksen käyttö lisäsi tutkimuksen luotettavuutta, koska vastaavaa jaottelu oli käytetty aikaisemmin. Toisaalta tutkimuksen luotettavuutta parantavana tekijän oli tutkijan oma sitoutuneisuus tutkimuskohteeseen oman työn kautta. Tutkijalla oli mahdollisuus keskustella tietosuoja-asetuksen tulkinnoista eri asiantuntijoiden, kuten tietosuojavaltuutetun kanssa ja kasvattaa omaa ymmärrystä ja osaamista työn edistyessä.

Sisällön erittelyä käytettiin kyselytutkimusten tulosten analysoinnissa. Sisällön erittelyllä pyrittiin kuvaamaan sekä määrällisesti prosenttiluvuin että sanallisesti vastausten tuloksia. Ronkaisen ym. (2011, 83–84) mukaan vastausten analysointi edellyttää ilmiön ymmärtämistä ja tulkitsemista. Sisällön erittelyllä kuvataan sisältöä ilmiönä sinänsä tai niitä ulkopuolisia ilmiöitä, joita sisällön ajatellaan ilmaisevan (Pietilä 1973, 52–53). Tarkoituksena oli saada tietää tutkittavien organisaatioiden nykytila suhteessa henkilötietolakiin. Kysymykset jaettiin osioihin ja kunkin kysymyksen otsikon jälkeen oli lyhyesti selostettu mitä kyseinen asia tarkoittaa ja viitattu henkilötietolain kyseiseen kohtaan. Tällä haluttiin varmistaa, että vastaaja tietää, mitä käsitteellä tarkoitetaan tai että vastaaja pystyi tarkastamaan kyseisen henkilötietolain lainkohdan. Luotettavuutta pyrittiin parantamaan sillä, että kyselyyn sai vastata täysin anonyymisti. Vastaajille kerrottiin, että tulokset julkaistaan niin, että yksittäinen organisaatio ei paljastu. Tarkoitus ei ollut syyllistää yksittäisiä organisaatioita siitä, että henkilötietolain vaatimuksia ei mahdollisesti noudateta. Tärkeintä oli saada tietää organisaatioiden mahdollisimman totuudenmukainen lähtötilanne suhteessa tietosuoja-asetukseen.

Sisällön erittely antoi tutkijalle tietyn vapauden ymmärtää tutkittavaa ilmiötä kokonaisvaltaisesti, unohtamatta raportoinnin tärkeyttä. Tuomi & Sarajärven (2009, 141) mukaan tutkimuksen yksityiskohtainen raportointi tukee tulosten luotettavuutta. Luotettavuuden kannalta tämä edellytti raportointia siitä, miten aineisto kerättiin ja analysoitiin. Tämä aiheutti myös haasteen, koska aineistoa oli paljon. Työn kuluessa oli haasteena rajata se mitä raportoi ja mitä jättää pois. Kyselytutkimuksen luotettavuutta lisäsi se, että kokonaisvastausprosentti kyselyssä oli 37 % (kunnat 36 %, kuntayhtymät 36 %, maakuntien liitot 50 %). Vastausprosenttia voi pitää hyvänä ja täten vastausten voidaan

arvioida edustavan kuntien, kuntayhtymien ja maakuntien liittojen nykytilaa koskien henkilötietolain noudattamista.

Työtä ohjasi ja luotettavuutta paransi sosiaali- ja terveydenhuollon paradigman hyödyntäminen. Lähtökohtana oli tiedon hallinta, tässä tapauksessa henkilötiedon hallinta ja sen näkyminen rekisterinpitäjän toimintaprosesseissa ja niiden kehittämisessä. Paradigman hyödyntäminen rajasi sitä, mihin tutkija työssään kiinnitti huomiota ja myös auttoi arviointitulosten ja kyselytutkimuksen tulosten yhdistämisessä. Haasteena oli yhdistää henkilötietolain suppeammat vaatimukset tietosuoja-asetuksen uusiin vaatimuksiin. Kysely tehtiin kuitenkin henkilötietolain pohjalta. Näin ollen kehittämiskohteiksi rekisterinpitäjille tulevat ei ainoastaan tyydyttävällä ja heikolla tasolla olevat asiat, vaan myös uudet asiat tietosuoja-asetuksessa.

7.3 Eettinen pohdinta

Tutkimusprosessin kaikkiin vaiheisiin liittyvät eettiset kysymykset. Eettinen kestävyys tukee myös tutkimuksen luotettavuutta. (Tuomi & Sarajärvi 2009, 127). Arkikielessä etiikka on kysymyksiä hyvästä ja pahasta, oikeasta ja väärästä (Hirsjärvi ym. 1997, 23). Eettisesti hyväksyttävä ja luotettava tutkimusta on sellainen, jossa on noudatettu hyvän tieteellisen käytännön periaatteita ja ohjeita (Tuomi & Sarajärvi 2009, 127–133). Suomessa tutkimuseettinen neuvottelukunta julkaisee hyvän tieteellisen käytännön ohjetta. Ohjeissa kuvataan muun muassa toimintatapoja, tiedonhankintaa, tutkimusta, arviointia, raportointia ja muiden tutkijoiden kunnioittamista. Lisäksi ohjeissa annetaan menettelytavat vilppiepäilyissä. (Tutkimuseettinen neuvottelukunta 2012.)

Ronkaisen ym. (2011, 152–153) mukaan hyvin tehty ja perusteltu tutkimus on hyvän tieteellisen käytännön mukaista. Eettisiä kysymyksiä pohdittaessa on otettava huomioon muun muassa plagiointikiellot, tulosten kriittinen tarkastelu, kattava raportointi, toisten tutkijoiden huomiointi ja jos määrärahoja on käytettävissä, niiden oikea käyttötarkoitus. (Hirsjärvi ym. 1997, 26–27.)

Tässä työssä eettiset kysymykset tulivat esiin erityisesti kyselytutkimuksen tekemisessä. Vastaajille kerrottiin, että kyselytutkimuksen vastauksia käytetään tutkijan pro gradu -

työssä. Vastaukset ovat tutkijan käytössä ja hävitetään työn valmistuttua. Vastaajien yksityisyyttä suojeltiin, sillä kyselytutkimukseen sai vastata anonyymisti. Vastaajan henkilöllisyyttä eikä organisaatiota kysytty. Jos vastaaja tämän ilmoitti, niin tieto jäi vain tutkijalle. Vastaajille kerrottiin, että työ on Itä-Suomen yliopiston lopputyöhön kuuluvaa opinnäytetyö; akateeminen riippumaton työ. Kysely lähetettiin Suomen kuntaliiton nimissä, mutta pro gradu työtä ei tehty Suomen kuntaliiton tilauksesta. Tulokset eivät näin ollen ole Suomen kuntaliiton virallinen kanta. Opinnäytetyön tulokset raportoidaan avoimesti opinnäytetyönä Itä-Suomen yliopiston kirjaston ja Kuntaliiton sivustolla. Vastauksista saatavia kehittämiskohteita hyödynnetään tulevissa koulutuksissa ja kehittämisessä yleensä.

7.3 Jatkotutkimusaiheet

Tehty tutkimus on ajankohtainen, tärkeä ja ensimmäinen, missä on tutkittu henkilötietolain noudattamista. Tietosuoja-asetusta sovelletaan 25.5.2018 lukien, organisaatioilla on enää vuosi aikaa valmistautua tietosuoja-asetuksen asettamiin vaatimuksiin. Tämän tutkimuksen tavoitteena on antaa sekä rekisterinpitäjille että koulutuksen suunnittelijoille apuvälineitä kehittämistyöhön. Tämä tutkimus kuvasi sitä hetkeä, kun Suomessa oli vielä voimassa henkilötietolaki ja tietosuoja-asetuksen soveltamishetki oli tuloillaan. Jatkotutkimuksena voisi selvittää tilannetta, kun tietosuoja-asetus on ollut jonkin aikaa voimassa. Nyt tehdystä tutkimuksesta saisi vertailukohdan siihen.

Lisäksi jatkossa voisi keskittyä tiettyihin tietosuoja-asetuksen kohtiin, esimerkiksi tutkia sitä, miten osoitusvelvollisuus tai ennakoiva riskianalyysi tai sisäänrakennetun tietosuojan vaatimukset näkyvät toiminnassa. Olisi myös mahdollista tutkia miten tietosuoja-asetuksen ensimmäisen artiklan tavoite luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä henkilötietojen vapaa liikkuvuus käytännössä ovat vahvistuneet Euroopan unionin alueella, sillä Euroopan unionin alueella on tietosuoja-asetuksen myötä yksi lainsäädäntö 28 eri maiden lainsäädännön sijasta.

LÄHTEET

Aarnio R. 2015. Tietosuojavaltuutetun lausunto liikenne- ja viestintäministeriön massadataa (big data) koskevasta selvityksestä. 3424/41/2015.

Aarnio R. 2016. Kaikki muuttuu. Blogikirjoitus. Saatavissa: <http://www.tietosuoja.fi/fi/index/blogi/6IUtCELFH/2016/CA7zhows3.html.stx> (Luettu 9.9.2016)

Ahonen P. 1985. Hallinnon arvioinnin lähestymistapoja. Valtiovarainministeriö. Helsinki.

Alasuutari P. 1993. Laadullinen tutkimus. Vastapaino. Tampere.

Alasuutari P. 2011. Laadullinen tutkimus. 2.0. Vastapaino. Tampere.

Berelson B. 1971. Content analysis in communication research. Hafner publishing company. New York.

Buttarelli G. 2015. Tiivistelmä Euroopan tietosuojavaltuutetun lausunnosta Meeting the challenges of big data: A call for transparency, user control, data protection by design and accountability. Saatavissa: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Big%20data/16-02-20_challenges_of_big_data_FL.pdf (Luettu 25.8.2016)

Chelimsky E. 1997. The coming transformations in evaluation. Teoksessa Chelimsky Eleanor & Shadish William R., (toim.) Evaluation for the 21st Century. A Handbook. Thousand Oaks, Sage Publications London, New Delhi. 1–26.

Council of Europe 2014. History of the Reform. Saatavissa: http://www.coe.int/t/dghl/standardsetting/cddh/reformechr/Background_en.asp (Luettu 21.5.2017)

Creswell J. W. 1994. Research Design Qualitative & Quantitative Approaches. Sage Publications Inc. USA.

Eräsaari R. 1999. Menestysuniversumia merkitsemässä. Teoksessa Eräsaari R., Lindqvist T., Mäntysaari M. ja Rajavaara M. (toim.). Arviointi ja asiantuntijuus. Gaudeamus. Tampere. 145–168.

Eskola A. 1968. Sosiologian tutkimusmenetelmä II. WSOY. Helsinki.

European Court of Human Rights 1987. Case of Leander v. Sweden. Judgment. Saatavissa: [http://hudoc.echr.coe.int/eng#{"fulltext":\["\"CASE OF LEANDER v. SWEDEN\""\],"documentcollectionid2":\["GRANDCHAMBER","CHAMBER"\],"itemid":\["001-57519"\]} \(Luettu 21.5.2017\)](http://hudoc.echr.coe.int/eng#{)

European Court of Human Rights 2014. Handbook on European data protection law. Saatavissa: http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf (Luettu 25.8.2016)

Euroopan komissio 2015a. Data Protection. Report. Special Eurobarometer 431. Saatavissa: http://ec.europa.eu/public_opinion/archives/ebs/ebs_431_en.pdf (Luettu 25.8.2016)

Euroopan komissio 2015b. Questions and Answers - Data protection reform. Saatavissa: http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm (Luettu 8.9.2016)

Euroopan komissio 2016. Euroopan komissio. Komission tiedonanto Euroopan parlamentille. Saatavissa: <http://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:52016PC0214> HYPERLINK "<http://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:52016PC0214&>

(Luettu 8.9.2016)

Euroopan unioni 2017. Ihmisoikeudet. Saatavissa: http://eur-lex.europa.eu/summary/glossary/human_rights.html (Luettu 21.5.2017)

Hirsjärvi S., Remes P. ja Sajavaara P. 2007. Tutki ja kirjoita. Tammi. Helsinki.

Hirsjärvi S. & Hurme H. 2001. Tutkimushaastattelu. Teemahaastattelun teoria ja käytäntö. Yliopistopaino. Helsinki.

Kautto T. & Henttonen P. 2017. Availability and findability of FOI and privacy statements on Finnish municipalities' websites. Tidsskriftet Arkiv. 8:1.1–13.

Kivi A-S. 2016. Henkilötietojen suojan ulottuvuudet perusoikeutena Euroopan unionissa: yksityisyyden suojasta itsenäiseksi perusoikeudeksi – ja takaisin? Pro gradu-tutkielma. Helsingin yliopisto. Oikeustieteellinen tiedekunta. Helsinki

Koillinen, M. 2012. Henkilötietojen suoja itsenäisenä perusoikeutena. Oikeus 42:2. 171–193.

Kuhn T. 1962. De vetenskapliga revolutionernas struktur. Originalens titel The Structure of Scientific Revolution. Till svenska av Örjan Björkhem. Lagerblads Tryckeri AB. Karlshamn.

Mladenov M. 2013. Protection of the Right to Privacy in the Practice of the European Court of Human Rights. Proceedings of Novi Sad Faculty of Law. 47 (3). 575.

Marz G. 1999. What's in a Name? Some Reflections on the Sociology of Anonymity. The Information Society. 15. 99-112.

Mäenpää O. 2016. Julkisuusperiaate. Talentum Media Oy. Helsinki.

Niiniluoto I. 1996. Informaatio, tieto ja yhteiskunta. Filosofinen käsiteanalyysi. Edita. Helsinki.

Niiniluoto I. 2003. Totuuden rakastaminen. Tieteenfilosofisia esseitä. Otava. Helsinki.

Oikeusministeriö 2016a. Euroopan unionin tietosuojalainsäädännön uudistaminen. Saatavilla: <http://www.oikeusministerio.fi/fi/index/valmisteilla/lakihankkeet/informaatio-oikeus/euroopanunionintietosuojalainsaadannonuudistaminen.html>
(Luettu 25.8.2016)

Oikeusministeriö 2016b. Henkilötietojen suoja koskevan kansallisen lainsäädännön tarkistaminen. Saatavissa:
http://www.oikeusministerio.fi/fi/index/valmisteilla/lakihankkeet/informaatio-oikeus/henkilotietojensuojakansallisenlainsaadannontarkistaminen_0.html
(Luettu 8.9.2016)

Pietilä V. 1973. Sisällön erittely. Gaudeamus. Helsinki.

Pohjola A. 2003. Tutkijan eettiset sitoumukset. Teoksessa Pohjola, Anneli, (toim.). Eettisesti kestävä sosiaalitutkimus. Lapin Yliopistopaino, Rovaniemi. 53–67.

Pitkänen O., Tiilikka P. ja Warma E. 2013. Henkilötietojen suoja. Talentum Media Oy. Helsinki.

Robson C. 2001. Käytännön arvioinnin perusteet. Opas evaluaation tekijöille ja tilaajille. Tammi. Helsinki.

Ronkainen S., Pehkonen L., Lindblom-Ylänne S. & Paavilainen E. 2011. Tutkimuksen voimasanat. Sanoma Pro Oy. Helsinki.

Saranto K. & Kuusisto-Niemi S. 2012. Tiedonhallinnan koulutusohjelma arvioitavana – kokemuksia kansainvälisestä akkreditoinnista. Finnish journal of eHealth and Welfare. 4(2): 140–144.

Scriven M. 1991. Evaluation Thesaurus. Sage. Newbury Park and New Delhi.

Sinkkonen S. & Kinnunen J. 1994. Arviointi ja seuranta julkisella sektorilla. Kuopion yliopiston julkaisu E. Yhteiskuntatieteet 22. Kuopion yliopisto. Kuopio.

Stakes 2001. Arviointi sosiaalipalveluissa. Katsaus arvioinnin peruskysymyksiin. Fin-Soc Työpapereita 3. Helsinki.

Suurla R. 2001. Helmiä kalastamassa. Avauksia tietämyksen hallintaan. Eduskunnan kanslian julkaisu 1. Edita. Helsinki.

