



LAUREA
AMMATTIKORKEAKOULU
Yhdessä enemmän

Tietosuojavastaava - organisaation asiantuntija tietosuoja-asioissa

Tiia Mansikka

2019 Laurea



Laurea-ammattikorkeakoulu

**Tietosuojavastaava - organisaation
asiantuntija tietosuoja-asioissa**

Tiia Mansikka
Liiketalous
Opinnäytetyö
Joulukuu, 2019

Tiia Mansikka

Tietosuojavastaava - organisaation asiantuntija tietosuoja-asioissa

Vuosi 2019 Sivumäärä 50

Opinnäytetyön tavoitteena oli tutkia tietosuoja-asetuksen tuomaa rekisterinpitäjän ja henkilötietojen käsittelijän velvollisuutta nimittää tietosuojavastaava ja ilmoittaa tietosuojavastaavan yhteystiedot valvontaviranomaiselle. Tarkoituksena oli myös tutkia tietosuojavastaavan rooleja suhteessa erilaisiin tahoihin sekä tutustua tietosuojavastaavan tehtäviin ja asemaan organisaatiossa.

Opinnäytetyön tutkimusmenetelmä oli lainopillinen eli oikeusdogmaattinen. Opinnäytetyön viitekehys muodostuu pääasiassa EU:n yleisestä tietosuoja-asetuksesta, WP 29-tietosuojatyöryhmän ohjeistuksesta sekä uuden tietosuojalainsäädännön mukaisesta kirjallisuudesta.

Opinnäytetyössä on toteutettu myös empiirinen tutkimus. Oma työkokemukseni tietosuojavaltuutetun toimistolla tietosuojavastaava-ilmoitusten käsittelijänä antaa käytännön kokemuksesta tietoa. Tuloksena syntyi kehittämissuhteita tietosuojavaltuutetun toimiston ilmoitusten käsittelyprosessiin. Ilmoitusten lukumäärästä voidaan myös päätellä, että kaikki organisaatiot, joita tietosuojavastaavan nimitysvelvollisuus koskee, eivät ole ilmoittaneet yhteystietoja tietosuojavaltuutetun toimistolle.

Asiasanat: tietosuoja-asetus, tietosuojavastaava, valvontaviranomainen, henkilötieto, rekisterinpitäjä

Tiia Mansikka

An expert of data protection in the organisation

Year	2019	Pages	50
------	------	-------	----

The purpose of this thesis was to study the requirement of the General Data Protection Regulation which obligates a controller and a processor to name a data protection officer and to inform the data protection officer's contact details to a supervisor authority. The aim was also to investigate the roles of a data protection officer between different organisations and to explore the tasks and position of a data protection officer in the organisation.

The research method of this thesis was juridical. The theoretical frame of reference was formed mainly from the common EU General Data Protection Regulation, Article 29 Working Party's guidance and literacy which is compatible with the new data protection law.

Empirical research has also been implemented in this study. My own personal work experience at the Office of the Data Protection Ombudsman as a processor for announcements of data protection officer gives knowledge from practice. As a result development suggestions came about involving the handling process of announcements at the Office of the Data Protection Ombudsman. It can also be assessed from the amount of announcements that not all organisations that are involved have informed the contact details to the Office of the Data Protection Ombudsman.

Keywords: General Data Protection Regulation, data protection officer, supervisory authority, personal data, controller

Lyhenteet ja käsitteet

EU - Euroopan unioni

GDPR - on lyhenne sanoista General Data Protection Regulation. Tarkoittaa EU:n yleistä tietosuojaa-asetusta.

Henkilötieto - tunnistettuun tai tunnistettavaan luonnolliseen henkilöön liittyvät tiedot.

Henkilötietojen käsittely - toimenpiteet, jotka kohdistuvat henkilötietoihin joko automaattista tietojen käsittelyä hyödyntäen tai manuaalisesti.

Henkilötietojen käsittelijä - rekisterinpitäjältä ulkopuolinen organisaatio tai ihminen, joka käsittelee henkilötietoja rekisterinpitäjän lukuun tämän ohjeiden mukaisesti.

Konserni - yritys, joka käyttää määräysvaltaa ja sen määräysvallan alla olevia yrityksiä.

Rekisterinpitäjä - organisaatio tai ihminen, joka määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot.

Rekisteröity - luonnollinen henkilö, jota henkilötieto koskee.

Tietosuoja - perusoikeus henkilötietojen käsittelyssä, jolla turvataan rekisteröidyn oikeuksien ja vapauksien toteutuminen.

Tietosuojavaltuutettu - kansallinen valvontaviranomainen, joka valvoo tietosuojalainsäädännön noudattamista.

Tietosuojavastaava - tietosuoja-asetuksen määrittämä asiantuntija, joka seuraa henkilötietojen käsittelyä ja tietosuojasäännösten noudattamista organisaatiossa.

TATTI-työryhmä - oikeusministeriön asettama EU:n yleisen tietosuoja-asetuksen täytäntöönpanotyöryhmä.

Tietosuojatyöryhmä WP 29 - EU:n jäsenvaltioiden tietosuojaviranomaisista koostuva itsenäinen, neuvoa-antava elin.

Vaikutuksenarviointi - menettely, jossa arvioidaan suunniteltujen käsittelytoimien vaikutuksia henkilötietojen suojaan.

Sisällys

1	Johdanto	7
2	Tutkimusmetodi ja oikeuslähdeoppi	7
3	Euroopan unioni ja EU-oikeus	9
3.1	EU:n toimielimet	9
3.2	EU-säädökset.....	10
4	Uusi tietosuojalainsäädäntö	11
4.1	EU:n yleinen tietosuoja-asetus	12
4.2	Tietosuojalaki	14
5	Tietosuojavaltuutetun toimisto	15
6	Tietosuojavastaavan nimittäminen.....	16
7	Organisaation tietosuojavastaava	18
7.1	Tietosuojavastaavan asema	19
7.2	Tietosuojavastaavan tehtävät	20
7.3	Resurssit	20
8	Tietosuojavastaavana toimiminen.....	22
8.1	Tietosuojavastaava ja johto	23
8.2	Tietosuojavastaava ja henkilöstö	24
8.3	Tietosuojavastaava ja valvontaviranomainen.....	25
8.4	Tietosuojavastaava ja rekisteröidyt	26
9	Tietosuojavastaavien yhteystiedot tietosuojavaltuutetun toimistolla	27
9.1	Ilmoitusten käsittely tietosuojavaltuutetun toimistolla	28
9.2	Tilastoja tietosuojavastaava-ilmoituksista	29
9.3	Huomiot ja korjausehdotukset	31
	Kuviot	37
	Taulukot	37
	Liitteet.....	38

1 Johdanto

Euroopan parlamentin ja neuvoston asetus (2016/679) luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus) on nykyisin henkilötietojen käsittelyn perusta. Kyseinen asetus astui voimaan 25.5.2016 kaikissa EU:n 28 jäsenmaassa ja kahden vuoden siirtymäajan jälkeen sitä alettiin soveltaa 25.5.2018. Monet ihmiset tuntevat sen GDPR:nä, joka on lyhenne englanninkielisistä sanoista General Data Protection Regulation. Yleinen tietosuoja-asetus on suoraan sovellettavaa lainsäädäntöä, jota täydennetään lisäksi kansallisella tietosuojalaille (1050/2018). Tietosuojalaki astui voimaan 1.1.2019. Yleisen tietosuoja-asetuksen tavoitteena on yhdenmukaistaa tietosuojalainsäädäntö Euroopan unionissa ja täten helpottaa myös palvelujen tarjoamista ulkomaille.¹ EU:n yleinen tietosuoja-asetus ja kansallinen tietosuojalaki ovat vielä niin tuoretta lainsäädäntöä, että ajantasaista oikeuskirjallisuutta on vielä hyvin vähän saatavilla.