Suomen tutkimuseettinen neuvottelukunta 2012. Hyvä tieteellinen käytäntö ja sen loukkausepäilyjen käsitteleminen Suomessa.
Saatavissa: http://www.tenk.fi/sites/tenk.fi/files/HTK_ohje_2012.pdf
(Luettu 11.9.2016)

Suomisanakirja. Sivistyssanakirja. Saatavissa: <https://www.suomisanakirja.fi/> (Luettu 11.9.2016)

Tavani H. 2007. Philosophical Theories of Privacy: Implications for an adequate online privacy policy. *Metaphilosophy*. 38 (1). 1-22.

Tietosuoja-valtuutetun toimisto 2013. Henkilötietolaki.
Saataavissa: <http://www.tietosuoja.fi/fi/index/lait/Henkilotietolaki.html>
(Luettu 9.9.2016)

Tietosuoja-valtuutetun toimisto 2016. Kysymyksiä ja vastauksia tietosuojauudistuksesta.
Saataavissa:
<http://www.tietosuoja.fi/fi/index/euntietosuojauudistus/kysymyksiajavastauksia.html>
(Luettu 25.8.2016)

Tietosuoja-lautakunta 2010. Henkilötietojen käsittelyä koskeva lupahakemus.
2/932/2009. 01.02.2010.

Tuomi J. ja A. Sarajärvi 2009. Laadullinen tutkimus ja sisällönanalyysi. Tammi. Helsinki.

Valtioneuvosto 2016. Digitalisoidaan julkiset palvelut.
Saataavissa: <http://valtioneuvosto.fi/hallitusohjelman-toteutus/digitalisaatio/karkihanke1>
(Luettu 30.10.2016)

Valtiovarainministeriö 2016. EU-tietosuojan kokonaisuudistus. VAHTI-raportti 1. Saataavissa: https://www.vahtiohje.fi/c/document_library/get_file?uuid=ddb05959-40d1-435f-af23-fd20fc21d63f&groupId=10229
(Luettu 25.8.2016)

Westin A. 1969. Privacy and Freedom. *Administrative Law Review*. 22(1). 101-106
Review by: Osborne M. Reynolds, Jr.

Vilkka H. 2007. Tutki ja mittaa. Määrällisen tutkimuksen perusteet. Tammi. Helsinki.

Virtanen P. 2007. Arviointi, Arviointitiedon luonne, tuottaminen ja hyödyntäminen. Edita Prima Oy. Helsinki.

Wray K. 2011. Kuhn and the Discovery of Paradigms. *Philosophy of the Social Sciences*. 41(3). 380–397.

WP29 2010. Working party on the protection of individuals with regard to the processing of personal data. Rules of procedure. Saataavilla: http://ec.europa.eu/justice/data-protection/article-29/files/rules-art-29_en.pdf (Luettu 19.2.2017)

WP29 2014. The Working Party Opinion 05/2014 on Anonymisation Techniques. Saataavissa: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf
(Luettu 9.9.2016)

Voutilainen T. (toim.), Oikarinen T. & Vartiainen N. 2016. Tiedonhallinnan lainsäädännön kehittämistarpeista. Tutkimusraportti. Valtiovarainministeriön julkaisu – 30/2016. Julkisen hallinnon ICT.

Vuorela T. 1990. Toiminnan arvioinnin tutkimusotteiden kehitys. Valtionhallinnon kehittämiskeskus. Helsinki.

Lainsäädäntö:

- L831/1994. Arkistolaki.
 A1030/1999. Asetus viranomaisen toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta.
 63/1999. Euroopan ihmisoikeussopimus. (Yleissopimus ihmisoikeuksien ja perusvapauksien suojaamiseksi) sellaisena kuin se on muutettuna yhdennellätoista pöytäkirjalla.
 95/46/EY. Euroopan parlamentin ja neuvoston direktiivi 95/46/EY annettu 24 päivänä lokakuuta 1995, yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta.
 2016/679. Euroopan parlamentin ja neuvoston yleinen tietosuoja-asetus (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus)
 2012/C326/02. Euroopan unionin perusoikeusasiakirja
 HE96/1998. Hallituksen esitys Eduskunnalle henkilötietolaiksi ja eräksi siihen liittyviksi laeiksi.
 L471/1987. Henkilörekisterilaki.
 L523/1999 Henkilötietolaki, HeTiL.
 L634/2011. Laki julkisen hallinnon tietohallinnon ohjauksesta.
 L159/2007. Laki sosiaali- ja terveydenhuollon sähköisestä käsittelystä.
 L13/2003. Laki sähköisestä asioinnista viranomaistoiminnassa.
 L61/2007. Laki sähköisestä lääkemääräyksestä.
 L621/1999. Laki viranomaisen toiminnan julkisuudesta
 L759/2004. Laki yksityisyyden suojasta työelämässä.
 L731/1999. Suomen perustuslaki.
 PeVL12/2002vp Perustuslakivaliokunnan lausunto - HE 216/2001 vp Hallituksen esitys laiksi ulosottolain muuttamisesta ja eräksi siihen liittyviksi laeiksi
 PeVL14/2002vp Perustuslakivaliokunnan lausunto - HE 9/2002 vp Hallituksen esitys Kansaneläkelaitoksen toimeenpanemiin etuuksiin liittyviin tietojen saamista ja luovuttamista koskevien säännösten muuttamiseksi.

Julkaisemattomat lähteet:

Hoppu-Mäenpää L. 2016. Tietosuoja-asetuksen vaatimukset sopimushallintaan. Julkaisematon power point esitys FCG:n koulutuksessa 21.9.2016 ICT-hankinnat.

Nurmi P. 2016. EU:n yleinen tietosuoja-asetus ja sen vaikutus Suomelle. Julkaisematon power point esitys 27.10.2019. Pohjoismaiden hallinnollisen liiton Suomen osasto ry:n kokouksessa (NAF).

Sulin I. 2016. Tietosuoja-asetuksen vaatimukset. Julkaisematon power point esitys FCG:n koulutuksessa 21.9.2016 ICT-hankinnat.

LIITTEET

LIITE 1. Yksityisyyden käsite Tavani (2007) teorioita mukaillen

Teoria	Ei-häiritä (Nonintrusion)	Eristäytyminen (Seclusion)	Kontrolli (Control)	Rajoittava (Limitation)
Yksityisyyden käsite	Jätetään rauhaan Vapaus toisten sekaantumiselta omiin asioihin	Henkilön annetaan olla yksin ”Mitä enemmän olet yksin, sitä enemmän yksityisyyttä = täydellinen yksityisyys”	Henkilö pystyy kontrolloimaan omia tietojaan	Henkilöllä on yksityisyyttä, kun henkilöstä oleva tieto on rajoitettua tai kiellettyä tietyissä konteksteissa
Tutkijoita mm.	Warren (1890), Brandeis (1890), Brennan (1972)	Gavison (1980), Westin (1967), Brandeis (1890), Warren (1890)	Fried (1990), Miller (1971), Westin (1967), Rachels (1975), Beardsley(1971)	Gavison (1980), Parent (1983), Allen (1988)
Ongelmia	Yksityisyyden käsite sekoittuu vapauden käsitteeseen ja myös yksityisyys ja oikeus yksityisyyteen sekoittuvat	Yksin autiolla saarella oleva yksityisyys on täydellistä, mutta nauttiiko henkilö siitä.	Ei ota huomioon minkälaiseen tietoon on kontrolli ja kuinka paljon henkilö voi kontrolloida omia tietojaan. Jos paljastaa kaikki tietonsa, voiko edelleen nauttia yksityisyydestä? Sekoittaa yksityisyyden ja autonomian.	Henkilöllä on täydellinen yksityisyys, jos kaikki tieto hänestä on salattu Teoria ei huomioi sitä, että henkilöllä voi olla yksityisyys ja siltä hän voi antaa luvan omiin tietoihinsa. Sekoittaa yksityisyyden käsitteen salassapitoon.
Korostaa	Korostaa fyysistä saavutettavuutta.	Korostaa fyysistä saavutettavuutta.	Erottaa vapauden käsitteen ja yksinäisyyden käsitteen yksityisyydestä, Korostaa valinnan vapautta.	Rajoittaa tai kieltää pääsyn muilta omiin tietoihin. Ei sekoita yksityisyyteen yksinäisyyttä, autonomiaa eikä vapautta.

LIITE 2. Henkilötietolain ja tietosuoja-asetuksen arviointitaulukko

Vertailu Henkilötietolaki ja EU-tietosuoja-asetus			
	Henkilötietolaki 523/1999	EU-tietosuoja-asetus, 679/2016	Selkeyttää/täydentää/uutta
Otsikot	Voimassa 1.6.1999–24.5.2018	Voimassa 25.5.2018 lukien	
Kohde ja tavoitteet	§1 Lain tarkoitus Toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia ja edistää hyvän tietojenkäsittelytavan kehittämistä ja noudattamista.	1 art. Kohde ja tavoitteet Luonnollisen henkilön suojeleminen henkilötietojen käsittelyssä, säännöt henkilötietojen vapaaseen liikkuvuuteen. Luonnollisten henkilöiden perusoikeuksien ja -vapauksien suojeleminen sekä oikeutta henkilötietojen suojaamiseen. Henkilötietojen vapaata liikkuvuutta unionin sisällä ei saa rajoittaa eikä kieltää syistä, jotka liittyvät luonnollisten henkilöiden suojelemaan henkilötietojen käsittelyssä.	Tietosuoja-asetus selkeyttää (vapaa liikkuvuus unionin sisällä). Henkilötietolain esivalmistelussa HE 96/1998 mainitaan myös vapaasta liikkuvuudesta unionin sisällä.
Soveltaminen, Aineellinen ja alueellinen soveltamisala	§2 Soveltamisala § 4 Suomen lain soveltaminen Henkilötietojen automaattiseen käsittelyyn ja kun henkilötiedot muodostavat tai niiden on tarkoitus muodostaa henkilöresteri tai sen osa. Soveltamisalue: henkilötietojen käsittelyyn, jossa rekisterinpitäjän toimipaikka on Suomessa tai rekisterinpitäjä käyttää henkilötietojen käsittelyssä Suomessa sijaitsevia laitteita.	2 art. Aineellinen soveltamisala ja Alueellinen soveltamisala 3 art. Henkilötietojen osittaisen tai kokonaan automaattiseen käsittelyyn sekä henkilötietojen käsittelyyn, jotka muodostavat rekisterin osan tai joiden tarkoitus on muodostaa rekisterin osa. Soveltamisala: jos rekisterinpitäjän tai henkilötietojen käsittelijän toimipaikka on unionin alueella tai jos henkilötietojen käsittely tapahtuu unionin alueella.	Tietosuoja-asetus selkeyttää , asetus koskee kaikkia jäsenvaltioita sekä unionin alueella tapahtuvaa henkilötietojen käsittelyä
Soveltamisalueen ulkopuolella	§2 Soveltamisala ulkopuolella Luonnollisen henkilön suorittama henkilötietojen käsittely	2 art. Aineellinen soveltamisalan ulkopuolella Luonnollisen henkilön suorittama henkilötietojen käsittely, henkilötietojen käsittely mikä ei liity unionin lainsäädäntöön, eikä ulko- ja turvallisuuspolitiikkaan eikä rikoksiin eikä unionin toimielinten suorittamaan henkilötietojen käsittelyyn.	Tietosuoja-asetus selkeyttää (rajaus: ei sovelleta lainsäädäntöön, joka ei kuulu unionin soveltamisalaan, ulko- ja turvallisuuspolitiikkaan, rikokset ja unionin toimielimet)
Määritelmät	§ 3 Määritelmät Henkilötieto, henkilötietojen käsittely, henkilöresteri, rekisterinpitäjä, rekisteröity, sivullinen, suostumus	4 art. Määritelmät Henkilötieto, käsittely, käsittelyn rajoittaminen, profilointi, pseudonymisointi, rekisteri, rekisterinpitäjä, henkilötietojen käsittelijä, vastaanottaja, kolmas osapuoli, suostumus, tietoturvaloukkaus, geneettiset tiedot, biometriset tiedot, terveystiedot, päätoimipaikka, edustaja, yritys, konserni, yritystä koskevat sitovat säännöt, valvontaviranomainen, osallistuva valvontaviranomainen, rajat ylittävä käsittely, merkityksellinen ja perusteltu vastalause, tietoyhteiskunnan palvelut, kansainvälinen järjestö	Tietosuoja-asetus täydentää (uusia määritelmiä, mitkä kuvaavat mm. uuden tekniikan tuomia mahdollisuuksia)

<p>Yleiset periaatteet</p>	<p>§ 5 Huolellisuusvelvoite § 6 Henkilötietojen käsittelyn suunnittelu, § 7 Käyttötarkoitussidonnaisuus Huolellisuusvelvoite (laillisuus, huolellisuus, hyvä tietojenkäsittelytapa, ei rajoiteta yksityisyyden suojan perusoikeuksia). Sitoo myös niitä, jotka toimivat rekisterinpitäjän lukuun. Suunnitteluelvoite (asiallinen perustelu, käsittelyn tarkoitus, säännönmukainen hankinta ja luovutus, määriteltävä ennen henkilötietojen keräämistä ja muodostamista henkilörekisteriksi) Käyttötarkoitussidonnaisuus (henkilötietoja saa käyttää vain suunnitellun käyttötarkoituksen mukaisesti. Tietoja saa käyttää historiallisen tutkimuksen, tieteellistä tai tilastotarkoitusta varten.</p>	<p>5 art. Henkilötietojen käsittelyä koskevat periaatteet Lainmukaisuus, kohtuullisuus, läpinäkyvyys, käyttötarkoitussidonnaisuus (tietty, nimenomainen ja laillinen tarkoitus), tietojen minimointi (asianmukaisuus, olennaisuus, rajoitettu), täsmällisyys (täsmällisiä, päivitettyjä), säilytyksen rajoittaminen, eheys ja luottamuksellisuus. Rekisterinpitäjällä on osoitusvelvollisuus siitä, että henkilötietojen käsittelyä koskevia periaatteita noudatetaan.</p>	<p>Tietosuoja-asetus täydentää (läpinäkyvyys, osoitusvelvollisuus)</p>
<p>Tietojen laatua koskevat periaatteet</p>	<p>§9 Tietojen laatua koskevat periaatteet Tarpeellisuusvaatimus, virheettömyysvaatimus</p>	<p>5 art. Henkilötietojen käsittelyä koskevat periaatteet Lainmukaisuus, kohtuullisuus, läpinäkyvyys, käyttötarkoitussidonnaisuus (tietty, nimenomainen ja laillinen tarkoitus), tietojen minimointi (asianmukaisuus, olennaisuus, rajoitettu), täsmällisyys (täsmällisiä, päivitettyjä), säilytyksen rajoittaminen, eheys ja luottamuksellisuus. Rekisterinpitäjällä on osoitusvelvollisuus siitä, että henkilötietojen käsittelyä koskevia periaatteita noudatetaan.</p>	<p>Tietosuoja-asetus täydentää (uusia määritelmiä, mitkä kuvaavat uuden tekniikan tuomia mahdollisuuksia)</p>

<p>Rekisteriseloste , Seloste käsittelytoimista</p>	<p>§ 10 Rekisteriseloste Rekisterinpitäjän on laadittava henkilörekisteristä rekisteriseloste. Sisältö: Rekisterinpitäjän ja tarvittaessa edustajan nimi ja yhteystiedot, henkilötietojen käsittelyn tarkoitus, kuvaus rekisteröityjen ryhmästä tai ryhmistä ja näihin liittyvistä tiedoista tai tietoryhmistä, tietojen säännönmukainen luovutus ja luovutetaan ko tietoja EU ulkopuolelle, kuvaus rekisterin suojauksen periaatteista.</p>	<p>30 art. Seloste käsittelytoimista Jokaisen rekisterinpitäjän ja tarvittaessa rekisterinpitäjän edustajan on ylläpidettävä selostetta käsittelytoimista. Sisältö: Rekisterinpitäjän ja mahdollisen yhteisrekisterinpitäjän, rekisterinpitäjän edustajan ja tietosuojavastaavan nimi ja yhteystiedot, käsittelyn tarkoitus, kuvaus rekisteröityjen ryhmistä ja henkilötietoryhmistä, tietojen luovutuksen vastaanottajien ryhmät, henkilötietojen siirtämisestä kolmanteen maahan tai kansainväliselle järjestölle, tietoryhmien poistamisen suunnitellut määräajat, tekniset ja organisatoriset turvatoimet. Lisäksi kunkin henkilötietojen käsittelijän ja tarvittaessa henkilötietojen käsittelijän edustajan on ylläpidettävä selostetta kaikista rekisterinpitäjän lukuun suoritettavista käsittelytoimista niin että seloste käsittää seuraavat tiedot henkilötietojen käsittelijän tai käsittelijöiden ja kunkin rekisterinpitäjän, jonka lukuun henkilötietojen käsittelijä toimii, sekä rekisterinpitäjän tai tarvittaessa henkilötietojen käsittelijän edustajan ja tietosuojavastaavan nimi ja yhteystiedot, kunkin rekisterinpitäjän lukuun suoritettujen käsittelyiden ryhmät; tarvittaessa tiedot henkilötietojen siirtämisestä kolmanteen maahan tai kansainväliselle järjestölle, mukaan lukien tieto siitä, mikä kolmas maa tai kansainvälinen järjestö on kyseessä, sekä asianmukaisia suojatoimia koskevat asiakirjat, jos kyseessä on 49 artiklan 1 kohdan toisessa alakohdassa tarkoitettu siirto, mahdollisuuksien mukaan yleinen kuvaus 32 artiklan 1 kohdassa tarkoitettua teknisistä ja organisatorisisturvatiedoista.</p>	<p>Tietosuoja-asetus täydentää (selosteessa mm. yhteisrekisterinpitäjä, tietosuojavastaava, määräaika tietojen poistamiselle, selostettava tekniset ja organisatoriset turvatoimet) 30 art. Tietosuoja-asetuksen velvollisuudet koskien selostetta eivät koske yritystä tai järjestöä, jossa on alle 250 työntekijää, paitsi jos sen suorittama käsittely todennäköisesti aiheuttaa riskin rekisteröidyn oikeuksille ja vapauksille, käsittely ei ole satunnaista tai käsittely kohdistuu 9 artiklan 1 kohdassa tarkoitettuihin erityisiin tietoryhmiin tai 10 artiklassa tarkoitettuihin rikostuomioita tai rikkomuksia koskeviin henkilötietoihin. Tietosuoja-asetuksen velvollisuudet koskien selostetta eivät koske yritystä tai järjestöä, jossa on alle 250 työntekijää, paitsi jos sen suorittama käsittely todennäköisesti aiheuttaa riskin rekisteröidyn oikeuksille ja vapauksille, käsittely ei ole satunnaista tai käsittely kohdistuu 9 artiklan 1 kohdassa tarkoitettuihin erityisiin tietoryhmiin tai 10 artiklassa tarkoitettuihin rikostuomioita tai rikkomuksia koskeviin henkilötietoihin. Tietosuoja-asetus täydentää (henkilötietojen käsittelijän tai käsittelijän edustajan on ylläpidettävä selostetta rekisterinpitäjän lukuun suoritettavista käsittelytoimista).</p>
<p>Tiedotus rekisteriselosteesta</p>	<p>§ 10 Rekisteriseloste Rekisteriseloste on pidettävä jokaisen saatavilla. Poikkeukset (valtion turvallisuus, puolustus, yleinen järjestys, turvallisuus, rikosten ehkäiseminen tai selvittäminen, verotus tai julkinen talous)</p>	<p>30 art. Seloste käsittelytoimista Kirjallinen mukaan lukien sähköisessä muodossa ja myös valvontaviranomaisen saatavilla</p>	<p>Tietosuoja-asetus täydentää (myös sähköisessä muodossa)</p>

<p>Arkaluonteiset tiedot, Erityiset henkilötietoryhmät</p>	<p>§ 11 Arkaluonteisten tietojen käsittelytieto Arkaluonteisten henkilötietojen käsittelykielto. Näitä ovat: rotu, etninen alkuperä, yhteiskunnallinen, poliittinen, uskonnollinen vakaumus tai ammattiliittoon kuuluminen, rikollinen teko, rangaistus tai muu rikoksen seuraamus, henkilön terveydentila, sairaus, vammaisuus, hoitotoimenpiteet, seksuaalinen suuntautuminen tai käyttäytyminen, sosiaalihuollon tarve tai sosiaalihuollon palvelu, tukitoimi tai etuus.</p>	<p>9 art. Erityisiä henkilötietoryhmiä koskeva käsittely Erityisiä henkilötietoryhmien koskevien henkilötietojen käsittelykielto: Näitä ovat: rotu tai etninen alkuperä, poliittinen mielipide, uskonnollinen tai filosofinen vakaumus tai ammattiliiton jäsenyys sekä geneettisten tai biometrinen tietojen käsittely henkilön yksiselitteistä tunnistamista varten tai terveyttä koskevien tietojen taikka luonnollisen henkilön seksuaalista käyttäytymistä ja suuntautumista koskevat tiedot. HUOM! PUUTTUU SOSIAALIHUOLTO</p>	<p>Tietosuoja-asetus täydentää (geneettiset ja biometriset tiedot) Sosiaalihuolto puuttuu.</p>
<p>Poikkeukset arkaluonteisten tietojen käsittelykiellosta</p>	<p>ammattiliittoon kuulumista koskevien tietojen käsittelyä ammattiyhdistysten ja niiden muodostaman liiton toiminnassa, jos tiedot koskevat näiden järjestöjen jäseniä taikka henkilöitä, joilla on järjestöihin säännölliset, järjestöjen tarkoituksiin liittyvät yhteydet, eikä tietoja luovuteta sivullisille ilman rekisteröidyn suostumusta, ammattiliittoon kuuluminen mikäli tarpeen rekisterinpitäjän oikeuksien ja velvoitteiden noudattamiseksi, terveydenhuollon toimintayksikköä tai terveydenhuollon ammattihenkilöä käsittelemästä näiden tässä toiminnassa saamia tietoja rekisteröidyn terveydentilasta, sairaudesta tai vammaisuudesta tai häneen kohdistetuista hoitotoimenpiteistä taikka muita rekisteröidyn hoidon kannalta välttämättömiä tietoja; vakuutuslaitos niiden käsitellessä vakuutustoiminnassa saatuja tietoja, sosiaalihuollon viranomaista tai muuta sosiaalihuollon etuuksia myöntävää viranomais- ta, laitosta tai yksityisten sosiaalipalvelujen tuottajaa käsittelemästä kyseisen viranomaisen, laitoksen tai palvelujen tuottajan toiminnassa saamia tietoja rekisteröidyn sosiaalihuollon tarpeesta tai hänen saamistaan sosiaalihuollon palveluista, tukitoimista tai hänelle myönnettyistä muista sosiaalihuollon etuuksista taikka muita rekisteröidyn huollon kannalta välttämättömiä tietoja; ja tietosuojalautakunnan luvalla. Arkaluonteiset tiedot on poistettava rekisteristä välittömästi sen jälkeen, kun käsittelylle ei ole perustetta. Peruste arviointia 5 v. välein.</p>	<p>9 art. Käsittelykielto ei koske mikäli: Nimenomainen suostumus, velvoitteet tai erityiset oikeudet (työoikeus, sosiaaliturva, sosiaalinen suojelu, säännelty lainsäädännössä tai lainsäädännön mukaisessa työehtosopimuksessa), elintärkeä etu (rekisteröity ei pysty fyysisesti tai juridisesti estynyt antamaan suostumuksen), poliittisen, filosofisen, uskonnollisen tai ammattiliitto-toimintaan liittyvän säätiön, yhdistyksen ja muun jäsenyys, rekisteröity saattanut julkiseksi, oikeusvaate, yleinen etu, ennalta ehkäisy, kansanterveys, sosiaalihuolto (edellyttää lakisääteistä salassapitovelvollisuutta), arkistointi, tieteellinen ja historiallinen tutkimustarkoitus.</p>	<p>Tietosuoja-asetus täydentää Tietosuoja-asetuksessa sosiaalihuolto tulee mainituksi tässä. Nykyinen henkilötietolaki on joltain osin tarkempi ja sisältää mm. määräyksen poistaa arkaluonteiset tiedot, kun niiden käyttämiselle ei ole perustetta.</p>

<p>Suostumus 7 art.</p>	<p>§ 3 Määritelmät Suostumus: yksiselitteinen ja nimenomainen Suostumus: kaikenlaista vapaaehtoista, yksilöityä ja tietoista tahdon ilmaisua, jolla rekisteröity hyväksyy henkilötietojensa käsittelyn</p>	<p>4 art. Määritelmät, 7 art. Suostumuksen edellytykset Suostumus: mitä tahansa vapaaehtoista, yksilöityä, tietoista ja yksiselitteistä tahdonilmaisua, jollarekisteröity hyväksyy henkilötietojensa käsittelyn antamalla suostumusta ilmaisevan lausuman tai toteuttamalla selkeästi suostumusta ilmaisevan toimen. Rekisterinpitäjällä osoitusvelvollisuus suostumuksen olemassaolosta, suostumuksen antamista koskeva pyyntö on esitettävä selvästi erillään muista asioista helposti ymmärrettävässä ja saatavilla olevassa muodossa selkeällä ja yksinkertaisella kielellä, oikeus peruuttaa suostumus, rekisterinpitäjän ilmoitettava oikeudesta peruuttaa suostumus, rekisterinpitäjän arvioitava kattavasti ovatko täytäntöönpanon ehdoksi asetettu suostumus sellaisiin henkilötietoihin, jotka eivät ole tarpeen.</p>	<p>Tietosuoja-asetus täydentää (suostumus muoto on kuvattu tarkemmin, rekisterinpitäjällä osoitusvelvollisuus suostumuksen olemassaolosta. Huom.! Suomessa Laki sähköisestä lääkemääräyksestä 2.2.2007/61 § 14 Suostumus- ja kieltoasiakirjat, Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä 9.2.2007/159 §12 Suostumus- ja kieltoasiakirja Määrittelevät suostumuksen ja mahdollisuuden peruuttaa suostumus henkilötietolakia tarkemmin. Tietosuoja-asetus täydentää (suostumus muoto on kuvattu tarkemmin, rekisterinpitäjällä osoitusvelvollisuus suostumuksen olemassaolosta.</p>
<p>Henkilötunnuksen käsittely</p>	<p>§ 13 Henkilötunnuksen käsittely Henkilötunnusta saa käsitellä rekisteröidyn yksiselitteisellä suostumuksella tai jos säädetään laissa. Lisäksi jos yksilöiminen on tärkeää (lakisääteinen tehtävä, rekisteröidyn tai rekisterinpitäjän oikeuksien tai velvollisuuksien toteuttamiseksi, historiallinen tai tieteellinen tutkimus). Henkilötunnusta saa käsitellä mm. vakuutus-, luottolaitos-, maksupalvelu-, vuokraus-, ja lainaustoiminta, luottotietotoiminta, terveydenhuollossa, sosiaalihuollossa, virka- työ- ja muita palvelussuhteita ja niihin liittyviä etuja koskevilla asioissa.</p>	<p>87 art. Kansallisen henkilötunnuksen käsitteleminen Jäsenvaltiot voivat määritellä tarkemmin erityiset kansallisen henkilönumeron tai muun yleisen tunnisteen käsittelyn edellytykset. Rekisteröidyn oikeuksia ja vapauksia on noudatettava sekä huolehdittava asianmukaisista suojaustoimista.</p>	<p>Tietosuoja-asetuksella annetaan kansallinen liikkumavara.</p>
<p>Henkilötietojen käsittely ja virallisten asiakirjojen julkisuus</p>	<p>§8 Käsittelyn yleiset edellytykset Oikeudesta saada tieto ja muusta henkilötietojen luovuttamisesta viranomaisen henkilörekisteristä on voimassa, mitä viranomaisten asiakirjojen julkisuudesta säädetään.</p>	<p>86 art. Henkilötietojen käsittely ja virallisten asiakirjojen julkisuus Viranomaiset taikka julkis- ja yksityisoikeudelliset yhteisöt voivat luovuttaa viranomaisten tai yhteisön hallussa olevien virallisten asiakirjojen sisältämiä henkilötietoja yleisen edun vuoksi toteutetun tehtävän suorittamiseksi viranomaiseen tai yhteisöön sovellettavan unionin oikeuden tai jäsenvaltion lainsäädännön mukaisesti. On huomioitava virallisten asiakirjojen julkisuus ja oikeus henkilötietojen suojaan.</p>	<p>Tietosuoja-asetuksella annetaan kansallinen liikkumavara. Suomessa laki viranomaisen toiminnan julkisuudesta 621/1999 sekä asetus viranomaisen toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta 1030/1999 määrittelevät viranomaisten asiakirjojen julkisuudesta.</p>

<p>Käsittely työsuhteen yhteydessä</p>	<p>§ 8 Käsittelyn yleiset edellytykset Henkilötietoja saa käsitellä jos rekisteröidyllä on asiakas- tai palvelussuhteen, jäsenyyden tai muun niihin verrattavan suhteen vuoksi asiallinen yhteys rekisterinpitäjän toimintaan tai jos kysymys on konsernin tai muun taloudellisen yhteenliittymän asiakkaita tai työntekijöitä koskevista tiedoista ja niitä tietoja käsitellään kyseisen yhteenliittymän sisällä</p>	<p>9 art. Erityisiä henkilötietoryhmiä koskeva käsittely ja 88 art. Käsittely työsuhteen yhteydessä Henkilötietoja saa käsitellä mikäli käsittely on tarpeen rekisterinpitäjän tai rekisteröidyn velvoitteiden ja erityisten oikeuksien noudattamiseksi työoikeuden tai jäsenvaltion lainsäädännön mukaisessa työehtosopimuksessa. Jäsenvaltiot voivat antaa lakisääteisesti tai työehtosopimuksella yksityiskohtaisempia sääntöjä työntekijöiden henkilötietojen käsittelystä. Säännökset on annettava komissiolle viimeistään 25.5.2018.</p>	<p>Tietosuoja-asetuksella annetaan kansallinen liikkumavara. Huom.! Laki yksityisyyden suojasta työelämässä 759/2004. Lain tarkoituksena on toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia työelämässä. Jäsenvaltiot voivat pitää voimassa tai ottaa käyttöön lisäehtoja, mukaan lukien rajoituksia, jotka koskevat geneettisten tietojen, biometristen tietojen tai terveystietojen käsittelyä (9 art.).</p>
<p>Lapsen suostumus</p>		<p>8 art. Tietoyhteiskunnan palveluihin liittyvään lapsen suostumukseen sovellettavat ehdot Tietoyhteiskunnan palveluihin alle 16 v vaaditaan suostumus vanhempainvastuunkantajalta. Vähintään 16 v voi antaa suostumuksen itse. Huom.! Jäsenvaltiot voit säätää alemman iän min. 13 v.</p>	<p>Tietosuoja-asetus tuo uutta. Huom.! Jäsenvaltiot voit säätää alemman iän min. 13 v. Huom.! Laki sähköisestä lääkemääräyksestä 61/2007/13 §, "Alaikäisen oikeus määrätä tietojensa luovutuksesta ikä ja kehitystason perusteella" Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä 159/2007 § 19 Laki potilaan asemasta ja oikeuksista 785/1992 7§ Alaikäisen potilaan asema. Huom. Sovelletaan tietoyhteiskunnan palveluihin, millä tarkoitetaan kaikkia tietoyhteiskunnan palveluja, toisin sanoen kaikkia etäpalveluina sähköisessä muodossa palvelun vastaanottajan henkilökohtaisesta pyynnöstä toimitettavia palveluja, joista tavallisesti maksetaan korvaus (EU-direktiivi 1535/2015 1 art.)</p>