Opinnäytetyössä perehdytään ensiksi käytettyyn tutkimusmetodiin eli lainoppiin sekä avataan oikeuslähteiden merkitystä oikeuden tulkinnassa. Työssä perehdytään myös EU:n lainsäätämisen prosessissa mukana oleviin toimielimiin sekä erilaisiin EU:n säädöksiin, sillä keskeisessä asemassa työssä on EU:n yleinen tietosuoja-asetus. Opinnäytetyö kertoo yleisen tietosuoja-asetuksen tuomasta tietosuojavastaavan nimitysvastuusta. Työssä perehdytään tietosuojavastaavan asemaan ja tehtäviin organisaatiossa. Lisäksi mietitään tietosuojavastaavan roolia suhteessa valvontaviranomaiseen, rekisteröityihin sekä oman organisaation henkilöstöön ja johtoon. Tietosuojavastaavien yhteystiedot tulee ilmoittaa kansalliselle valvontaviranomaiselle, joka Suomessa on tietosuojavaltuutettu. Työssä mietitään miten tietosuojavastaava-ilmoitusten käsittelyprosessia voitaisiin kehittää sekä millaisia päätelmiä saapuneiden ilmoitusten lukumäärästä voidaan tehdä.

2 Tutkimusmetodi ja oikeuslähdeoppi

Opinnäytetyössä käytettiin tutkimusmetodinä lainoppia eli oikeusdogmatiikkaa. Lainopillisessa tutkimuksessa tarkoitus on selvittää oikeuslähteiden perusteella voimassa olevaa oikeutta eli miten lakia tulkitaan.² Oikeudellisen ratkaisun tulisi aina perustua oikeuslähteisiin. Tehdyn

¹ EU:n yleinen tietosuoja-asetus & ks. Hanninen, Laine, Rantala, Rusi & Varhela 2017, 13.

² Nykänen 2013, 50.

kannanoton tai ratkaisun vahvuus sekä hyväksyttävyyys ovat riippuvaisia siitä, mihin oikeuslähteeseen kannanotto tai ratkaisu perustuu. Oikeuslähteet voidaan jakaa niiden velvoittavuusasteen mukaan vahvasti velvoittaviin, heikosti velvoittaviin sekä sallittuihin oikeuslähteisiin. Vahvasti velvoittavia oikeuslähteitä ovat lait ja maan tapa, heikosti velvoittaviin oikeuslähteisiin kuuluvat lainvalmisteluaineistot sekä oikeuskäytäntö. Oikeuskirjallisuus sekä reaaliset argumentit luetaan sallittuihin oikeuslähteisiin, jotka ovat oikeuslähteiden välisessä hierarkiassa heikoimmassa asemassa. Jaottelu edellä mainittuihin kategorioihin perustuu siihen, mitä seuraamuksia esimerkiksi tuomarille voi seurata, jos hän ei huomioi oikeuslähteitä ratkaisua tehdessään.³ Tuomarin syrjäyttäessä vahvasti velvoittavan oikeuslähteen, on kyseessä tuomarin tekemä virkavirhe ja täten hänen tekemänsä ratkaisu ei ole laillinen. Heikosti velvoittavan oikeuslähteen syrjäyttämisestä ei seuraa tuomarille sanktiota, mutta ratkaisu useimmiten tulee kuitenkin muuttumaan ylemmässä oikeusasteessa. Sallitun oikeuslähteen tarkoituksena on tukea tehtyä ratkaisua tai tulkintaa.⁴ Tässä työssä on käytetty vahvasti velvoittavia oikeuslähteitä, kuten EU:n yleistä tietosuoja-asetusta sekä kansallista tietosuojalakia. Heikosti velvoittavia oikeuslähteitä työssä ovat muun muassa TATTI-työryhmän mietintö. Työssä käytetty oikeuskirjallisuus luetaan puolestaan sallittuihin oikeuslähteisiin.

Lain tulkinnassa eteen saattaa tulla tilanne, jossa lait ovat ristiriidassa keskenään. Tällöin asia ratkaistaan normihierarkian mukaan. Suomessa perustuslaki on hierarkiassa ylimpänä. Perustuslain alapuolella seuraavana ovat tavalliset lait ja niiden jälkeen lakien perusteella annetut asetukset ja päätökset. Ristiriitatilanteessa hierarkiassa ylempänä oleva syrjäyttää alempana olevan säädöksen. Tämä tunnetaan ”lex superior derogat legi inferiori -sääntönä”.⁵

Ristiriita syntyy myös silloin kun tapaukseen sovelletaan yleissäännöstä sekä erityissäännöstä. Kaikkiin tunnusmerkit täyttäviin tapauksiin sovelletaan aina yleissäännöstä, mutta jos on olemassa tapaukseen soveltuva erityissäännös, syrjäyttää tämä ristiriidassa olevan yleissäännöksen. Tämä tunnetaan oikeustieteessä ”lex specialis derogat legi generali -sääntönä”. Käytännössä tapaukseen sovelletaan yleislakia, mutta tapaukseen soveltuvat erityislaista tulevat säädökset syrjäyttävät ristiriitatilanteissa yleislain. Yleissäännös sekä erityissäännös saattavat olla kirjoitettu myös samaan lakiin.⁶ Esimerkiksi tietosuojalaki on yleislaki, joka täsmentää ja täydentää yleistä tietosuoja-asetusta. Tietosuoja-asetusta puolestaan sovelletaan lähtökohteisesti kaikenlaiseen henkilötietojen käsittelyyn. Henkilötietojen käsittelyyn liittyvää erityis-

³ Nykänen 2013, 66-67.

⁴ Aarnio 2011, 69-70.

⁵ Nykänen 2013, 73.

⁶ Nykänen 2013, 75.

lainsäädäntöä ovat esimerkiksi laki sähköisen viestinnän palveluista (917/2014), luottotietolaki (527/2007) sekä laki yksityisyyden suojasta työelämässä (759/2014), joka tunnetaan työelämän tietosuojalakina.⁷

Ristiriitatilanne syntyy myös silloin kun kaksi samantasoista eri aikaan säädettyä lakia ovat ristiriidassa keskenään. Tällöin tapauksessa noudatetaan ”lex posterior derogat legi priori -sääntöä”, joka tarkoittaa, että uudempi säännös syrjäyttää aiemman säännöksen ristiriitatilanteessa.⁸

3 Euroopan unioni ja EU-oikeus

Euroopan unioni on taloudellinen ja poliittinen liitto, johon kuuluu 28 jäsenmaata. Jäsenmaat kattavat merkittävän osan Euroopan maanosasta. Euroopan unionin tarkoitus on muuan muassa edistää kansalaisten hyvinvointia, tieteellistä ja teknistä kehitystä, vapaata liikkuvuutta sekä jäsenvaltioiden välistä yhteisvastuuta. Lisäksi EU pyrkii torjumaan syrjäytymistä, kunnioittamaan kulttuurien moninaisuutta ja toteuttamaan kestävästä kehitystä. Monien EU:n jäsenmaiden väliltä onkin poistettu rajatarkastukset ja kansalaiset voivat liikkua vapaasti lähes kaikissa EU-maissa. Euroopan unioni pyrkii pitämään hallinnon ja toimielinten toiminnan avoimena ja demokraattisena. Päätökset pyritään tekemään mahdollisimman lähellä kansalaisia.⁹

3.1 EU:n toimielimet

Euroopan unionin toimielimiin kuuluvat Euroopan parlamentti, Eurooppa-neuvosto, neuvosto, Euroopan komissio, Euroopan unionin tuomioistuin, Euroopan keskuspankki sekä tilintarkastustuomioistuin. Euroopan unionin lainsäädäntöprosessissa avainasemassa ovat komissio, parlamentti sekä neuvosto. Lainsäädäntöaloitteet tulevat useimmiten komissiolta, parlamentti ja neuvosto ovat tasavertaisia lainsäädäntövallankäyttäjiä.¹⁰ Avataan seuraavaksi hiukan näiden lainsäädäntöprosessiin kuuluvien toimielinten kokoonpanoa ja toimintaa.