<p>Käsittelyn yleiset edellytykset, Käsittelyn lainmukaisuus</p>	<p>§8 Käsittelyn yleiset edellytykset Henkilötietoja saa käsitellä, jos: rekisteröity on antanut yksiselitteisen suostumuksen, toimeksianto tai sopimus, elintärkeä etu, lakisääteinen tehtävä tai velvoite, asiakas- tai palvelussuhde, jäsenyys tai asiallinen yhteys, konsernin tai muun taloudellisen yhteenliittymän asiakkaat tai työntekijät, maksupalvelu tai tietojenkäsittely toimeksiannon perusteella, jos kysymys on henkilön asemaa, tehtäviä ja niiden hoitoa julkisyhteisössä tai elinkeinoelämässä kuvaavista yleisesti saatavilla olevista tiedosta, tietosuojalautakunnan lupa.</p>	<p>6 art. Käsittelyn lainmukaisuus Käsittely on lainmukaista, jos vähintään yksi täyttyy: rekisteröity on antanut suostumuksen, sopimuksen täytäntöönpano, rekisterinpitäjän lakisääteinen velvoite, elintärkeä etu, yleinen etu, julkinen valta (huom. jäsenvaltiot voivat pitää yksityiskohteisempaa säännöksiä) sekä käsittely on tarpeen rekisterinpitäjän tai kolmannen osapuolen oikeutettujen etujen toteuttamiseksi (ei koske viranomaisia)</p>	<p>Tietosuoja-asetus selkeyttää.</p>
<p>Henkilötietojen käsittely erityisiä tarkoituksia varten</p>	<p>§16 Viranomaisen suunnittelu- ja selvitystehtävät, §17 Henkilömatrikkeli, §18 Sukututkimus, §19 Suoramarkkinointi ja muut osoitteelliset lähetykset Henkilötietolaissa on erikseen määritelty, miten henkilötietoja tulee käsitellä ko. tapauksissa.</p>	<p>21 art. Vastustamisoikeus. Jos henkilötietoja käsitellään suoramarkkinointia varten, rekisteröidyllä on oikeus, milloin tahansa vastustaa häntä koskevien henkilötietojen käsittelyä tällaista markkinointia varten, mukaan lukien profilointia silloin kun se liittyy tällaiseen suoramarkkinointiin. Jos henkilötietoja käsitellään tieteellisiä tai historiallisia tutkimustarkoituksia tai tilastollisia tarkoituksia varten 89 artiklan 1 kohdan mukaisesti, rekisteröidyllä on oikeus henkilökohtaiseen tilanteeseensa liittyvällä perusteella vastustaa häntä itseään koskevien henkilötietojen käsittelyä, paitsi jos käsittely on tarpeen yleistä etua koskevan tehtävän suorittamiseksi.</p>	<p>Tietosuoja-asetus selkeyttää ja osittain tuo uutta Suoramarkkinointi, tutkimus. Tietosuoja-asetuksessa ei mainita henkilömatrikkeliä eikä sukututkimuksia eikä viranomaisen suunnittelu ja selvitystehtäviä.</p>
<p>Henkilötietojen käsittely erityisiä tarkoituksia varten Henkilötietojen siirto arkistoon</p>	<p>§14 Tutkimus, §15 Tilasto 35 § Henkilötietojen siirto arkistoon Henkilötietojen käytöstä ja suojaamisesta sekä niissä olevien tietojen luovuttamisesta arkistolaitokseen tai siihen verrattavaa arkistoon on voimassa, mitä erikseen säädetään.</p>	<p>89 art. Yleisen edun mukaisia arkistointitarkoituksia taikka tieteellisiä tai historiallisia tutkimustarkoituksia tai tilastollisia tarkoituksia varten tapahtuvaa käsittelyä koskevat suojatoimet ja poikkeukset Käsittelyyn on sovellettava rekisteröidyn oikeuksia ja vapauksia koskevia asianmukaisia suojatoimia. Suojatoimilla on varmistettava, että on toteutettu tekniset ja organisatoriset toimenpiteet, joilla taataan etenkin tietojen minimoinnin periaatteen noudattaminen esim. pseudonymisoinnilla. Jäsenvaltioissa tai unionin oikeudessa voidaan säätää poikkeuksia artikloihin 15, 16, 18, 19, 20 ja 21 tietyissä tapauksissa, jotta voidaan käsitellä tietoja otsikoiden tarkoituksiin.</p>	<p>Tietosuoja-asetus täydentää, painottaa teknisiä ja organisatorisia toimenpiteitä. Tässä osiossa myös tutkimustarkoitus ja tilastollinen tarkoitus.</p>

<p>Käsittely joka ei edellytä tunnistamista</p>		<p>11 art. Käsittely, joka ei edellytä tunnistamista Jos henkilötietojen käsittelyn tarkoitus ei edellytä rekisteröidyn tunnistamista, ei rekisterinpitäjällä ole velvollisuutta säilyttää, hankkia tai käsitellä lisätietoja rekisteröidyn tunnistamista varten. Rekisterinpitäjän on ilmoitettava rekisteröidylle, mikäli rekisterinpitäjä ei pysty tunnistamaan rekisteröityä.</p>	<p>Tietosuoja-asetus tuo uutta. Rekisterinpitäjällä velvollisuus tunnistaa rekisteröity.</p>
<p>Henkilötietojen siirto Euroopan unionin puolelle</p>	<p>§ 22 Yleiset edellytykset § 22 a Komission päätökset § 23 Poikkeusperusteet Henkilötietoja voidaan siirtää Euroopan unionin ulkopuolelle, jos kyseisessä maassa taataan tietosuojan riittävä taso. Voidaan siirtää, kun Euroopan yhteisöjen komissio todennut, että kyseisessä maassa taataan tietosuojan riittävä taso. § 23 säädetään poikkeusperusteista tietojen siirtokieltoon, niitä ovat mm. yksiselitteinen suostumus, elintärkeä etu, yleinen etu, toimeksianto. Tietosuojavaltuutetun ohje: Jotta henkilötietojen ulkomaille siirto olisi laillista, tulee kahden edellytyksen täytyä:a) tietojen siirron tulee olla kyseisessä tilanteessa sallittua Suomessa jab) henkilötietojen ulkomaille siirron tulee täyttää henkilötietolaissa määritellyt, EU:n ulkopuolelletapahtuvaa siirtoa koskevat erityisedellytykset</p>	<p>Henkilötietojen siirrot kolmansiin maihin tai kansainvälisille järjestöille 44 art. Siirtoja koskeva yleinen periaate 45 art. Siirto tietosuojan riittävyttä koskevan päätöksen perusteella 46 art. Siirto asianmukaisia suojaotoimia soveltaen 47 art. Yritystä koskevat säännöt 48 art. Siirrot ja luovutukset, joita ei sallita unionin lainsäädännössä 49 art. Erityistilanteita koskeva poikkeukset 50 art. Kansainvälinen yhteistyö henkilötietojen suojaamiseksi Rekisterinpitäjän ja henkilötietojen käsittelijän on noudettava luvun V edellytyksiä ja säännöksiä, jotta henkilötietojen suojan tasoa ei vaaranneta. Komissio päättää ja julkaisee luettelon siitä, onko kyseinen kolmas maa tai yksi tai useampi tietty sektori tai kyseinen kansainvälinen järjestö riittävällä tietosuojan tasolla. Komissio julkaisee myös vastaavasti luettelo, joissa tietosuojan taso ei ole riittävä. Henkilötietojen siirto on mahdollinen, jos rekisterinpitäjä tai henkilötietojen käsittelijä on toteuttanut asianmukaiset suojaotoimet ja rekisteröityjen saattavilla on täytäntöönpanokelpoisia oikeuksia ja tehokkaita oikeussuojakeinoja. Siirto on mahdollista myös sellaisissa erityistilanteissa, mitkä on lueteltu 49 artiklassa (mm. suostumus, sopimus, yleinen etu).</p>	<p>Tietosuoja-asetus täydentää. Rekisterinpitäjän ja henkilötietojen käsittelijän vastuu korostuu. Komissio julkaisee luettelo turvallisuudesta alueista ja myös luettelo alueista, jotka eivät ole turvallisia. Kansainvälinen yhteistyö korostuu.</p>

<p>Rekisteröidyn oikeudet</p>	<p>§ 24 Informointi tietojenkäsittelystä § 25 Informointi tietojen käsittelystä tietyissä tapauksissa Rekisterinpitäjän on henkilötietoja kerätessään informoitava rekisteröityä seuraavilla tiedoilla: rekisterinpitäjä, edustaja, käsittelyn tarkoitus, säännönmukaiset luovutukset, miten rekisteröity pystyy käyttämään oikeuksiaan. Tiedot on annettava henkilötietoja kerätessä ja tallettaessa tai, jos tiedot hankitaan muulta kuin rekisteröidyltä itseltään ja tietoja on tarkoitus luovuttaa, viimeistään silloin kuin tietoja ensi kerran luovutetaan. Informoinnista voidaan poiketa, jos rekisteröity on saanut tiedot, jos se on välttämätöntä valtion turvallisuuden ym. vuoksi. Suoramainonnassa, etämyynnissä, markkina- ja mielipidetutkimuksen kyselyssä ym. on informoitava mistä tiedot hankittu. Puhelinmyynnissä vastaavat tiedot on annettava pyynnöstä.</p>	<p>12 art. Läpinäkyvä informointi, viestintä ja yksityiskohtaiset säännöt rekisteröidyn oikeuksien käyttöä varten Rekisterinpitäjän on toteutettava asianmukaiset toimenpiteet, jotta rekisteröity saa 13 ja 14 art. olevat tiedot ja 15-22 art. ja 34 art. mukaiset tiedot tiiviisti esitetyssä läpinäkyvässä, helposti ymmärrettävässä ja saatavilla olevassa muodossa selkeällä ja yksinkertaisella kielellä, varsinkin kun tiedot on tarkoitettu lapselle. Tiedot on toimitettava kirjallisesti tai muulla tavoin ja tapauksen mukaan sähköisessä muodossa. Jos rekisteröity pyytää, tiedot voidaan antaa suullisesti. Rekisteröidyn henkilöllisyys on varmistettava. Rekisterinpitäjällä on velvollisuus tunnistaa rekisteröity. Rekisterinpitäjän on lisäksi ilmoitettava rekisteröidylle tiedot toimenpiteistä, joihin on ryhdytty 15-22 art. nojalla ja viimeistään kuukauden kuluessa. Jos rekisteröity esittää pyynnön sähköisesti, tiedot on toimitettava sähköisesti, paitsi jos rekisteröity toisin pyytää. Jollei rekisterinpitäjä toteuta pyyntöjä rekisteröidyn pyynnön perusteella, rekisterinpitäjä on ilmoitettava syy viimeistään 1 kk kuluessa ja kerrottava mahdollisuudesta tehdä valitus. 13-14 ja 15–22 ja 34 art. perustuvat pyynnöt ovat maksuttomia. Mutta jos pyynnöt ovat perusteettomia tai kohtuuttomia tai toistuvia, rekisterinpitäjä voi periä kohtuullisen maksun, kieltäytyä suorittamasta pyydettyä toimea. Rekisterinpitäjän on osoitettava pyynnön ilmeinen perusteettomuus tai kohtuuttomuus. Artiklan 13–14 mukaiset tiedot voidaan antaa vakiomuotoisilla kuvakkeilla.</p>	<p>Tietosuoja-asetus täydentää sääntelyä koskien informointia ja rekisterinpitäjän velvollisuuksia. Rekisterinpitäjällä velvollisuus tunnistaa rekisteröity.</p>
--------------------------------------	--	---	---

Rekisteröidyn oikeudet		<p>13 art. Toimitettavat tiedot, kun henkilötietoja kerätään rekisteröidyltä Kun rekisteröidyltä kerätään häntä koskevia henkilötietoja on rekisteröidylle toimitettava seuraavat tiedot: rekisterinpitäjän/edustajan identiteetti ja yhteystiedot, tietosuojavastaavan yhteystiedot, käsittelyn tarkoitus ja oikeusperuste, vastaanottajat/ryhmät, tieto mahdollisesta siirrosta kolmanteen maahan tai kansainväliselle järjestölle, rekisterinpitäjän tai kolmannen osapuolen oikeutetut edut(ei koske viranomaisia), lisäksi on informoitava henkilötietojen säilytysaika, oikeus tarkastaa/oikaista/poistaa/rajoittaa/vastustaa/siirtää tietoja, oikeus peruuttaa suostumus, oikeus tehdä valitus, onko henkilötietojen antaminen lakisääteinen tai sopimukseen perustuva vaatimus, onko pakko toimittaa henkilötiedot, seuraamukset jollei toimita henkilötietoja, profiloinnin olemassaolo, muut käyttötarkoitukset. Tietoja ei tarvitse antaa, jos rekisteröity on jo saanut tiedot.</p>	<p>Tietosuoja-asetus täydentää sääntelyä koskien informointia ja täten rekisterinpitäjän velvollisuuksia.</p>
Rekisteröidyn oikeudet		<p>Rekisterinpitäjän on toimitettava rekisteröidylle seuraavat tiedot, kun henkilötietoja saadaan (henkilötietojen säilytysaika tai määrittämiskriteerit, miten rekisteröity voi käyttää oikeutta tarkastaa, oikaista, poistaa , rajoittaa tai vastustaa sekä oikeutta siirtää tiedot järjestelmästä toiseen, oikeus peruuttaa suostumus, oikeus tehdä valitus, onko henkilötietojen antaminen lakisääteinen tai sopimukseen perustuva vaatimus, onko pakko toimittaa tiedot, mitä seuraa jollei toimita, automaattisen profiloinnin olemassaolo). Käyttötarkoituksen muutos.</p>	<p>Tietosuoja-asetus täydentää sääntelyä koskien informointia ja täten rekisterinpitäjän velvollisuuksia.</p>

<p>Toimitettavat henkilötiedot, kun tietoja ei ole saatu rekisteröidyltä</p>		<p>14 art. Toimitettavat henkilötiedot, kun tietoja ei ole saatu rekisteröidyltä Kun tietoja ei ole saatu rekisteröidyltä, niin rekisterinpitäjän on toimitettava rekisteröidylle seuraavat tiedot: rekisterinpitäjän/edustajan tiedot, tietosuojavastaavan tiedot, käsittelyn tarkoitus, oikeusperusta, henkilötietoryhmät, vastaanottajat/vastaanottajaryhmät, siirtotieto, henkilötietojen säilytysaika/määrittämiskriteerit, oikeus tarkistaa/oikaista/poistaa/rajoittaa/siirtää tiedot, peruuttaa suostumus, oikeus tehdä valitus, profiloinnin olemassaolo. Käyttötarkoituksen muutos.</p>	<p>Tietosuoja-asetus täydentää sääntelyä koskien informointia ja täten rekisterinpitäjän velvollisuuksia.</p>
<p>Rekisterinpitäjän on toimitettava tiedot</p>	<p>§ 24 Informointi tietojen käsittelystä Tiedot on annettava henkilötietoja kerätessä ja tallettaessa, tai jos tiedot hankintaan muulta kuin rekisteröidyltä itseltään ja tietoja on tarkoitus luovuttaa, viimeistään silloin kun tietoja ensi kerran luovutetaan. Tiedonantovelvollisuudesta voidaan poiketa jos rekisteröity on saanut tiedot, jos se välttämätöntä valtion turvallisuuden, puolustuksen tai yleisen järjestyksen ja turvallisuuden vuoksi, rikosten ehkäisemiseksi tai selvittämiseksi taikka verotukseen tai julkiseen talouteen liittyvän valvontatehtävän vuoksi tai kerätessä tietoja muualta kuin rekisteröidyltä itseltään, jos tietojen antaminen rekisteröidylle on mahdotonta ja vaatii kohtuutonta vaivaa, tai aiheuttaa olennaista vahinkoa tai haittaa ja jos tietojen keräämisestä, tallentamista tai luovuttamisesta on nimenomaisesti säädetty.</p>	<p>14 art. Toimitettavat henkilötiedot, kun tietoja ei ole saatu rekisteröidyltä Tiedot on toimitettava kohtuullisen ajan kuluttua, viimeistään kuukauden kuluessa, kun yhteydenotto rekisteröityyn tapahtuu, tietojen luovutushetkellä. Jos rekisterinpitäjä aikoo käsitellä tietoja edelleen muuhun tarkoitukseen, on tästä ilmoitettava rekisteröidylle ja annettava samat tiedot, kuin tietoja kerätessä. Informointia ei tarvitse tehdä, mikäli rekisteröity on saanut tiedot, tietojen toimittaminen on mahdotonta tai vaatisi kohtuutonta vaivaa (erityisesti tietojen käsittely arkistoinnissa, tieteellisessä tai historiallisessa tutkimuksessa taikka tilastoinnissa), tietojen hankinnasta tai luovuttamisesta säädetään unionin oikeudessa tai jäsenvaltion lainsäädännössä, tiedot on pidettävä luottamuksellisena.</p>	<p>Tietosuoja-asetus täydentää sääntelyä koskien informointia ja täten rekisterinpitäjän velvollisuuksia.</p>

Rekisteröidyn oikeudet, tarkastusoikeus ja tarkastusoikeuden toteuttaminen, rekisteröidyn oikeus saada pääsy tietoihin	§ 26 Tarkastusoikeus Tarkastusoikeus (mitä tietoja talletettu tai ettei rekisterissä ole häntä koskevia tietoja, säännönmukaiset tietolähteet, mihin rekisterin tietoja käytetään ja säännönmukaiset luovutukset ja automaattisen käsittelyn toimintaperiaatteet). Toteuttaminen (henkilökohtainen käynti, kirjallisesti allekirjoitettu tai vastaava varmennus) tiedot annettava ilman aiheutonta viivytystä, ymmärrettävässä muodossa. Jos kieltäydytään tietojen antamisesta annettava todistus. 3 kk vastaamattomuus tulkitaan kieltäytymiseksi. Asian voi viedä tietosuojavaltuutetulle. Rekisterinpitäjä voi pyytää korvauksen, jos edellisestä tietojen antamisesta on kulunut vähemmän kuin yksi vuosi. Korvauksen tulee olla kohtuullinen eikä saa ylittää välittömiä kustannuksia.	15 art. Rekisteröidyn oikeus saada pääsy tietoihin Oikeus saada rekisterinpitäjältä vahvistus siitä, että häntä koskevia henkilötietoja käsitellään ei tai ei käsitellä (tarkoitus, henkilötietoryhmät, vastaanottajat, suunniteltu säilytysaika tai kriteerit, tiedon oikaiseminen tai poisto, rajoittaminen tai vastustaminen, tietojen alkuperä, profilointi, siirto kolmanteen maahan tai kansainväliselle järjestölle ja siirtoa koskevat suojatoimet). Tiedot toimitettava jäljennöksenä tai jos rekisteröity esittää pyynnön sähköisesti, niin tiedot on toimitettava sähköisesti yleisesti käytetyssä muodossa, paitsi jos rekisteröity toisin pyytää. Rekisterinpitäjä voi pyytää kohtuullisen maksun.	Tietosuoja-asetus täydentää henkilö-tietolakia. Lisää mm. sähköinen toimitaminen ja suojatoimien kuvaaminen.
Tarkastusoikeuden rajoitukset	§ 27 Tarkastusoikeuden rajoitukset Tarkastusoikeutta ei ole, jos tiedon antaminen vaarantaa valtion turvallisuutta, puolustusta tai yleistä järjestystä ja turvallisuutta, taikka haittaa rikosten ehkäisemistä tai selvittämistä, tiedon antaminen aiheuttaa vakavaa vaaraa rekisteröidyn terveydelle tai jonkun muun oikeudelle, henkilötiedot ovat yksinomaan historiallista tai tieteellistä tutkimusta tai tilastointia varten, henkilötietoja käytetään valvonta- ja tarkastustehtävissä.	15 art. Rekisteröidyn oikeus saada pääsy tietoihin Jäljennös tiedoista ei saa vaikuttaa haitallisesti muiden oikeuksiin tai vapauksiin. Rekisteröidyllä oikeus saada tietää, että häntä koskevia henkilötietoja käsitellään tai että niitä ei käsitellä. Tiedot on annettava rekisteröidylle sähköisesti yleisesti käytetyssä muodossa, jos rekisteröity näin pyytää.	Tietosuoja-asetus täydentää. Henkilötietolaissa on tarkemmin määriteltä, milloin oikeutta omiin tietoihin ei ole., esim. jos tiedon antamisesta on vaaraa omalle terveydelle.
Rekisteröidyn oikeudet, tiedon korjaaminen	§29 Tiedon korjaaminen Rekisterinpitäjän on ilman aiheutonta viivytystä oma-aloitteisesti tai rekisteröidyn vaatimuksesta oikaistava, poistettava tai täydennettävä rekisterissä oleva, käsitteilyn tarkoituksen kannalta virheellinen, tarpeeton, puutteellinen tai vanhentunut henkilötieto. Virheellisen tiedon levittäminen on myös estettävä. Jollei rekisterinpitäjä hyväksy tiedon korjaamista, on annetta kirjallinen todistus. Virheellisestä tiedosta on myös ilmoitettava sille, jolle rekisterinpitäjä on luovuttanut tai saanut virheellisen tiedon, jollei ole mahdotonta tai vaatii kohtuutonta vaivaa.	16 art. Oikeus tiedon oikaiseminen Rekisteröidyllä oikeus vaatia epätarkkojen tai virheellisten henkilötietojen oikaisemista ilman aiheutonta viivytystä . Rekisteröidyllä oikeus saada puutteelliset henkilötiedot täydennettynä.	Tietosuoja-asetus täydentää. Henkilötietolaissa on tarkemmin määriteltä mm. rekisterinpitäjän velvollisuudesta oma-aloitteisesti korjata virheellinen tieto.

<p>Rekisteröidyn oikeudet, kielto-oikeus, oikeus tiedon poistamiseen</p>	<p>§ 30 Kielto-oikeus Rekisteröidyllä on oikeus kieltää rekisterinpitäjää käsittelemästä itseään koskevia tietoja koskien: suorainonta, etämyynti, suoramarkkinointi, markkina - ja mielipidetutkimus, henkilömatrikkeli ja sukututkimus. Huom. § 14 tutkimus, § 15 tilasto, 16 § Viranomaisen suunnittelu- ja selvitystehtävät, § 35 Henkilötietojen siirto arkistoon</p>	<p>17 art. Oikeus tiedon poistamiseen (oikeus tulla unohtetuksi) Rekisteröidyllä on oikeus saada rekisterinpitäjä poistamaan rekisteröityä koskevat henkilötiedot ilman aiheetonta viivytystä ja rekisterinpitäjällä on velvollisuus poistaa henkilötiedot, kun: henkilötietoja ei enää tarvita niihin tarkoituksiin, joita varten ne kerättiin ja käsiteltiin , rekisteröity peruuttaa suostumuksen eikä käsittelyyn ole muuta laillista perustella, rekisteröity vastustaa käsittelyä, henkilötietoja on käsitelty lainvastaisesti, poistaminen perustuu lakiin). Poistamista ei sovelleta, jos käsittely on tarpeen: sanavapautta ja tiedonvälityksen vapautta koskevan oikeuden käyttämiseksi, henkilötietojen käsittely perustuu lakisääteiseen velvoitteeseen, käsittely on yleistä etua tai julkisen vallan käyttöä, arkistotarkoitus, tieteellinen ja historiallinen tutkimus tai tilasto, tai oikeudellinen vaade. Rekisterinpitäjän oin ilmoitettava henkilötietoja käsitteleville rekisterinpitäjille, että rekisteröity on pyytänyt poistamaan henkilötietoihin liittyvät linkit, jäljennökset ja kopiot, mikäli rekisteröidyllä on oikeus saada tiedot poistettua. 89 art. Säättää arkistoinnista, tutkimuksesta ja tilastoinnista, periaate tietojen minimoinnin periaatteen noudattaminen</p>	<p>Tietosuoja-asetus täydentää. Rekisteröidyllä oikeus tulla jossain tapauksissa unohtetuksi. Tietojen minimointi.</p>
<p>Rekisteröidyn oikeudet</p>		<p>18 art. Oikeus käsittelyn rajoittamiseen Rekisteröidyllä on oikeus käsittelyn rajoittamiseen, jos yksi seuraavista täyttyy: rekisteröity kiistää henkilötietojen paikansapitävyyden, käsittely on lainvastaista, rekisteröity vastustaa henkilötietojen poistamista ja vaatii rajoittamista, rekisterinpitäjä ei enää tarvitse kyseisiä henkilötietoja, mutta rekisteröity tarvitsee niitä oikeudelliseen vaateeseen, rekisteröity vastustaa henkilötietojen käsittelyä. Rajoitettuja tietoja saa käsitellä ainoastaan rekisteröidyn suostumuksella, taikka oikeudellisen vaateen laatimiseksi, esittämiseksi tai puolustamiseksi, tai oikeuksien suojaamiseksi tai tärkeän yleisen edun koskevista syistä. Rekisterinpitäjällä ilmoitusvelvollisuus.</p>	<p>Tietosuoja-asetus tuo uutta.</p>

Rekisteröidyn oikeudet		19 art. Henkilötietojen oikaisua tai poistoa tai käsittelyn rajoitusta koskeva ilmoitusvelvollisuus Rekisterinpitäjän on ilmoitettava kaikenlaisista 16 artiklan, 17 artiklan 1 kohdan ja 18 artiklan mukaisesti tehdyistä henkilötietojen oikaisusta, poistoista tai käsittelyn rajoituksista jokaiselle vastaanottajalle, jolle henkilötietoja on luovutettu, paitsi jos tämä osoittautuu mahdottomaksi tai vaatii kohtuutonta vaivaa. Rekisterinpitäjän on ilmoitettava rekisteröidylle näistä vastaanottajista, jos rekisteröity sitä pyytää.	Tietosuoja-asetus tuo uutta.
Rekisteröidyn oikeudet		20 art. Oikeus siirtää tiedot järjestelmästä toiseen Rekisteröidyllä on oikeus saada häntä koskevat henkilötiedot jäsennellyssä, yleisesti käytetyssä ja koneellisesti luettavassa muodossa ja oikeus siirtää kyseiset tiedot toiselle rekisterinpitäjälle, jos käsittely perustuu suostumukseen, sopimukseen ja käsittely on automaattista. Tätä ei sovelleta, käsittelyyn, joka on tarpeen yleistä etua koskevan tehtävän suorittamiseen tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämistä varten.	Tietosuoja-asetus tuo uutta. Tietojen siirto järjestelmästä toiseen.
Rekisteröidyn oikeudet, 21 art.		21 art. Vastustamisoikeus Rekisteröidyllä on oikeus henkilökohtaiseen erityiseen tilanteeseensa liittyvällä perusteella milloin tahansa vastustaa häntä koskevien henkilötietojen käsittelyä, joka perustuu 6 art. kohtiin e tai f (e) yleistä etua koskevan tehtävän suorittamiseksi tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi tai f) 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.) Kohtaa f ei sovelleta viranomaisten suorittaman tietojenkäsittelyn yhteydessä. Rekisterinpitäjä ei saa käsitellä tällaisia tietoja, jollei se voi osoittaa huomattavan tärkeää etua ja perusteltu syy. Huomioitava on myös tietojen käyttö 89 art. mukaisiin tarkoituksiin. Rekisteröidyllä on oikeus vastustaa henkilötietojen käsittelyä, paitsi jos on kyseessä yleistä etua koskevan tehtävän suorittaminen.	Tietosuoja-asetus tuo uutta.

Rekisteröidyn oikeudet, 21 art.	§ 30 Kielto-oikeus Rekisteröidyllä on oikeus kieltää rekisterinpitäjää käsittelemästä itseään koskevia tietoja koskien: suoramainonta, etämyynti, suoramarkkinointi, markkina - ja mielipidetutkimus, henkilömatrikkeli ja sukututkimus.	21 art. Vastustamisoikeus Rekisteröidyllä on oikeus, milloin tahansa vastustaa häntä koskevien henkilötietojen käsittelyä suoramarkkinointia varten, mukaan lukien profilointi. Jos kiello on olemassa, tietoja ei saa enää käsitellä tähän tarkoitukseen. Oikeudesta vastustaa on saatettava rekisteröidyn tietoon ja esitettävä selkeästi muusta tiedotuksesta erillään.	Tietosuoja-asetus tuo uutta.
Rekisteröidyn oikeudet	§ 31 Automatisoitu päätös Automatisoitu päätös, mikä arvioi rekisteröidyn tiettyjä ominaisuuksia ja josta aiheutuu rekisteröidylle oikeudellisia vaikutuksia tai muuten vaikuttaa häneen merkittävällä tavalla, on sallittu vain jos siitä on laissa säädetty tai päätös tehdään sopimuksen tekemisen tai täytäntöönpanon yhteydessä. Rekisteröidyn oikeudet on suojattava tai että päätöksellä täytetään rekisteröidyn pyyntö. § 36 mukaan tietosuojavaltuutetulle on tehtävä ilmoitus automatisoidun päätöksentekojärjestelmän käyttöönotosta. Poikkeuksia ilmoitusvelvollisuuteen mm. jos käsittelystä säädetään laissa.	22 art. Automatisoidut yksittäispäätökset, profilointi mukaan luettuna Rekisteröidyllä on oikeus olla joutumatta sellaisen päätöksen kohteeksi, joka perustuu pelkästään automaattiseen käsittelyyn, kuten profilointiin ja jolla on häneen koskevia oikeusvaikutuksia tai joka vaikuttaa häneen merkittävästi. Profilointi on sallittua vain, jos päätös on välttämätön rekisteröidyn ja rekisterinpitäjän välisen sopimuksen tekemistä tai täytäntöönpanoa varten. Profilointi perustuu lainsäädäntöön tai rekisteröidyn nimenomaiseen suostumukseen. Rekisterinpitäjän on huolehdittava rekisteröityjen etujen suojaamiseksi. Päätökset eivät saa perustua erityisiin henkilöryhmiin, paitsi jos on olemassa suostumus tai asia perustuu yleiseen etuun.	Tietosuoja-asetus täydentää. Lisänä profilointi sekä tarkemmat määräykset milloin profilointi on sallittua.
Rajoitukset	§ 27 Tarkastusoikeuden rajoitukset Tarkastusoikeutta ei ole, jos tiedon antaminen vahingoittaa valtion turvallisuutta, puolustusta tai yleistä järjestystä ja turvallisuutta, tiedon antamisesta saattaisi aiheutua vakavaa vaaraa rekisteröidylle tai jonkun muun oikeuksille, henkilötietoja käytetään yksinomaan historiallista tai tieteellistä tutkimusta taikka tilastointia varten.	23 art. Rajoitukset Unionin oikeudessa tai lainsäädännössä voidaan lainsäädäntötoimenpiteellä rajoittaa rekisteröidyn oikeuksia, tietoturvaloukkauksista ilmoittamista ja henkilötietojen käsittelyä koskevia periaatteita, jotta voidaan taata mm. kansallinen turvallisuus, puolustus, yleinen turvallisuus.	Tietosuoja-asetus täydentää. Tietosuoja-asetuksella annetaan lisäksi kansallista liikkumavaraa

Rekisterinpitäjän vastuu	§ 5 Huolellisuusvelvoite § 6 Henkilötietojen käsittelyn suunnittelu, § 7 Käyttötarkoitus-sidonnaisuus Huolellisuusvelvoite (laillisuus, huolellisuus, hyvä tietojenkäsittelytapa, ei rajoiteta rekisteröidyn yksityiselämän suojaa ja muita yksityisyyden suojan turvaavia perusoikeuksia. Velvollisuus on myös sillä, joka itsenäisenä elinkeinon- tai toiminnanharjoittajana toimii rekisterinpitäjän lukuun. 6 § Henkilötietojen käsittelyn tulee olla asiallisesti perusteltua. Henkilötietojen säännönmukainen hankinta ja luovutus on määriteltävä ennen henkilötietojen keräämistä tai muodostumista henkilörekisteriksi. 7§ Henkilötietoja saa käyttää vain siihen tarkoitukseen mihin tiedot on kerätty pois lukien historiallinen tutkimus, tieteellinen tai tilastokäyttö.	24 art. Rekisterinpitäjän vastuu Rekisterinpitäjän on toteutettava tarvittavat tekniset ja organisatoriset toimenpiteet, joilla voidaan varmistaa ja osoittaa, että käsittelyssä noudatetaan asetusta. Rekisterinpitäjän on pantava täytäntöön asianmukaiset tietosuojaa koskevat toimintaperiaatteet. Käytännössä säännöillä ja sertifiointimekanismeilla voidaan osoittaa, että asetettuja velvollisuuksia noudatetaan.	Tietosuoja-asetus täydentää. Rekisterinpitäjällä osoitusvelvollisuus.
---------------------------------	---	---	--