Euroopan parlamentti koostuu 751 jäsenestä, jonka tehtävä on edustaa kansalaisia EU:n toimielin- ja päätöksentekojärjestelmässä. Jäsenet parlamenttiin valitaan viiden vuoden välein

⁷ Tietosuojavaltuutetun toimisto. Lainsäädäntöä.

⁸ Nykänen 2013, 76.

⁹ Euroopan unioni. Perustietoa Euroopan unionista.

¹⁰ Ojanen 2016, 25.

suorilla vaaleilla. Viimeisimmät parlamenttivaalit olivat tänä vuonna eli 2019 ja Suomesta sinne valittiin 13 jäsentä. Parlamentti toimii poliittisten näkemystensä mukaan samalla periaatteella kun Suomen eduskunta. Tämä tarkoittaa sitä, että parlamenttiin valitut kansalaiset edustavat poliittisia näkemyksiään, eivät omaa kansalaisuuttaan. Parlamentilla on säädös- ja budjettivaltaa ja parlamentti on vastuussa komission poliittisesta valvonnasta. Lisäksi sen tehtäviin kuuluu nimittää Euroopan oikeusasiamies.¹¹

Neuvosto, joka tunnetaan myös ministeriöneuvostona, koostuu jäsenvaltioiden ministereistä. Ministeri edustaa jäsenmaansa näkemyksiä EU:n toimielin- ja päätöksentekuelimessä. Neuvoston kokouksiin osallistuu aina yksi ministeri jokaisesta jäsenmaasta. Neuvostolla on kymmenen eri kokoonpanoa ja jäsenvaltiota edustava ministeri määräytyy aina käsiteltävän asian mukaan. Neuvosto ja parlamentti ovat tasavertaisia lainsäätäjiä kun kysymyksessä on tavallinen lainsäätämisyjärjestys. EU-säädöksiä hyväksytään määräenemmistöllä; mitä suurempi jäsenmaan väkiluku on, sitä enemmän edustajalla on ääniä käytettävissään. Neuvostolla on myös puheenjohtaja. Puheenjohtajuus kestää puoli vuotta kerrallaan ja se kiertää jäsenmaiden välillä ennakkoon sovitulla tavalla. Suomen vuoro olla puheenjohtajamaana on vuonna 2020.¹²

Komissio on puolestaan riippumaton elin, joka koostuu jäsenmaiden komissaareista. Kustakin jäsenvaltiosta valitaan yksi edustaja viideksi vuodeksi kerrallaan. Komissaarin tehtävä ei ole edustaa jäsenmaata eikä ottaa ohjeita hallitukselta, vaan se toimii riippumattomassa asemassa. Komissiota sanotaan EU:n ”moottoriksi” ja siellä työskentelee yhteensä n. 38 000 toimihenkilöä. Komissiolla on vahva asema lainsäädäntöaloitteiden tekijänä, mutta se toimii myös EU:n edustajana suhteessa kolmansiiin maihin sekä muihin kansainvälisiin järjestöihin sekä johtaa kansainvälisiä neuvotteluita.¹³

3.2 EU-säädökset

Euroopan unionista tehdyn sopimuksen ja Euroopan unionin toiminnasta tehdyn sopimuksen konsolidoidut toisinnot (2016/C 202/01) 288 artiklan mukaan toimielimet hyväksyvät asetuksia, direktiivejä ja päätöksiä. Asetus on velvoittava ja sitä sovelletaan suoraan sellaisenaan kaikissa EU:n jäsenmaissa. Direktiivi puolestaan jättää jäsenvaltioiden viranomaisille valittavaksi muodot ja keinot, joilla se toteuttaa direktiivin tuomat vaatimukset. Päätös on kaikilta

¹¹ Euroopan unioni. Euroopan parlamentti & ks. Ojanen 2016, 26-27.

¹² Euroopan unioni. Euroopan unionin neuvosto & ks. Ojanen 2016, 28.

¹³ Euroopan unioni. Euroopan komissio & ks. Ojanen 2016, 30.

osin velvoittava. Jos päätöksessä on nimetty kenelle se on osoitettu, velvoittaa päätös vain niitä tahoja. Lausunnot ja suositukset eivät ole sitovia.¹⁴

Asetuksen velvoittavuus saattaa koskea niin EU:n toimielimiä, jäsenvaltioita kuin myös luonnollisia henkilöitä ja muita oikeushenkilöitä. Asetuksen erityispiirre on se, että sitä sovelletaan kaikissa EU:n jäsenvaltioissa sellaisenaan. EU:n tuomioistuin on katsonut, että kansallista lainsäädäntöä ei saa antaa asetuksen soveltamisalalla ellei siitä ole erikseen asetuksessa säädetty. Tämän tarkoitus on suojata asetuksen kykyä tulla sellaisenaan voimassaolevaksi oikeudeksi jokaisessa jäsenmaassa. Asetusten tarkoituksena on yleensä yhtenäistää jäsenvaltioiden lainsäädäntöä.¹⁵ Opinnäytetyössä keskeisessä roolissa on EU:n yleinen tietosuojasetus.

Direktiivit ovat myös oikeudellisesti sitovia, mutta ne velvoittavat suoraan välittömästi vain jäsenmaita. Siinäkin velvoitettavuus tulee vaan saavutettavasta tuloksesta. Direktiivissä asetetaan aina määräaika, milloin se tulee olla implementoitu jäsenmaassa eli määräpäivä direktiivin täytäntöönpanolle. Eduskuntavaalit sekä valtioneuvoston tai ministeriön asetukset ovat yleisimmät tavat Suomessa panna direktiivit täytäntöön. Myös yleissitova työehtosopimus on hyväksytty implementointikeino. Direktiiviä ei tarvitse erikseen panna täytäntöön, jos valtion kansallinen lainsäädäntö täyttää jo direktiivin tuomat vaatimukset. Direktiivin tarkoitus on yleensä yhdenmukaistaa kansallisia lainsäädäntöjä.¹⁶

Päätös velvoittaa niitä, joille se on osoitettu. Päätökset voidaan osoittaa esimerkiksi yritykselle, jäsenvaltiolle tai EU-toimielimelle. Asetukseen ja direktiiviin verrattuna päätös on paljon yksityiskohtaisempi ja täsmällisempi sisällöltään. Päätöksellä voi olla myös välitön oikeusvaikutus. Se voi vaikuttaa esimerkiksi jäsenmaan kansallisen oikeuden tulkintaan ja päätöksen rikkominen voi tuoda mukanaan vahingonkorvausvastuun.¹⁷

4 Uusi tietosuojalainsäädäntö

Vuonna 2012 huomattiin, että EU:n tietosuojalainsäädäntö ei vastannut enää globaalin tietoympäristön tuomiin vaatimuksiin vaan oli jäljessä kehityksestä. Tietosuojalainsäädännön uudistamisen tarkoitus on pyrkiä turvaamaan henkilötietojen suoja perusoikeutena, kehittämään digitaalitaloutta ja tehostamaan torjuntaa rikollisuutta ja terrorismia vastaan. Uudistuksen

¹⁴ Ks. Ojanen 2016, 43-47.

¹⁵ Ojanen 2016, 43-44.

¹⁶ Ojanen 2016, 45-47.