<p>Tietoturvallisuus ja tietojen säilytys Rekisterinpitäjän velvollisuudet, henkilötietojen käsittelijä</p>	<p>§ 32 Tietojen suojaaminen Rekisterinpitäjän on toteuttava tarpeelliset tekniset ja organisatoriset toimenpiteet henkilötietojen suojaamiseksi (asiattomalta pääsylvä tietoihin, ja vahingossa tai laittomasti tapahtuvalta tietojen hävittämislä, muuttamiselta, luovuttamiselta, siirtämiseltä tai muulta laittomalta käsittelyltä. Jos toimii rekisterinpitäjän lukuun tai jolle rekisterinpitäjä luovuttaa tietoja on annettava asianmukaiset selvitykset ja sitoumukset sekä muutoin riittävät takeet suojaamisesta.</p>	<p>32 art. Käsitteilyn turvallisuus Ottaen huomioon uusin tekniikka ja toteuttamiskustannukset, käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat, todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava riskiä vastaavan turvallisuustason varmistamiseksi asianmukaiset tekniset ja organisatoriset toimenpiteet: henkilötietojen pseudonymisointi ja salaust, kyky taata käsittelyjärjestelmien ja palveluiden jatkuva luottamuksellisuus, eheys, käytettävyyt ja vikasietoisuus, kyky palauttaa nopeasti tietojen saatavuus ja pääsy tietoihin, menettely, jolla testataan, tutkitaan ja arvioidaan säännöllisesti teknisten ja organisatoristen toimenpiteiden tehokkuutta. Huomiota on kiinnitettävä erityisesti riskeihin, erityisesti siirrettyjen, tallennettujen tai muutoin käsiteltyjen henkilötietojen vahingossa tapahtuvan tai laittoman tuhoamisen, häviämisen, muuttamisen, luvattoman luovuttamisen tai henkilötietoihin pääsyn vuoksi. Käytännēsäännöillä tai sertifiointi-mekanismeilla voidaan osoittaa vaatimusten noudattaminen. Rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava toimenpiteet sen varmistamiseksi, että jokainen rekisterinpitäjän tai henkilötietojen käsittelijän alaisuudessa toimiva luonnollinen henkilö, jolla on pääsy henkilötietoihin, käsittelee niitä ainoastaan rekisterinpitäjän ohjeiden mukaisesti, ellei unionin oikeudessa tai jäsenvaltion lainsäädännössä toisin vaadita.</p>	<p>Tietosuoja-asetus tuo uutta. Velvollisuuksia (mm. osoitusvastuu asetuksen noudattamisesta ja toimintaperiaatteiden täytäntöönpano, riskiperusteinen toiminta, huomioitava sekä organisatoriset että tekniset toimenpiteet, toiminnan jatkuvuuden turvaaminen (käytännēsäännöt, sertifiointi-menettelmät). Suomessa laki viranomaisen toiminnan julkisuudesta 621/1999 sisältää hyvän tiedonhallintatavan § 18 (saatavuus, käytettävyyt, suojaus, eheys)</p>
--	---	--	---

<p>Sisäänrakennettu ja oletusarvoinen tietosuoja</p>		<p>25 art. Sisäänrakennettu ja oletusarvoinen tietosuoja Rekisterinpitäjän on käsittelytapojen määrittämisen ja itse käsittelyn yhteydessä toteutettava tehokkaasti tietosuoja-periaatteita (tietojen minimointi, täytäntöönpanoa varten asianmukaiset tekniset ja organisatoriset toimenpiteet (pseudonymisointi, suojatoimet), jotta ne saadaan sisällytettyä käsittelyn osaksi ja jotta käsittely vastaisi asetuksen vaatimuksia ja rekisteröidyn oikeuksia suojataan. On pidettävä huoli, että käsitellään vain tarpeellisia henkilötietoja. Sertifiointimekanismia voidaan käyttää osoittamiseksi, että vaatimuksia noudetaan.</p>	<p>Tietosuoja-asetus tuo uutta. Velvollisuuksia mm. rekisterinpitäjän on ottaen huomioon uusimman tekniikan ja toteuttamiskustannukset sekä käsittelyn luonteen, laajuuden, asiayhteyden ja tarkoitukset sekä käsittelyn aiheuttamat todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit luonnollisten henkilöiden oikeuksille ja vapauksille. Rekisterinpitäjän on toimittava riskipohjaisesti.</p>
<p>Yhteisrekisterinpitäjä</p>		<p>26 art. Yhteisrekisterinpitäjät Jos vähintään kaksi rekisterinpitäjää määrittää yhdessä käsittelyn tarkoitukset ja keinot, ne ovat yhteisrekisterinpitäjiä. Heidän tulee määritellä vastualueet, todelliset roolit ja suhteet rekisteröityihin.</p>	<p>Tietosuoja-asetus tuo uutta. Henkilötietolaissa ei ole yhteisrekisterinpitäjää.</p>

<p>Rekisterinpitäjän velvollisuudet, henkilötietojen käsittelijä</p>	<p>§ 32 Tietojen suojaaminen § 33 Vaitiolovelvollisuus §5 Huolellisuusvelvoite §6 Henkilötietojen käsittelyn suunnittelu § 7 Käyttötarkoitussidonnaisuus § 32 Itsenäisen elinkeinoharjoittajan, joka toimii rekisterinpitäjän lukuun tai jolle luovutetaan tietoja teknisen käyttöyhteyden avulla, on annettava rekisterinpitäjälle asianmukaiset selvitykset ja sitoumukset sekä riittävät takeet henkilötietojen suojaamisesta. §33 Jos on saanut tietää jotakin toisen henkilön ominaisuuksista, henkilökohtaisista oloista tai taloudellisesta asemasta, ei saa ilmaista saamiaan tietojaan sivulliselle. Huolellisuusvelvoite (laillisuus, huolellisuus, hyvä tietojenkäsittelytapa, ei rajoiteta rekisteröidyn yksityiselämän suojaa ja muita yksityisyyden suojan turvaavia perusoikeuksia. Sama velvollisuus on sillä, joka itsenäisenä elinkeinon- tai toiminnanharjoittajana toimii rekisterinpitäjän lukuun. 6 § Henkilötietojen käsittelyn tulee olla asiallisesti perusteltua. Henkilötietojen säännönmukainen hankinta ja luovutus on määriteltävä ennen henkilötietojen keräämistä tai muodostumista henkilörekisteriksi. 7 § Henkilötietoja saa käyttää vain siihen tarkoitukseen mihin tiedot on kerätty pois lukien historiallinen tutkimus, tieteellinen tai tilastokäyttö.</p>	<p>28 art. Henkilötietojen käsittelijä Henkilötietojen käsittelijällä tulee olla riittävät suojatoimet asianmukaisten teknisten ja organisatoristen toimien täytäntöönpanemiseksi niin, että käsittely täyttää asetuksen vaatimukset ja varmistetaan rekisteröidyn oikeuksien suojelu. Ei saa käyttää toisen henkilötietojen käsittelijän palveluksia ilman rekisterinpitäjän erityistä ja tai yleistä kirjallista lupaa, tiedotettava kaikista suunnitelluista muutoksista, käsittely on määritettävä sopimuksella, käsittely rekisterinpitäjän ohjeiden mukaisesti, salassapitovelvollisuus, toteuttaa 32 art. vaaditut toimenpiteet, huolehtia rekisteröidyn oikeuksista, turvallisuustaso, palauttaa henkilötiedot rekisterinpitäjälle. Sopimuksen tulee olla kirjallinen mukaan lukien sähköisessä muodossa. Kun toinen henkilötietojen käsittelijä ei täytä tietosuojavelvoitteitaan, alkupe- räinen henkilötietojen käsittelijä on täysimääräisesti vastuussa suhteessa rekisterinpitäjään. 90 art. Salassapitovelvollisuus. Jäsenvaltiot voivat antaa erityissääntöjä valvontaviranomaiselle saada tietoja rekisterinpitäjältä ja saada pääsy henkilötietoihin.</p>	<p>Tietosuoja-asetus täydentää. Tarkempia määräyksiä myös henkilötietojen käsittelijälle. Edellyttää rekisterinpitäjältä kattavan sopimuksen tekemistä ja hyvää ohjeistusta. Valvontaviranomainen voi hyväksyä vakiosopimuslausekkeita.</p>
<p>Tietojenkäsittely rekisterinpitäjän ja henkilötietojen käsittelijän alaisuudessa</p>		<p>29 art. Tietojenkäsittely rekisterinpitäjän ja henkilötietojen käsittelijän alaisuudessa 33 art. Henkilötietojen tietoturvaloukkauksista ilmoittaminen valvontaviranomaisille Henkilötietoja saa käsitellä vain rekisterinpitäjän ohjeiden mukaisesti. Henkilötietojen käsittelijän on ilmoitettava rekisterinpitäjälle tietoturvaloukkauksista ilman aiheetonta viivytystä</p>	<p>Tietosuoja-asetus täydentää ja tuottaa (33 art.) Korostaa rekisterinpitäjän ohjeita.</p>

<p>Tietoturvaloukkauksista ilmoittaminen</p>		<p>33 art. Henkilötietojen tietoturvaloukkauksista ilmoittaminen Tietoturvaloukkauksesta on ilmoitettava valvontaviranomaiselle ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 72 h kuluessa, paitsi jos ei todennäköisesti aiheudu luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvaa riskiä. Ilmoitus pitää sisällään: (kuvaus, tietosuojavastaavan yhteystiedot, seuraukset, ryhmät joita koskee, toimenpiteet). Rekisterinpitäjän on dokumentoitava kaikki henkilötietojen tietoturvaloukkaukset sen vaikutukset ja toteutetut korjaavat toimet. Henkilötietojen käsittelijän on ilmoitettava tietoturvaloukkauksesta rekisterinpitäjälle ilman aiheetonta viivytystä.</p>	<p>Tietosuoja-asetus tuo uutta. Henkilötietojen tietoturvaloukkauksista on tehtävä määräajassa ilmoitus valvontaviranomaiselle. Myös henkilötietojen käsittelijän on tehtävä viipymättä ilmoitus rekisterinpitäjälle. Valvontaviranomaisen on voitava dokumentoinnin avulla tarkistaa, että artiklaa on noudatettu.</p>
<p>Tietoturvaloukkauksista ilmoittaminen rekisteröidylle</p>		<p>34 art. Henkilötietojen tietoturvaloukkauksista ilmoittaminen rekisteröidylle Kun tietoturvaloukkaus aiheuttaa korkean riskin luonnolliselle henkilölle, on rekisterinpitäjän ilmoitettava tietoturvaloukkauksesta ilman aiheetonta viivytystä. Ilmoituksessa oltava tietosuojavastaavan yhteystiedot, seuraukset, toimenpiteet. Ilmoitusta ei tarvitse tehdä, jos se vaatisi kohtuutonta vaivaa, rekisterinpitäjä on toteuttanut tekniset ja organisatoriset suoja-toimenpiteet ja toteuttanut jatkotoimenpiteitä riskin välttämiseksi.</p>	<p>Tietosuoja-asetus tuo uutta. Tietoturvaloukkauksista on ilmoitettava ilman aiheetonta viivytystä rekisteröidylle.</p>

<p>Henkilörekisterin hävittäminen</p>	<p>§ 34 Henkilörekisterin hävittäminen Tarpeeton henkilörekisteri on hävitettävä, jollei siihen talletettuja tietoja ole erikseen säädetty tai määrätty säilytettäväksi tai jollei rekisteriä siirretä arkistoon § 35 mukaisesti.</p>	<p>17 art. Oikeus tiedon poistamiseen Rekisteröidyllä on oikeus saada rekisterinpitäjä poistamaan rekisteröityä koskevat henkilötiedot ilman aiheetonta viivytystä ja rekisterinpitäjällä on velvollisuus poistaa henkilötiedot, kun: henkilötietoja ei enää tarvita niihin tarkoituksiin, joita varten ne kerättiin ja käsiteltiin, rekisteröity peruuttaa suostumuksen eikä käsittelyyn ole muuta laillista perustella, rekisteröity vastustaa käsittelyä, henkilötietoja on käsitelty lainvastaisesti, poistaminen perustuu lakiin). Poistamista ei sovelleta, jos käsittely on tarpeen: sanavapautta ja tiedonvälityksen vapautta koskevan oikeuden käyttämiseksi, henkilötietojen käsittely perustuu lakisääteiseen velvoitteen, käsittely on yleistä etua tai julkisen vallan käyttöä, arkistotarkoitus, tieteellinen ja historiallinen tutkimus tai tilasto, tai oikeudellinen vaade. Rekisterinpitäjän oin ilmoitettava henkilötietoja käsitteleville rekisterinpitäjille, että rekisteröity on pyytänyt poistamaan henkilötietoihin liittyvät linkit, jäljennökset ja kopiot, mikäli rekisteröidyllä on oikeus saada tiedot poistettua.</p>	<p>Tietosuoja-asetus täydentää</p>
--	---	--	---

		<p>Huom. 89 art. Yleisen edun mukaisia arkistointitarkoituksia taikka tieteellisiä tai historiallisia tutkimustarkoituksiatai tilastollisia tarkoituksia varten tapahtuvaa käsittelyä koskevat suojatoimet ja poikkeukset Yleisen edun mukaisia arkistointitarkoituksia taikka tieteellisiä ja historiallisia tutkimus-tarkoituksia tai tilastollisia tarkoituksia varten tapahtuvaan käsittelyyn sovelletaan rekisteröidyn oikeuksia ja vapauksia koskevia asianmukaisia suojatoimia tämän asetuksen mukaisesti. Näillä suojatoimilla on varmistettava, että on toteutettu tekniset ja organisatoriset toimenpiteet, joilla taataan etenkin tietojen minimoinnin periaatteen noudattaminen. Tällaisia toimenpiteitä voivat olla esimerkiksi pseudonymisointi, jos mainitut tarkoitukset voidaan täyttää tällä tavoin. Jos nämä tarkoitukset on mahdollista täyttää käsittelemällä myöhemmin tietoja, minkä johdosta ei ole mahdollista tai ei ole enää mahdollista tunnistaa rekisteröityjä, nämä tarkoitukset on täytettävä tällä tavoin. Kansallinen lainsäädäntö voi säätää poikkeuksia ilmoittamiseen ja pääsy henkilötietoihin, tietojen oikaisemiseen ja poistamiseen sekä oikeuteen vastustaan henkilötietojen käsittelyä ja automaattisesti tehtäviä yksittäispäätöksiä.</p>	<p>Tietosuoja-asetus täydentää, painottaa teknisiä ja organisatorisia toimenpiteitä</p>
Käytännäsäännöt	<p>42 § Toimialakohtaiset käytännäsäännöt Rekisterinpitäjät tai näitä edustavat yhteisöt voivat laatia toimialakohtaisia käytännäsääntöjä. Tietosuoja-valtuutettu voi tarkastaa.</p>	<p>40 art. Käytännäsäännöt Jäsenvaltioiden, valvontaviranomaisten, tietosuojaneuvoston ja komission on edistettävä käytännäsääntöjen laatimista. Käytännäsäännöt toimitettava valvontaviranomaiselle. Valvontaviranomainen toimittaa käytännäsäännöt tietosuojaneuvostolle, jos ne liittyvät käsittelytoimiin useissa eri jäsenvaltioissa.</p>	<p>Tietosuoja-asetus täydentää nykyistä, sillä alueena on EU:n jäsenvaltiot.</p>
Henkilötietojen käsittelyn ohjaus ja valvonta	<p>§ 38 Tietosuojaviranomaiset Tietosuojavaltuutettu ja tietosuojalautakunta</p>	<p>51 art. Valvontaviranomainen 68 art. Euroopan tietosuojaneuvosto</p>	<p>Tietosuoja-asetus täydentää nykyistä, sillä alueena on EU:n jäsenvaltiot.</p>

Vahingonkorvausvelvollisuus	47 § Vahingonkorvausvelvollisuus Taloudellinen ja muu vahinko rekisteröidylle tai muulle henkilölle	82 art. Vastuu ja oikeus korvauksen saamiseen Kukin rekisterinpitäjän on vastuussa vahingosta, joka on aiheutunut käsittelystä, jolla on rikottu asetusta. Myös henkilötietojen käsittelijä on vastuussa vahingosta, jos se ei noudattanut henkilötietojen käsittelijälle osoitettuja velvoitteita tai jos se on toiminut rekisterinpitäjän lainmukaisen ohjeistuksen ulkopuolella tai sen vastaisesti.	Tietosuoja-asetus tuo uutta , vastuu myös henkilötietojen käsittelijällä, jos ei ole noudattanut asetuksen velvoitteita tai jos se on toiminut rekisterinpitäjän ohjeistuksen ulkopuolella tai sen vastaisesti.
Uhkakko	46§ Uhkakko Tietosuojavaltuutettu voi asettaa uhkasakon päätöksensä tehosteeksi.	83 art. Hallinnollisten sakkojen määräämisen yleiset edellytykset 84 art. Seuraamukset Hallinnollinen sakko 10-20 milj. euroa tai yritystä koskeva 2-4 % kokonaisliikevaihdosta	Tietosuoja-asetus tuo uutta. Sakot määräytyvät mm. mitä asetuksen kohtaa rikkoo.
Rangaistussäännökset	48 § Rangaistussäännökset Henkilörekisteririkkomus		
Ilmoitusvelvollisuus, Vaikutustenarviointi ja Ennakkokuuleminen	36 § Ilmoitusvelvollisuus 37§ Ilmoituksen tekeminen Ilmoitusvelvollisuus tietosuojavaltuutetulle henkilötietojen automaattisesta käsittelystä ja jos henkilötietoja siirretään EU:ssa tai EU:n ulkopuolelle tai automatisoidun päätöksentekojärjestelmän käyttöönotosta. Ilmoitusvelvollisuutta ei ole mm. lakisääteisissä asioissa.	35 art. Tietosuojaa koskeva vaikutustenarviointi 36 art. Ennakkokuuleminen Jos uutta teknologiaa käytettäessä muodostuu korkea riski luonnollisen henkilön oikeuksille ja vapauksille, on rekisterinpitäjän tehtävä vaikutusten arviointi. Rekisterinpitäjän on pyydettävä neuvoa tietosuojavastaavalta. Valvontaviranomaisten tulee julkaista luettelo käsittelytoimien tyypeistä, jolloin vaikutusten arviointi on tehtävä. Rekisterinpitäjän on ennen käsittelyä kuultava valvontaviranomaista korkean riskin käsittelyissä, jollei riskiä ole saatu pienennettyä.	Tietosuoja-asetus tuo uutta. Vaikutustenarviointi ja ennakkokuuleminen.

Tietosuoja-vastaavan nimittäminen		37 art. Tietosuojavastaavan nimittäminen 38 art. Tietosuojavastaavan asema 39 art. Tietosuojavastaavan tehtävät Rekisterinpitäjän ja henkilötietojen käsittelijän on nimitettävä tietosuojavastaava, kun tietojenkäsittelyä suorittaa jokin muu viranomainen tai julkishallinnon elin kuin lainkäyttötehtävää hoitava tuomioistuin, ydintehtävät muodostuvat käsittelytoimista, jotka edellyttävät laajamittaista rekisteröityjen säännöllistä ja järjestelmällistä seuranta- tai erityisiin henkilöryhmiin. Konsernilla voi olla yksi ja viranomaisilla yhteinen, lisäksi tietosuojavastaavan tehtävää voi hoitaa palvelusopimuksen perusteella. Tietosuojavastaavan yhteystiedot on ilmoitettava valvontaviranomaiselle. Tietosuojavastaavan asemasta säädetään artiklassa 38 ja tehtävistä säädetään 39 artiklassa.	Tietosuoja-asetus tuo uutta, henkilö-tietolaissa ei ole velvollisuutta nimit-tää tietosuojavastaava. Tietosuoja-vastaavan nimittäminen on §24, L sähköisestä lääkemääräyksestä 61/2007:Rekisterinpitäjällä, terveydenhuollon toimintayksiköllä, sosiaalihuol-lon toimintayksiköllä ja apteekilla on oltava seuranta- ja valvontatehtävää varten nimettynä tietosuojavastaava sekä L sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä 159/2007 §20: Jokaisella palvelujen antajalla ja Kansaneläkelaitoksella on oltava seuranta- ja valvontatehtävää varten tietosuojavastaava
Sertifiointi		42 art. Sertifiointi Jäsenvaltion, valvontaviranomaiset, tietosuojaneuvosto ja komissio kannustavat ottamaan käyttöön tietosuojaa koskevia sertifiointimekanismeja sekä tietosuojasinettejä ja -merkkejä. Sertifiointimekanismien käyttöönotto on vapaaehtoista.	Tietosuoja-asetus tuo uutta.
Tietosuojaviranomais-ten tiedonsaanti- ja tarkastusoikeus, Yhteis-työ valvontaviranomai-sen kanssa	39 § Tietosuojaviranomaisten tiedonsaanti- ja tarkastusoikeus Tietosuojavaltuutetulla on oikeus saada salassapito-säännösten estämättä tiedot käsiteltävistä henkilöistä sekä tiedot, jotka ovat tarpeen henkilötietojen käsittelyn lainmukaisuuden valvonnassa.	31 art. Yhteistyö valvontaviranomaisen kanssa Rekisterinpitäjän tai henkilötietojen käsittelijän tai niiden edustajien on pyynnöstä tehtävä yhteistyötä valvontaviranomaisen kanssa.	Tietosuoja-asetus täydentää.

LIITE 3. Yhteenvedo henkilötietolain ja tietosuoja-asetuksen arvioinnista.**Selkeyttää**

Soveltamisalue (1-2 art.)

Käsittelyn lainmukaisuus (6 art.)

Rekisteröidyn vastustamisoikeus (21 art.)

Täydentää

Lisää määritelmiä (4 art.)

Käsittelyn yleiset periaatteet, osoitusvelvollisuus, toiminnan läpinäkyvyys (5 art.).

Suostumus olemassaolo ja sisältö (4 art. ja 7 art.)

Eriyiset henkilötietoryhmät (9 art.).

Rekisteröidyn oikeudet (12–17 art.), tarkemmin Liite 4

Automatisoidut päätökset ja profilointi (22 art.)

Rajoituksia rekisteröidyn oikeuksiin (23 art.)

Vastuu teknisistä ja organisatorista toimenpiteistä, osoitusvelvollisuus (24 art.)

Henkilötietojen käsittelijä ja velvollisuudet (28-29 art.)

Seloste käsittelytoimista (30 art.)

Käytännestännöt (40 art.)

Valvontaviranomainen (31 art., 51 art., 68 art.)

Edellytykset henkilötietojen siirtoon EU:n ulkopuolelle (44 art-50 art.)

Arkistoon siirto, painottaa teknisiä ja organisatorisia toimenpiteitä (89 art.).

Uutta

Lapsen suostumus tietoyhteiskunnan palveluihin (8 art.)

Rekisterinpitäjän velvollisuus tunnistaa rekisteröity (11 art.)

Rekisteröidyn oikeudet (18- 21 artiklat), tarkemmin Liite 4

Sisäänrakennettu ja oletusarvoinen tietosuoja (25 art.)

Yhteisrekisterinpito (26 art.)

Riskiperustainen toiminta (32 art.)

Ilmoitus tietoturvaloukkauksista valvontaviranomaiselle ja rekisteröidylle, aikarajoitus (33-34 art.)

Vaikutustenarviointi (35 art.)

Ennakkokuuleminen (36 art.)

Tietosuojavastaavan nimittäminen, asema ja tehtävät (37-39 art.)

Sertifiointimenettely (42 art.)

Rekisterinpitäjän ja henkilötietojen käsittelijän vastuu vahingosta ja korvausvelvollisuus (82 art.)

Hallinnolliset sakot (83-84 art.)

LIITE 4. Rekisteröidyn oikeudet.**Alla ryhmiteltynä lyhyesti rekisteröidyn oikeudet, mitkä täydentyvät henkilötietolaista verrattuna henkilötietolakiin.**

Oikeus informaatioon (art. 12, 13 ja 14):

- oikeus saada enemmän informaatiota henkilötietoja kerätessä
- jos tietoa ei kerätä rekisteröidyltä, oikeus saada informaatio kohtuullisessa ajassa tai viestittäessä rekisteröidylle ensimmäisen kerran
- informaatio tiiviisti esitettyssä ja helposti ymmärrettävässä muodossa selkeällä ja yksinkertaisella kielellä
- velvollisuus tunnistaa rekisteröity

Tarkastusoikeus (15 art.):

- oikeus saada rekisterinpitäjältä vahvistus, että häntä koskevia henkilötietoja käsitellään tai ei käsitellä
- jos henkilötietoja käsitellään, rekisteröidyllä on oikeus saada tieto muun muassa käsittelyn tarkoituksista ja kyseessä olevista henkilötietojen ryhmistä
- oikeus saada jäljennös käsiteltävistä henkilötiedoista yleisesti käytetyssä sähköisessä muodossa, jos rekisteröity tekee tarkastuspyynnön sähköisesti eikä toisin pyydä

Oikeus tiedon oikaisemiseen (16 art.):

- rekisteröidyllä oikeus vaatia epätarkkojen tai virheellisten henkilötietojen oikaisemista ilman aiheetonta viivytystä sekä oikeus saada puutteelliset henkilötiedot täydennettyä

Oikeus tietojen poistamiseen (17 art.):

- oikeus vaatia, että rekisterinpitäjä poistaa rekisteröityä koskevat tiedot, kun muun muassa tietoja ei enää tarvita niihin tarkoituksiin, joita varten henkilötie-

dot on kerätty ja käsitelty, rekisteröity on peruuttanut suostumuksensa eikä käsitelyyn ole muuta laillista perustetta

- rekisterinpitäjä on ilmoitettava henkilötietoja käsitteleville, että rekisteröity on pyytänyt poistamaan henkilötietoihin liittyvät linkit, jäljennökset ja kopiot, mikäli rekisteröidyllä on tietojen poistamisen oikeus
- poistamista ei sovelleta muun muassa, jos käsittely perustuu lakisääteiseen velvoitteeseen

Alla ryhmiteltynä lyhyesti rekisteröidyn oikeudet, mitkä ovat uutta tietosuojasetuksessa verrattuna henkilötietolakiin.

Oikeus käsittelyn rajoittamiseen ja oikaisua tai poisto tai käsittelyn rajoitusta koskeva ilmoitusvelvollisuus (18, 19 art.):

- rekisteröidyllä on tietyissä tapauksissa oikeus käsittelyn rajoittamiseen
- näitä tapauksissa ovat muun muassa rekisteröity kiistää henkilötietojen paikkansapitävyyden, käsittely on lainvastaista, rekisteröity vastustaa henkilötietojen poistamista ja vaatii rajoittamista
- rajoitettuja tietoja saa käsitellä vain rekisteröidyn suostumuksella
- rekisterinpitäjällä on ilmoitusvelvollisuus koskien henkilötietojen oikaisua, poistoa tai käsittelyn rajoitusta
- rekisterinpitäjän on tehtävä ilmoitus jokaiselle vastaanottajalle, jolle henkilötietoja on luovutettu, jollei ilmoitus ole mahdotonta tai vaatii kohtuutonta vaivaa
- rekisterinpitäjän on ilmoitettava rekisteröidylle näistä vastaanottajista, jos rekisteröity sitä pyytää

Oikeus siirtää tiedot (20 art.)

- rekisteröidyn oikeus saada siirrettyä tiedot ne henkilötiedot, jotka rekisteröity on toimittanut rekisterinpitäjälle, järjestelmästä toiseen jäsennellyssä, yleisesti käytetyssä ja koneellisesti luettavassa muodossa ja siirtää tiedot toiselle rekisterinpitäjälle, jos käsittely perustuu suostumukseen tai sopimukseen ja käsittely suoritetaan automaattisesti

- edellä mainituissa tilanteissa oikeus saada henkilötiedot siirrettyä suoraan rekisterinpitäjältä toiselle, jos se teknisesti mahdollista
- siirto-oikeus ei kuitenkaan koske sellaisia henkilötietoja, joka koskee yleistä etua tai rekisterinpitäjän julkisen vallan käyttämistä varten.

Vastustamisoikeus (21 art.)

- rekisteröidyllä on oikeus vastustaa henkilötietojensa käsittelyä, jos kyseessä on yleistä etua koskevan tehtävän suorittaminen tai julkisen vallan käyttö, paitsi jos rekisterinpitäjä voi osoittaa, että käsittelyyn on olemassa huomattavan tärkeä ja perusteltu syy
- jos henkilötietoja käsitellään suoramarkkinointia varten, rekisteröidyllä on oikeus vastustaa käsittelyä, milloin tahansa
- poikkeuksia tähän vastustamiseen on muun muassa, kun henkilötietoja käsitellään yleisen edun mukaisiin arkistointitarkoituksiin taikka tieteellisiä tai historiallisiin tutkimustarkoituksiin tai tilastollisia tarkoituksia varten.
- tieto vastustamisoikeudesta on saatettava rekisteröidyn tietoon ja esitettävä muusta tiedotuksesta erillään

LIITE 5. Kysely lähtötilanne EU-tietosuoja-asetukseen liittyvistä velvoitteista**Lähtötilanne EU-tietosuoja-asetukseen liittyvistä velvoitteista**

Arvoisa vastaaja,

tällä kyselyllä on tarkoitus selvittää henkilötietolain soveltamisen nykytilanne organisaatiossanne. Euroopan unionin laajuinen EU-tietosuoja-asetus (2016/679) astuu voimaan 25.5.2018 ja samanaikaisesti nykyinen henkilötietolaki (523/1999) kumoutuu. Tietosuoja-asetus sisältää osittain samoja velvoitteita kuin henkilötietolaki, mutta tietosuoja-asetus tuo mukanaan myös uusia velvoitteita rekisterinpitäjälle. Lisäksi tietosuoja-asetuksen rinnalle on tulossa yleinen henkilötietolaki.

Vastauksianne käytetään hyödyksi rekisterinpitäjien velvollisuuksien ohjeistamiseen ja tietosuojakoulutuksen suunnittelussa. Kysely tuottaa aineistoa myös Kuntaliiton tiedonhallinnan erityisasiantuntija Tuula Sepon opinnäytetyöhön Itä-Suomen yliopiston sosiaali- ja terveydenhuollon tietohallinnon maisteriohjelmassa. Vastausten tulkinta ei tämän vuoksi ole Kuntaliiton virallinen kannanotto, vaikka kysely lähetetään Kuntaliitosta.

Vastaustanne käsittelee kyselyn tekijä, eikä yksittäistä organisaatiota ole mahdollista tunnistaa tuloksista. Tulokset julkistetaan organisaation tyyppin ja kuntien osalta kuntakoon perustuvan ryhmittelyn mukaisesti Kuntaliiton verkkosivuilla (www.kunnat.fi) ja yliopiston sivuilla (<http://www.uef.fi/web/kirjasto/tiedonhaku-ja-tiedonhaun-opetus/opinnaytetyot>).

Vastaukset hävitetään, kun opinnäyte on julkistettu.

Opinnäytetyön ohjaajina toimivat FT, lehtori Sirpa Kuusisto-Niemi Itä-Suomen yliopistosta ja Kuntaliitosta OTT, lakimies Ida Sulin. Toivomme, että osallistutte kyselyyn, jonka tuloksia käytämme hyväksi myös palvelumme parantamiseksi.

Pyydämme lisäksi ottamaan huomioon, että sosiaali- ja terveydenhuolto ei kuulu kyselyn piiriin. Kysely koskee siis kuntien, kuntayhtymien ja maakuntien muuta toimintaa.

Kysely koostuu seuraavista osioista:

Taustatiedot (kysymykset 1-5)

Henkilötietojen käsittelyä koskevat yleiset periaatteet (kysymykset 6-11)

Rekisteröidyn oikeudet (kysymykset 12–13)

Rekisteriseloste (kysymykset 14–16)

Tietosuojavastaava (kysymykset 17–18)

Tietoturva ja riskienhallinta (kysymykset 19)

Valmistautuminen EU-tietosuoja-asetukseen (kysymykset 20–26)

Kyselyyn vastaamista ei voi keskeyttää, mutta voitte etukäteen tutustua kysymyksiin esimerkiksi tulostamalla lomakkeen. Kyselyn linkin voi välittää organisaatiossanne eteenpäin ja siihen voi vastata useampi toimiala, esimerkiksi tekninen toimi, opetustoimi.