¹⁷ Ojanen 2016, 47.

vuoksi Euroopan unionin tietosuojalainsäädännön pohjaksi muodostuivat Euroopan parlamentin ja neuvoston direktiivi (2016/680) luonnollisten henkilöiden suojelusta toimivaltaisten viranomaisten suorittamassa henkilötietojen käsittelyssä rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten sekä näiden tietojen vapaasta liikkuvuudesta ja neuvoston puitepäättöksen 2008/977/YOS kumoamisesta (rikosasioiden tietosuojadirektiivi) ja jo aiemmin mainittu EU:n yleinen tietosuoja-asetus. Vanha lainsäädäntö sai väistyä uuden tieltä. Täten vuoden 1995 annettu Euroopan parlamentin ja neuvoston direktiivi 95/46/EY yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta korvattiin yleisellä tietosuoja-asetuksella ja uusi rikosasioiden tietosuojadirektiivi puolestaan korvasi vuoden 2008 puitepäättöksen (2008/977/YOS) rikosasioissa tehtävissä sekä poliisi- ja oikeudellisessa yhteistyössä käsiteltävien henkilötietojen suojaamisesta. Tässä työssä keskitytään yleisen tietosuoja-asetuksen tuomiin oikeuksiin ja velvollisuuksiin ja rikosasioiden direktiivi on rajattu työn ulkopuolelle. Yleinen tietosuoja-asetus koskee lähtökohtaisesti kaikenlaista henkilötietojen käsittelyä pitäen sisällään säännökset rekisterinpitäjän ja henkilötietojen käsittelijän velvollisuuksista sekä rekisteröidyn oikeuksista.¹⁸ Se toi mukanaan rekisteröidyille enemmän oikeuksia, rekisterinpitäjälle uusia velvollisuuksia, viranomaisille laajemmat valtuudet sekä vahvan ja yhtenäisen tietosuojakehyksen koko Euroopan unionille.¹⁹ Yleistä tietosuoja-asetusta on sovellettu jo noin puolitoista vuotta, mutta silti se saattaa olla tuntematon monille organisaatioille.²⁰

4.1 EU:n yleinen tietosuoja-asetus

Ajatus tietosuojalainsäädännön muutoksesta alkoi vuonna 2012 maaliskuussa kun Euroopan komissio ehdotti EU:n oikeudellisen kehyksen uudistamista koskien henkilötietosuojaa. Tämän jälkeen asiasta alettiin keskustelemaan vilkkaasti. Vuoden 2013 lokakuussa Euroopan parlamentin kansalaisvapauksien sekä oikeus- ja sisäasioiden valiokunta eli LIBE-valiokunta äänesti mietinnöissään tietosuoja-asetuksen puolesta, myös Euroopan parlamentti kannatti asetusta vuoden 2014 maaliskuussa ja hyväksyi LIBE-valiokunnan mietinnön. Käsittely siirtyi ministerineuvostoon eli Euroopan unionin neuvostoon, mutta siellä tietosuoja-asetusta ei hyväksytty sellaisenaan. Tämän vuoksi tietosuoja-asetuksen käsittely siirrettiin kolmikantaneuvotteluihin kesäkuussa 2015. Kolmikantaneuvotteluihin osallistuvat Euroopan parlamentti, komissio sekä

¹⁸ EU:n yleinen tietosuoja-asetus & ks. Eduskunta. EU:n tietosuojauudistuksen kansallinen täytäntöönpano.

¹⁹ EU:n yleinen tietosuoja-asetus & ks. Opitietosuoja.fi

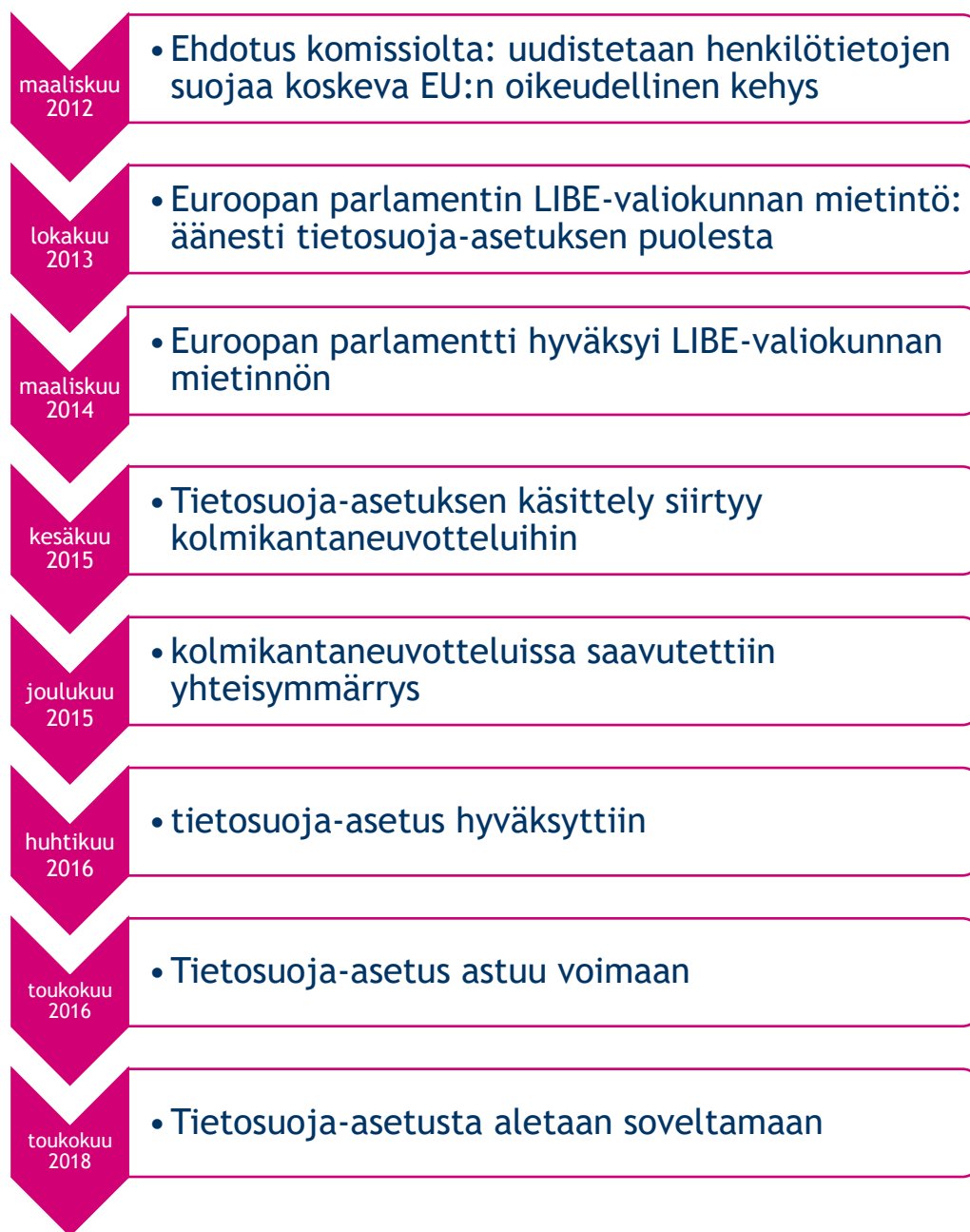
²⁰ Lakimiesuutiset. GDPR on edelleen monelle vieras.

ministeriöneuvosto ja niiden tarkoitus oli löytää kompromissi tietosuoja-asetuksen sisällöstä.²¹ Joulukuussa 2015 kolmikantaneuvotteluissa saavutettiin yhteisymmärrys.²² Yleisen tietosuoja-asetuksen 99 artiklassa määritellään asetuksen voimaantulo ja soveltaminen, jonka mukaan tietosuoja-asetus hyväksyttiin keväällä 2016 ja se astui voimaan 25.5.2016 eli kahdente-nakymmenentenä päivänä siitä, kun se julkaistiin Euroopan unionin virallisessa lehdessä. Kahden vuoden siirtymäajan jälkeen sitä alettiin soveltamaan 25.5.2018 kaikissa EU:n jäsenmaissa.²³ Kuviossa 1 on havainnollistettu EU:n yleisen tietosuoja-asetuksen valmisteluaikataulua.

²¹ Andreasson, Koivisto & Ylipartanen 2015, 30-31.

²² Euroopan unionin neuvosto, Toimielinten välinen asia: 2012/0011 (COD), 2.

²³ Ks. Korpisaari 2018, 645.



Kuvio 1: Tietosuoja-asetuksen valmistelu

4.2 Tietosuojalaki

Tietosuoja-asetusta piti täydentää kansallisella lainsäädännöllä, joten oikeusministeriö asetti vuoden 2016 helmikuussa TATTI-työryhmän, jonka pääasiallisena tehtävänä oli valmistella lainsäädäntöehdotus tietosuoja-asetuksen antaman liikkumavaran täydentämiseksi. TATTI-työryhmä ehdottikin, että henkilötietolaki (523/1999) kumotaan ja säädetään uusi henkilötie-

tojen suojaa koskeva tietosuojalaki, joka toimii yleislakina täsmentäen ja täydentäen tietosuojasetusta. TATTI-työryhmä valmisteli myös ehdotuksen kansallisesta valvontaviranomaisesta. Tietosuojalain oli tarkoitus astua voimaan samaan aikaan kun tietosuojasetusta alettiin soveltamaan.²⁴ TATTI-työryhmän lopetettua 16.2.2018 valmistelutyön, asia siirtyi eduskunnan käsittelyyn. Hallituksen esitys (HE 9/2018) eduskunnalle EU:n yleistä tietosuojasetusta täydentäväksi lainsäädännöksi vastaanotettiin eduskunnassa 1.3.2018. Tämän jälkeen asiaa käsiteltiin useassa valiokunnassa ja siitä pyydettiin useita lausuntoja. Eduskunnassa lakiehdotusta käsiteltiin eduskuntakäsittelyssä 6.11.2018 ja 3.11.2018. Jälkimmäisessä eduskuntakäsittelyssä tietosuojalaki hyväksyttiin ja se astui voimaan 1.1.2019.²⁵ Tietosuojain 37 §:n mukaan tietosuojalailla kumottiin henkilötietolaki ja laki tietosuojalautakunnasta ja tietosuojavaltuutetusta (389/1994).

5 Tietosuojavaltuutetun toimisto

Tietosuojalain 8 §:n mukaan tietosuojasetuksen mukaisena kansallisena valvontaviranomaisena toimii oikeusministeriön yhteydessä tietosuojavaltuutettu. Tietosuojalain 9 §:n mukaan tietosuojavaltuutetun toimistossa tulee olla lisäksi vähintään kaksi apulaistietosuojavaltuutettua. Tietosuojavaltuutetun toimistossa on lisäksi esittelijöitä ja muuta henkilöstöä. Tietosuojalain 10 §:ssä määritellään tietosuojavaltuutetun ja apulaistietosuojavaltuutettujen kelpoisuusvaatimukset sekä nimitysperusteet, jonka mukaan tietosuojavaltuutetun ja apulaistietosuojavaltuutettujen kelpoisuusvaatimuksena pidetään oikeustieteen ylempää korkeakoulututkintoa, joka on muu kuin kansainvälisen ja vertailevan oikeustieteen maisterin tutkinto. Lisäksi vaatimuksena tietosuojavaltuutetun tai apulaistietosuojavaltuutetun virkaan on, että henkilö on perehtynyt henkilötietojen suojaa koskeviin asioihin ja osoittanut käytännön johtamistaitoa. Lisäksi henkilöllä tulee olla kyky hoitaa kansainvälisiä tehtäviä.

Tietosuojavaltuutetun toimisto aloitti toimintansa vuonna 1988 kun jo kumottu henkilörekisterilaki (471/1987) astui voimaan.²⁶ Tietosuojavaltuutettuna on toiminut Reijo Aarnio vuodesta 1997. Valtioneuvosto on nimittänyt apulaistietosuojavaltuutetuiksi Jari Råmanin ja Anu Taluksen 1.5.2019 lähtien. Tietosuojavaltuutetun ja apulaistietosuojavaltuutettujen toimikausi on viisi vuotta. Toimistossa työskentelee noin 40 henkilöä tietosuojavaltuutetun ja apulaistietosuojavaltuutettujen lisäksi.²⁷

²⁴ EU:n yleisen tietosuojasetuksen täytäntöönpanoryhmän (TATTI) mietintö, 13.

²⁵ Eduskunta. EU:n yleisen tietosuojasetuksen (GDPR) täytäntöönpano - Uusi tietosuojalaki.

²⁶ Andreasson ym. 2014, 46-47.

²⁷ Tietosuojavaltuutetun toimisto.

Tietosuojavaltuutetun tehtävät on määritelty tietosuojasetuksen 58 artiklassa. Valvontaviranomaiselle on annettu erilaisia tutkintavaltuuksia, korjaavia toimivaltuuksia sekä hyväksymis- ja neuvontavaltuuksia. Yleisesti keskustelua on aiheuttanut erityisesti tietosuojasetuksen tuoma sakotus mahdollisuus, jolloin tietyin edellytyksin voidaan määrätä rekisterinpitäjälle tai henkilötietojen käsittelijälle hallinnollinen sakko. Lisäksi kansallisessa lainsäädännössä eli tietosuojalain 14 §:ssä on säädetty tietosuojavaltuutetun tehtävistä ja toimivaltuuksista: tietosuojavaltuutettu ei valvo eduskunnan oikeusasiamiehen tai valtioneuvoston oikeuskanslerin toimintaa. Sen mukaan Euroopan tietosuojaneuvoston edustajana toimii Suomesta tietosuojavaltuutettu. Tietosuojavaltuutetun tehtäviin kuuluu myös akkreditoita tietosuojasetuksen mukainen sertifiointielin sekä laatia vuosittainen toimintakertomus.

6 Tietosuojavastaavan nimittäminen

Tietosuojasetuksen 37 artiklassa määritellään, missä tapauksissa rekisterinpitäjän ja henkilötietojen käsittelijän tulee nimittää tietosuojavastaava. Kyseisen artiklan 1 kohdan a alakohdan mukaan tietosuojavastaava tulee nimittää jos tietojenkäsittelyä suorittaa viranomainen tai julkishallinnon elin pois lukien tuomioistuin, joka hoitaa lainkäyttötehtäviään. Hallintolain (434/2003) 2 §:n mukaan viranomaisella tarkoitetaan valtion viranomaisia, kunnallisia viranomaisia, itsenäisiä julkisoikeudellisia laitoksia sekä eduskunnan virastoja ja tasavallan presidentin kansliaa. Lisäksi esimerkiksi hallituksen esityksessä (9/2018) eduskunnalle yliopiston katsotaan olevan julkisoikeudellinen laitos, jolloin sen katsotaan myös olevan velvollinen nimittämään tietosuojavastaava.²⁸

Tietosuojasetuksen 37 artiklan 1 kohdan b alakohdan mukaan organisaatiossa tulee olla tietosuojavastaava jos organisaation ydintehtävät muodostuvat sellaisista käsittelytoimista, jotka luonteensa, laajuutensa tai/ja tarkoituksensa vuoksi edellyttävät laajamittaista rekisteröityjen seuranta säännöllisesti tai järjestelmällisesti. Laajamittaiselle käsittelylle ei ole määritelmää tietosuojasetuksessa, mutta arvioitaessa laajamittaisuutta tulisi huomioida mm. rekisteröityjen lukumäärä, käsiteltävä tietomäärä, käsittelytoiminnan kesto ja pysyvyys sekä sen maantieteellinen laajuus. Laajamittaista käsittelyä katsotaan olevan esimerkiksi potilastietojen käsittely sairaalassa, asiakastietojen käsittely pankissa sekä puhelinalvelujen tarjoajien suorittama tietojenkäsittely.²⁹ Tietosuojasetuksessa ei myöskään ole määritelmää

²⁸ HE 9/2018, 56.