Merkitkää tällöin toimiala kysymykseen nro 2.

Lisätietoja kyselystä antaa erityisasiantuntija Tuula Seppo, tuula.seppo@kuntaliitto.fi, puh. 050 428 82 55

Taustakysymykset

1. Valitkaa organisaationne *

Kunta (vastatkaa tällöin kysymykseen nro 3)

Kuntayhtymä, mikä?

Maakuntien liitto

Muu, mikä?

2. Koskeeko vastauksenne *

Koko organisaatiota, ilman SOTE:a

Tiettyä toimialaa tai yksikköä, mikä?

3. Jos vastauksenne koskee peruskuntaa, niin kunnan asukasmäärä (tähän kysymykseen vastaavat vain kunnat)

alle 10.000

10.001-50.000

50.001-100.000

yli 100.000

4. Kyselyyn vastaajan/vastaajien asemat *

Voitte valita useamman kuin yhden, jos vastaatte kyselyyn yhdessä.

Hallintojohtaja tai vastaava hallinnosta vastaava

Tietohallintojohtaja ja vastaava tietohallinnosta vastaava

Asiakirjahallintojohtaja/Arkistajohtaja tai ko. alueista vastaava

Tietosuojavastaava

Tietoturvajohdaja tai vastaava tietoturvasta vastaava

Joku muu, kuka?

5. Onko organisaationne strategiassa tai kehittämistoiminnassa huomioitu henkilötietojen käsittelyyn tai yleisesti tiedonhallintaan liittyviä asioita? *

- Kyllä
- On huomioitu osittain
- Ei
- En tiedä

Henkilötietojen käsittelyä koskevat yleiset periaatteet

Henkilötietojen käsittelyä säädetään henkilötietolain 2 luvussa (§:t 5-9). Henkilötietoja tulee käsitellä huolellisesti ja asiallisesti ja hyvän tietojenkäsittelytavan mukaisesti. Henkilötietojen käytön tulee olla asiallisesti perusteltua ja käyttötarkoitussidonnaista (käyttötarkoitussidonnaisuus = tiettyyn tarkoitukseen kerättyjä henkilötietoja ei saa käyttää muihin tarkoituksiin, poikkeus tutkimus ja tilastointi). Vain tarpeellisia henkilötietoja saa käsitellä. Lisäksi henkilötietojen tulee olla virheettömiä. Laki sisältää lisäksi määräykset tietojen laatuun koskeviin periaatteisiin.

Henkilötieto = kaikenlainen luonnollista henkilöä taikka hänen ominaisuuksiaan tai elinolosuhteitaan kuvaavat merkinnät, joista henkilö tai hänen perheensä taikka hänen kanssaan yhteisessä taloudessa asuvat voidaan tunnistaa. Henkilötietoja ovat esimerkiksi nimi, henkilötunnus, sijaintitieto, verkkotunniste, auton rekisteritunnus, valokuva, bonuskortti, katuosoite, peitenimi.

Henkilötietojen käsittely = henkilötietojen kerääminen, tallettaminen, järjestäminen, käyttö, siirtäminen, luovuttaminen, säilyttäminen, muuttaminen, yhdistäminen, suojaaminen, poistaminen, tuhoaminen ja muut henkilötietoihin kohdistuvat toimenpiteet

Rekisterinpitäjä = yksi tai useampi henkilö, yhteisö, laitos tai säätiö, joka käyttöä varten henkilörekisteri perustetaan ja jolla on oikeus määrätä henkilörekisterin käytöstä tai jonka tehtäväksi rekisterinpito on lailla säädetty.

Rekisteröity = henkilö, jota henkilötieto koskee
Käyttötarkoitussidonnaisuuden vaatimus merkitsee, että tiettyyn tarkoitukseen kerättyjä henkilötietoja ei saa käyttää muuhun tarkoitukseen

6. Onko organisaatiossanne määritelty kenellä on oikeus käsitellä henkilötietoja? *

Henkilötietolaki 5 §

- Kyllä
- On määritelty osittain
- Ei
- En tiedä

7. Onko organisaatiollanne ohjeet seuraavista asioista? *

Henkilötietolaki §:t 3, 5-9 ja 13 §, 35 § Suostumus on kaikenlainen vapaaehtoinen, yksilöity ja tietoinen tahdon ilmaisu, jolla rekisteröity hyväksyy henkilötietojensa käsittelyn.

	Kyllä	Ei	En tiedä
Henkilötietojen käsittelystä	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Henkilötunnuksen käsittelystä	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Suostumuksen käsittelystä	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Asiakirjallisen tiedon säilyttämisen periaatteista	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

8. Onko organisaationne ohjeistanut tai onko sopimuksissanne mainintaa henkilötietojen käsittelystä koskien ulkopuolisia henkilötietojen käsittelijöitä (esim. ostopalveluiden tuottajia tai tietojärjestelmätoimittajia)?

Henkilötietolaki 5 §

	Kyllä	Ei	En tiedä
Ohjeistettu erillisillä ohjeilla	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Huomioitu sopimuksissa	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Muulla tavoin, miten? _____	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

9. Pystytkö todentamaan toiminnassanne käyttötarkoituksen, jota varten henkilötietoja kerätään? (Esimerkiksi palkanmaksu, koulutuksen osallistujaluettelo) *

Henkilötietolaki 7 §

- Kyllä
Ei
En tiedä

10. Käsittelettekö organisaatiossanne arkaluonteisia henkilötietoja (näitä ovat esimerkiksi rotu, henkilön yhteiskunnallinen, poliittinen tai uskonnollinen vakaumus tai ammattiliittoon kuuluminen, etninen alkuperä, terveystiedot, sosiaalihuollon tarve ja palvelut, seksuaalinen suuntautuminen) *

Henkilötietolaki §:t 11-12

- Kyllä Ei En tiedä

11. Jos vastasitte kyllä edelliseen kysymykseen, niin voitteko täsmentää, onko organisaatiossanne ohjeistusta arkaluonteisten henkilötietojen käsittelystä?

Henkilötietolaki § 11 ja § 12

- Kyllä Ei En tiedä

Rekisteröidyn oikeudet

Rekisteröityä on informoitava henkilötietojen käsittelystä. Rekisteröidyllä on tarkastusoikeus siihen, mitä tietoja hänestä on talletettu tai ettei rekisterissä ole häntä koskevia tietoja. Rekisteröidylle on ilmoitettava säännönmukaiset tietolähteet sekä mihin rekisterin tietoja käytetään. Rekisteröidyllä on oikeus saada tietää automaattiseen käsittelyyn liittyvistä periaatteista. Rekisteröidyllä on oikeus saada virheellinen, tarpeeton, puutteellinen tai vanhentunut henkilötieto oikaistavaksi, poistettavaksi tai täydennettäväksi. Henkilötietolaki §:t 24-31

12. Informoitteko rekisteröityä? *

Henkilötietolaki 3 §: Rekisteröity on henkilö, jota henkilötieto koskee.

	Kyllä	Ei	En tiedä
Mistä rekisteröidyn tiedot on hankittu tai saatu	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Rekisterinpitäjistä ja sen mahdollisesta edustajasta	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Henkilötietojen käsittelyn tarkoituksesta	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Mihin rekisteröityjen ryhmään henkilötietoja kerätään (esim. työntekijät ja heidän palkanmaksua varten)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Miten rekisteröity voi käyttää tarkastusoikeuttaan	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Mihin henkilötietoja säännönmukaisesti luovutetaan	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Siirretäänkö tietoja EU:n tai Euroopan talousalueen ulkopuolelle	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Henkilörekisterin suojauksen periaatteista	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

13. Onko organisaatiossanne ohjeet *

Henkilötietolaki §:t 26-30

	Kyllä	Ei	En tiedä
Siitä, kuinka rekisteröity voi tarkastaa omat tietonsa	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Siitä, kuinka virheellinen, tarpeeton, puutteellinen tai vanhentunut henkilötieto korjataan tai poistetaan	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Siitä, kuinka rekisteröidyllä on oikeus kieltää rekisterinpitäjää käsittelemästä häntä itseään koskevia tietoja suoramainontaa, etämyyntiä ja muuta suoramarkkinoita sekä markkina- ja mielipidetutkimusta samoin kuin henkilömatrikkelia ja sukututkimusta varten	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Rekisteriseloste

Rekisterinpitäjän on laadittava henkilörekisteristä rekisteriseloste, josta ilmenee rekisterinpitäjän ja tarvittaessa tämän edustajan nimi ja yhteystiedot, henkilötietojen käsittelyn tarkoitus, kuvaus rekisteröityjen ryhmästä tai ryhmistä ja näihin liittyvistä tiedoista tai tietoryhmistä, mihin tietoja säännönmukaisesti luovutetaan ja siirretäänkö

tietoja EU:n tai EU:n talousalueen ulkopuolelle sekä kuvaus rekisterin suojauksen periaatteista (Henkilötietolaki 10 §)

14. Arvioikaa missä määrin organisaatiossanne on tehty rekisteriselosteet henkilörekistereistä? *

Henkilötietolaki 10 §

- Kaikki tai lähes kaikki on tehty
- Noin puolet tai enemmän on tehty
- Selvästi alle puolet on tehty
- Ei ole tehty ollenkaan
- En tiedä

15. Onko rekistereille määritelty yhteyshenkilö? *

Henkilötietolaki 10 §

- Kyllä
- Ei
- En tiedä

16. Ovatko rekisteriselosteet rekisteröityjen saatavilla? *

Henkilötietolaki 10 §

- Ilmoitustaululla
- Internetissä
- Muualla, missä?
-

Tietosuojavastaava

Tietosuojavastaavan nimittämistä ei ole säädetty henkilötietolaissa. EU-tietosuoja-asetuksessa säädetään, että rekisterinpitäjän ja henkilötietojen käsittelijän on nimitettävä tietosuojavastaava. SOTE:ssa tietosuojavastaavia on, koska laissa sosiaali- ja terveydenhuollon sähköisestä käsittelystä 159/2007 ja laissa sähköisestä lääkemääräyksestä 61/2007 säädetään tietosuojavastaavan nimittämisestä.

17. Onko organisaatiossanne nimitetty tietosuojavastaava ja määritelty hänen tehtävänsä? (muu kuin sosiaali- ja terveydenhuollon tietosuojavastaava) *

- | | Kyllä | Ei | En tiedä |
|--|-----------------------|-----------------------|-----------------------|
| Tietosuojavastaava on nimitetty | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Tietosuojavastaavan tehtävät on määritelty | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

18. Jos vastasit edelliseen kysymykseen kyllä, niin voitko tarkentaa missä tai miten tietosuojavastaavan tehtävät on määritelty? (esim. tehtäväkuvaus, johtosäännöt, toimintasäännöt)

500 merkkiä jäljellä

Tietoturva ja riskienhallinta

Henkilötietolaki 32 §: Rekisterinpitäjän on toteutettava tekniset ja organisatoriset toimenpiteet henkilötietojen suojaamiseksi asiattomalta pääsylvä tietoihin ja vahingossa tai laittomasti tapahtuvalta tietojen hävittämiseltä, muuttamiselta, luovuttamiselta, siirtämiseltä taikka muulta laittomalta käsittelylvä.

19. Onko organisaatiollanne *

Henkilötietolaki 32 §

	Kyllä	Ei	En tiedä
Tietoturvaohjeet henkilötietojen käsittelyyn	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Käytössä tietotilinpäätös tai vastaava	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Riskianalyysi henkilötietojen käytöstä	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Nimitetty tietoturvapäällikkö tai vastaava	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Valmistautuminen EU-tietosuoja-asetukseen

20. Oletteko saanut tai hankkinut tietoa EU-tietosuoja-asetuksesta ja sen voimaantulosta? *

- Kyllä, voitteko lisäksi täsmentää mistä olette saaneet/hankkineet tietoja?

- Ei
- En tiedä

21. Tiedättekö, millaisia muutoksia EU-tietosuoja asetus aiheuttaa nykyisiin käytäntöihin? *

- Kyllä, voitteko täsmentää millaisia muutoksia?

- Ei
- En tiedä

22. Oletteko aloittaneet kehittämistoimet EU-tietosuoja-asetuksen vaatimusten täyttämiseksi? *

- Kyllä Ei En tiedä Kehittämistoimet ovat suunnitteilla

23. Oletteko tietoinen VM:n julkaisemasta Vahti-ohje 1/2016 koskien EU-tietosuojan kokonaisuudistusta? *

Löytyy osoitteesta: https://www.vahtiohje.fi/c/document_library/get_file?uuid=c97ee414-1fc0-4a91-969c-2ef0657605d1&groupId=10128

Kyllä Ei En tiedä

24. Oletteko te tai onko joku organisaatiostanne osallistunut EU-tietosuoja-koulutukseen? *

Kyllä
 Ei
 En tiedä

25. Mihin asioihin EU-tietosuoja-asetuksessa kaipaatte tukea tai koulutusta? (valitkaa 4 tärkeintä) *

- Käsitteisiin ja yleisiin periaatteisiin
- Henkilötietojen käsittelyohjeisiin
- Rekisterinpitäjän velvollisuuksiin
- Rekisteröidyn oikeuksiin
- Sopimukseen liittyviin muutoksiin
- Hankintoihin liittyviin muutoksiin
- Tietosuojavastaavan nimittämiseen ja tehtäviin
- Tietoturvaohjeistukseen ja riskianalyyysien tekemiseen
- Osoitusvelvollisuuteen
- Sisäänrakennettuun ja oletusarvoiseen tietosuojaan
- Yhteistyöhön tietosuojaviranomaisen kanssa
- Ennakkokuulemiseen
- Muuhun, mihin?

26. Haluatteko lausua vielä jotakin henkilötietojen käsittelyyn liittyen?

500 merkkiä jäljellä

LIITE 6. Kehittämissuosituksukset rekisterinpitäjille

Välitöntä kehittämistä vaativat asiat (uudet tai heikolla tasolla olevat)

Aloita kehittämistoimet

Selvitä uudet käsitteet ja selvitä tietosuoja-asetuksen soveltamisalue

Selvitä lainmukaisen käsittelyn periaatteet ja niiden hallinnolliset ja tekniset toimintatavat

Suunnittele henkilötietojen käyttö

Huolehdi rekisteröidyn oikeuksien turvaamisesta, huomioi uudet oikeudet ja tee ohjeistus henkilötietojen käsittelijöille

Nimitä tietosuojavastaava ja määrittele hänen tehtävänsä

Suostumusmenettely

Tee ohjeistus ulkopuolisille henkilötietojen käsittelijöille

Selvitä miten tietosuoja huomioidaan hankinnoissa

Ota käyttöön sisäänrakennettu ja oletusarvoinen tietosuoja prosesseissa ja tietojärjestelmissä

Huolehdi rekisteriselosteiden saatavuudesta (kirjallinen + sähköinen)

Huolehdi tietoturvasta ja tee riskianalyysi henkilötietojen käytöstä, käytä tietotilinpäätöstä, ja määrittele ilmoitusmenettely tietoturvaloukkauksista

Tee säännöt luovutuksille ja siirroille EU:n ja Euroopan talousalueen ulkopuolelle

Selvitä mahdollisia yhteisrekisterinpitoa, vakiosopimuslausekkeiden ja käytäntösääntöjen käyttöä sekä menettelyä sertifiointissa, vaikutustenarvioinnissa ja ennakkokuulemisissa

Kehittämistä tai päivittämistä vaativat asiat

Tee ohjeistus henkilötietojen ja tunnusten käsittelystä

Päivitä henkilötietojen käyttötarkoitus

Päivitä käyttöoikeudet

Huomioi erityiset henkilötietoryhmät

Päivitä sopimukset tietosuoja-asetusta vastaaviksi

Tee selosteet käsittelytoimista (rekisteriselosteet) ja päivitä rekisteriselosteiden yhteyshenkilöt

Nimitä tietoturvapäällikkö tai vastuuta tietoturvasta vastaava

Laadi tietoturvaohjeet

Päivitä asiakirjallisen tiedon säilyttämisen periaatteet ja huomiointi käytännössä

Osallistu koulutuksiin ja perehdy ohjeisiin