²⁹ WP 243, 8.

säännölliselle tai järjestelmälliselle seurannalle, mutta kuitenkin sen johdanto-osassa puhutaan rekisteröityjen verkkokäyttäytymisen seurannasta. Tällaisella seurannalla voitaisiin tarkoittaa esimerkiksi profilointia.³⁰ Tietosuojaryhmä WP 29:n mukaan säännöllisyydellä tarkoitetaan muun muassa toimintaa, joka jatkuu, toistuu tai on jatkuvaa. Järjestelmällisellä puolestaan tarkoitetaan toimintaa, joka on esimerkiksi järjestelmän mukaista tai se toteutetaan osana tiedonkeruusuunnitelmaa tai strategiaa. Konkreettisesti järjestelmällisellä ja säännöllisellä rekisteröityjen seurannalla voidaan tarkoittaa esimerkiksi tietoliikenneverkon ylläpitoa, sijainnin seuraamista mobiilisovelluksella, videovalvontaa tai kanta-asiakasohjelmia.³¹

Tietosuoja-asetuksen 37 artiklan 1 kohdan c alakohdan mukaan tietosuojavastaava tulee nimittää jos organisaation ydintehtävät muodostuvat laajamittaisesta käsittelystä, joka kohdistuu erityisiin henkilötietoryhmiin ja rikostuomioita tai rikkomuksia koskeviin tietoihin. Tietosuoja-asetuksen 9 artiklan mukaan erityisillä henkilötietoryhmillä tarkoitetaan henkilötietojen käsittelyä, josta ilmenee esimerkiksi rotu tai etninen alkuperä, poliittisia mielipiteitä, uskonnollinen tai filosofinen vakaumus. Myös henkilön kuuluminen ammattiliittoon, hänen terveyttään koskevat tiedot tai seksuaalista käyttäytymistä sekä suuntautumista koskevat tiedot ovat erityisiä henkilötietoja. Myös geneettisten ja biometristen tietojen käsittely henkilön tunnistamista varten on pääsääntöisesti kiellettyä. Edellä mainitut henkilötiedot voivat loukata henkilön yksityisyyttä. Henkilötietolaissa käytettiin tällaisista tiedoista nimitystä arkaluonteinen henkilötieto, kun taas yleisessä tietosuoja-asetuksessa puhutaan erityisiin henkilötietoryhmiin kuuluvista tiedoista.³²

Tietosuojavastaava voidaan nimittää organisaatioon myös vapaaehtoisesti. Vapaaehtoisesti nimitettyä tietosuojavastaavaa koskevat kuitenkin samat säännökset kuin tietosuoja-asetuksen perusteella nimitettyyn tietosuojavastaavaan.³³ Tietosuoja-asetuksen kanssa samaan aikaan tullessa rikosasioiden tietosuojadirektiivissä 32 artiklassa säädetään tietosuojavastavan nimittämisestä melko saman lailla kuin tietosuoja-asetuksessa. Kansallinen erityislainsäädäntö saattaa velvoittaa myös tietosuojavastavan nimitykselle, esimerkiksi Suomessa on ollut jo pitkään velvollisuus nimittää terveydenhuollossa tietosuojavastaava. Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä 20 § ja laki sähköisestä lääkemääräyksestä 24 § määrittelevät, että tietosuojavastaava tulee olla nimettynä terveyden- ja sosiaalihuollon toimintayksiköihin, apteekkeihin sekä Kansaneläkelaitokseen seuranta- ja valvonta-tehtäviä varten.

³⁰ Tietosuoja-asetus & ks. Warmo-Lehtinen 2018, 353.

³¹ WP 243, 10.

³² Korpisaari 2018, 148-149.

³³ Warmo-Lehtinen 2018, 347.

Jos rekisterinpitäjä tai henkilötietojen käsittelijä haluaa nimittää vapaaehtoisesti tietosuoja-vastaavan, mutta ei halua kuitenkaan noudattaa sen tuomia tietosuoja-asetuksen mukaisia velvoitteita, tulisi tietosuojavastaavan nimike olla jokin muu kuin tietosuojavastaava. Tällöin ihmisille ei tule epäselvyyttä siitä, että kyseessä olisi yleisen tietosuoja-asetuksen mukainen tietosuojavastaava. Rekisterinpitäjä tai henkilötietojen käsittelijä saattaa olla myös epävarma siitä, tuleeko sen nimittää tietosuojavastaava. Tällaisessa tapauksessa rekisterinpitäjän tai henkilötietojen käsittelijän tulisi tehdä kirjallinen arvio asiasta. Tämä arvio on osa organisaation osoitusvelvollisuutta, jolla voidaan näyttää toteen, että tietosuoja-asetusta noudatetaan.³⁴

Tietosuoja-asetuksen 37 artiklan 2 kohdan mukaan konserni voi halutessaan nimittää vain yhden tietosuojavastaavan. Tällaisessa tapauksessa kuitenkin tulee olla mahdollista saada yhteys tietosuojavastaavaan mistä tahansa toimipaikasta. Myös viranomainen tai julkishallinnon elin voi nimittää yhden tietosuojavastaavan useampaa tällaista viranomaista tai julkishallinnon elintä varten huomioiden kuitenkin organisaation rakenteen ja suuruuden. Tietosuojavastaavan tulee pitää yhteyttä rekisteröityihin ja valvontaviranomaiseen näiden käyttämällä kielellä.³⁵

7 Organisaation tietosuojavastaava

Tietosuojavastaava toimii tehtävässään riippumattomassa asemassa. Tämä tarkoittaa käytännössä sitä, että tietosuojavastaava ei ota vastaan ohjeita siitä, miten hänen tulisi tehtäviään suorittaa. Rekisterinpitäjän ja henkilötietojen käsittelijän tulee varmistaa, että tietosuoja-vastaavan riippumattomuus toteutuu. Tietosuojavastaava ei ole henkilökohtaisesti vastuussa organisaation henkilötietojen käsittelystä, vaan kokonaisvastuu lainmukaisesta käsittelystä on aina rekisterinpitäjällä tai henkilötietojen käsittelijällä.³⁶ Tietosuojavastaavan nimittämistä miettiessä tulisi huomioida henkilön ammattipätevyys, asiantuntemus sekä valmius selviytyä tietosuojavastaavan tehtävistä, vaikka varsinaisia vaatimuksia ei ole koulutuksesta tai kokemuksesta asetettu. Tietosuojavastaava voi olla organisaation henkilöstöä tai tietosuojavastaava voidaan ottaa palvelusopimuksella myös organisaation ulkopuolelta.³⁷

³⁴ Warma-Lehtinen 2018, 348.

³⁵ WP 243, 12.

³⁶ Warma-Lehtinen 2018, 363-364.

³⁷ Hanninen ym. 2017, 121.

Tietosuojavastaavaa ei voi rangaista tai erottaa sillä perusteella, että hän on hoitanut tietosuojavastaavan tehtäviään. Rangaistus voi tarkoittaa esimerkiksi ylennyksen viivästyistä tai etuuden epäämistä, jonka toiset työntekijät saavat. Tämän tarkoitus on suojata tietosuojavastaavaa tietosuojatehtävien hoidossa, vahvistaa hänen riippumatonta asemaa sekä varmistaa, että tietosuojavastaavan toiminta on itsenäistä. Jos kyseessä on lainmukainen peruste, joka koskee myös muita työntekijöitä eikä liity hänen työtehtävänsä hoitoon voidaan tietosuojavastaava tällöin erottaa. Tällaisia syitä voivat olla esimerkiksi varkaus tai seksuaalinen häirintä. Yleisessä tietosuojasetuksessa ei kuitenkaan määritellä miten ja milloin tietosuojavastaava voidaan erottaa.

Tietosuojavastaava voi hoitaa myös muita tehtäviä ja velvollisuuksia toimiessaan tietosuojavastaavana. Organisaation tulee kuitenkin varmistaa, että kyseiset tehtävät ja velvollisuudet eivät aiheuta eturistiriitoja. Eturistiriidat tulee arvioida aina tapauskohtaisesti koska on olemassa erilaisia organisaatorakenteita. Tietosuojavastaavana ei voi toimia henkilö, joka organisaatiossa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot. Lähtökohtaisesti katsotaan, että ylemmän johtoaseman omaavat henkilöt kuten esimerkiksi pääjohtaja, henkilöstöpäällikkö tai IT-päällikkö voivat aiheuttaa eturistiriitoja ja täten he eivät voi toimia tietosuojavastaavana.³⁸

7.1 Tietosuojavastaavan asema

Rekisterinpitäjän ja henkilötietojen käsittelijän tulee varmistaa, että henkilötietojen suoja koskevien kysymysten käsittelyyn on otettu riittävän ajoissa ja asianmukaisesti mukaan myös tietosuojavastaava. Tietosuojavastaavan osallistumisella tietosuojakysymysten käsittelyyn helpotetaan tietosuojalainsäädännön noudattamista. On tärkeää pitää tietosuojavastaava ajan tasalla ja pyytää neuvoja alusta lähtien. Vaikutustendarvioinnin osalta tietosuojasetuksessa on nimenomaan säädetty tietosuojavastaavan varhaisesta mukanaolosta sekä siitä, että rekisterinpitäjän on pyydettävä tietosuojavastaavalta neuvoja koskien vaikutustendarviointia. Rekisterinpitäjän ja henkilötietojen käsittelijän tulisi kutsua tietosuojavastaava säännöllisesti johdon kokouksiin. Tietosuojavastaavaa tulisi kuulla mahdollisimman pian, mikäli organisaatiossa tapahtuu tietoturvaloukkaus. Tietosuojavastaava olisi hyvä ottaa mukaan tietosuojaa koskeviin päätöksentekoon ja tietosuojavastaavan näkemys tulisi huomioida asianmukaisesti.

³⁸ WP 243, 17-18.

Erimielisyystilanteissa, joissa tietosuojavastaavan mielipide eroaa johdon mielipiteistä ja tietosuojavastaavan neuvoja ei noudateta, tulisi dokumentoida perusteet miksi näin on toimittu.³⁹

7.2 Tietosuojavastaavan tehtävät

Tietosuojavastaavan tehtävät on määritelty tietosuoja-asetuksen 39 artiklassa. Tietosuojavastaavan tulee antaa tietoja ja neuvoja organisaatiolle ja organisaatiossa henkilötietoja käsitteleville työntekijöille tietosuoja-asetuksen ja muiden tietosuojasäännösten mukaisista velvollisuuksista. Tietosuojavastaavan tehtävänä on seurata tietosuoja-asetuksen sekä muun tietosuojalainsäädännön noudattamista ja organisaation henkilötietojen suojaan liittyviä toimintamenettelyjä kuten vastuunjakoa, tiedon lisäämistä, henkilöstön koulutusta sekä tarkastuksia. Vaikutustenarvioinnissa tietosuojavastaava antaa pyydettyä neuvoja ja valvoo sen toteutumista. Tietosuojavastaava toimii valvontaviranomaisen yhteyspisteenä ennakkokuulemisessa sekä muissa mahdollisissa kysymyksissä.

Rekisterinpitäjällä ja henkilötietojen käsittelijällä on oikeus määritellä tietosuojavastaavalle myös muita tehtäviä.⁴⁰ WP29-tietosuojaryhmä suosittelee, että tietosuojavastaavalta pyydetään neuvoja esimerkiksi vaikutustenarviointia koskevissa kysymyksissä, kuten onko sellainen syytä tehdä, mitä menetelmiä siinä olisi syytä noudattaa, toteutetaanko se organisaatiossa sisäisesti vai olisiko se hyvä ulkoistaa. Lisäksi tietosuojavastaavalta voidaan pyytää näkemystä siitä toteutettiin vai vaikutustenarviointi oikein ja onko sen mukana tuomat päätelmät tietosuojalainsäädännön vaatimukset täyttäviä. Rekisterinpitäjän ja tietosuojavastaavan näkemysten erotessa, tulisi vaikutusten arviointia koskevissa asiakirjoissa olla kirjallinen perustelu, miksi tietosuojavastaavan ohjeita ei noudatettu. Tietosuojavastaavaa olisi hyvä kuulla myös rekisteröidyn oikeuksiin ja etuihin koskevien riskien arvioinnissa ja toteutuksessa.⁴¹

7.3 Resurssit

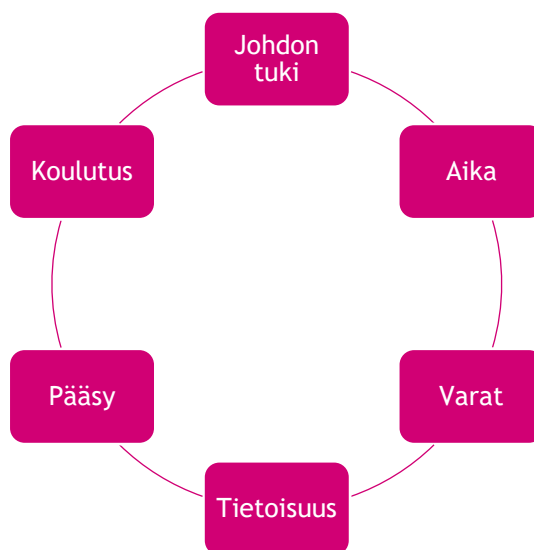
Yleisen tietosuoja-asetuksen 38 artiklan 2 kohdan mukaan organisaation on tuettava tietosuojavastaavaa tämän suorittaessa tehtäviään ”antamalla tälle resurssit, jotka ovat tarpeen näiden tehtävien täyttämiseksi, samoin kuin pääsyn henkilötietoihin ja käsittelytoimiin, sekä tä-

³⁹ WP 243, 15.

⁴⁰ Warmo-Lehtinen 2018, 368.

⁴¹ WP 243, 19-20.

män asiantuntemuksen ylläpitämiseksi”. Organisaation johdon tulisi tukea tietosuojavastaavaa. Tietosuojavastaavalla tulisi olla tarvittava aika tehtävien hoitamiseen. Jos tietosuojavastaavaa ei ole nimetty kokoaikaisesti hoitamaan tietosuojavastaavan tehtäviä, olisi suositeltavaa, että hänelle määriteltäisiin prosenttiosuus ajasta, joka käytetään tietosuojavastaavan tehtävien hoitamiseen. Hyvän käytännön tapaista olisi myös määrittää tietosuojavastaavan tehtävien hoitamiseen tarvittava aika, asianmukainen prioriteettitaso sekä laatia työsuunnitelma. Tietosuojavastaava tarvitsee myös muita resursseja, joita ovat esimerkiksi palvelut, tilat ja laitteet sekä mahdollisesti henkilöstö. Tietosuojavastaavalle voidaan antaa käyttöön henkilöstöä muodostaen tietosuojavastaavan tiimin, joka auttaa tietosuojavastaavaa tehtävissään. Koko organisaation tulisi tietää tietosuojavastaavan olemassa olosta ja tehtävästä, joten olisi hyvä että, tietosuojavastaavan nimityksestä tiedotetaan virallisesti koko henkilöstölle. Erityisen tärkeää on tarjota tietosuojavastaavalle pääsy palveluihin, jotka ovat tarpeellisia hänen tehtäviensä hoidon kannalta. Tietosuojavastaavan tulisi voida kehittää ja ylläpitää asiantuntemustaan, jonka vuoksi hänen olisi hyvä osallistua koulutuksiin ja kursseille. Tietosuojavastaavan tehtävä tulee olla resursoitu riittävästi suhteessa suoritettavaan tietojenkäsittelyyn eli resurssien tarve suurenee mitä monimutkaisemmista ja arkaluonteisimmista käsitteilytoimista on kysymys.⁴² Kuviossa 2 on havainnollistettu tietosuojavastaavan tarvitsemia resursseja.



Kuvio 2: Tietosuojavastaavalle tarjottavat resurssit

⁴² WP 243, 16.

8 Tietosuojavastaavana toimiminen

Tietosuojavastaavan työ on haastavaa. Hänen tulisi seurata lainsäädäntöä, määräyksiä ja ohjeistuksia ja reagoitava niiden tuomiin muutoksiin. Lisäksi tietosuojavastaavan työhön kuuluu tiedon jakaminen ja erilaisten asioiden valvonta organisaation sisällä. Tietosuojavastaava on usein vuorovaikutuksessa erilaisten tahojen kanssa. Aika on yleensä rajallista, varsinkin jos hoitaa tietosuojavastaavan tehtäviä muun työn ohella. Tietosuojavastaava kokeekin usein, että aika ei riitä kaiken työn tekemiseen ja työ saattaa olla osittain vain pintapuolista. Tietosuojavastaavan on tärkeää huolehtia omasta jaksamisestaan.⁴³

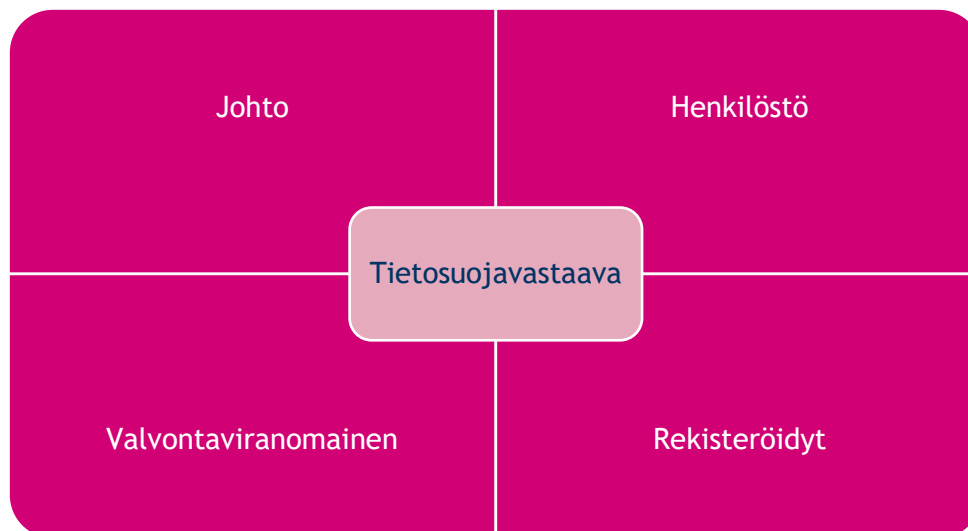
Tietosuojavastaavan aika on rajallinen ja tehtävää saattaa olla usein liian paljon. Oman jaksamisen vuoksi olisi tärkeää opetella priorisoimaan tehtäviään päivittäisessä työssä. Suuret linjaukset priorisoinnista tietosuojavastaavan tulisi kuitenkin tehdä yhdessä johdon kanssa, jotta saadaan yhteinen päätös asioiden tärkeydestä. Priorisointiperusteita voivat olla esimerkiksi kiireellisyys, kiinnostavuus tai merkittävyys. Asiakkaisiin liittyvät tietosuoja-asiat menevät yleensä priorisointilistan kärkeen. Tietosuojavastaavaa voi auttaa myös se, että tekee oman työnsä näkyväksi. Tämä tarkoittaa sitä, että pilkkoo isot kokonaisuudet pienemmiksi palloiksi. Yksittäiset tehtävät on helpompi aikatauluttaa ja työnkuormittavuus yleensä vähenee. Työnnäkyväksi tekemisen keinoja on kirjoittaa esimerkiksi päiväkirjaa työtehtävistä tai tehdä niistä huoneen seinälle taulu.⁴⁴

Tietosuojavastaava toimii organisaation sisäisenä erityisasiantuntijana tietosuoja-asioissa. Hän on yhteydessä niin johtoon kun henkilöstöön. Lisäksi tietosuojavastaava toimii rekisteröityjen ja valvontaviranomaisen yhteyspisteenä.⁴⁵ Kuviossa 3 on kuvattu tietosuojavastaavan roolit.

⁴³ Andreasson, Riikonen & Ylipartanen 2019, 103-104.

⁴⁴ Andreasson ym. 2019, 105-106.

⁴⁵ Protietosuojavastaava. Toukokuussa 2018 voimaan tuleva EU:n tietosuoja-asetus laajentaa tietosuojavastaavien ammattikuntaa.



Kuvio 3: Tietosuojavastaavan roolit

8.1 Tietosuojavastaava ja johto

Tietosuojavastaava tekee yhteistyötä johdon kanssa. Tiivis yhteistyö ja johdon sitoutuminen ovat perusedellytykset tietosuojatyön onnistumiselle. Tietosuojan toteutuminen organisaatiossa on viimekädessä aina johdon vastuulla. Johdon tulisi laatia tietosuoja- ja tietoturvapoliittikka, joista käy ilmi johdon asettamat tavoitteet koskien tietosuojaa ja tietoturvaa organisaatiossa. Henkilötietojen käsittelylle asetetut periaatteet sekä tietosuojan merkitys organisaatiossa tulisi kuvata tietosuojapolitiikassa. Tietoturvapoliitikassa puolestaan määritellään tietoturvan kohteet, periaatteet sekä vastuujao. Tietosuoja-asetus toi mukanaan osoitusvelvollisuuden, joka tarkoittaa sitä, että organisaation tulee pystyä osoittamaan miten se on varmistanut teknisin, hallinnollisin ja organisatorisin toimenpiteiden avulla tietosuojavelvollisuuksien toteutumisen organisaatiossaan. Tietosuojavastaavan tehtävä on raportoida suoraan ylimmälle johdolle, joten johdon tulee olla tietoinen tietosuojan tasosta organisaatiossa.⁴⁶

Aiemmin on jo mainittu, että yksi tietosuojavastaavalle tarjottava resurssi olisi johdon tuki. Johdon tuen voidaan katsoa muodostuvan toiminnanedellytyksistä, kuten esimerkiksi tavoitteista, osallistumismahdollisuuksista ja tiedon jakamisesta. Toimintaedellytyksiä voidaan katsoa olevan kaikki sellainen joka luo pohjan sille, että tietosuojavastaava voi hoitaa työnsä.

⁴⁶ Andreasson ym. 2019, 109, 113-114.

Johdon tulisi laatia tietosuojavastaavalle selkeä ja toimenkuva, jossa on määritelty tietosuojavastaavalle kuuluvat valtuudet ja vastuut. Johdon tulee tarjota tietosuojavastaavalle myös tarpeelliset resurssit.⁴⁷

Kannustus on tärkeä osa johdon tukea, esimerkiksi palkkiot, palaute ja motivointi ovat hyviä tapoja kannustaa tietosuojavastaavaa työssään. Tietosuojavastaavaa kuten myös muita työntekijöitä kannattaa ohjata itseohjautuvuuteen ja omaan ajatteluun, täten he tuovat omia näkökulmiaan ja ehdotuksiaan asioiden kehittämiseen ja uudistamiseen. Hyvä johto asetta tietosuojavastaavalle tavoitteita, joiden saavuttamisesta voidaan palkita esimerkiksi rahallisella palkkiolla, jonka suuruus on suhteutettu työn vaativuuteen. Johon tulee seurata asetettujen tavoitteiden täyttymistä ja antaa tietosuojavastaavalle palautetta työsuorituksistaan. Nämä edellä mainitut keinot motivoivat tietosuojavastaavaa ja lisäävät täten työn mielekkyyttä.⁴⁸

Johdon tukeen kuuluu myös luottamus, johon voidaan lukea esimerkiksi kuuntelu, kunnioitus sekä vastuun antaminen. Toiminnan edellytysten ja kannustuksen ollessa kunnossa, syntyy tietosuojavastavan ja johdon välille useimmiten luottamus. Avoin viestintä sekä toiminnan läpinäkyvyys lisäävät luottamusta. Johdon tulisi kuunnella tietosuojavastaavaa, antaa hänen mielipiteilleen ja näkemyksilleen arvostusta. Kun luottamus henkilöön on kunnossa, annetaan hänelle usein myös lisää vastuuta. Tietosuojavastaavaa ei kuitenkaan saa jättää yksin vastuun kanssa, vaan johdon tulee tukea antamalla tarvittaessa ohjausta sekä seurata tehtävien hoitoa.⁴⁹

8.2 Tietosuojavastaava ja henkilöstö

Tietosuojavastavan tulee olla henkilöstön tukena neuvon, tiedottaen ja kouluttaen. Tietosuojavastavan yksi keskeinen tehtävä on suunnitella ja laatia ohjeistukset koskien henkilötietojen käsittelyä. Ohjeistuksia tulee tarkastella ja päivittää tarvittaessa, se ei ole vain kertaluonteinen projekti. Ohjeistusten laadinnassa voi ja kannattaa tehdä yhteistyötä muiden samankaltaisten toimijoiden kanssa, sillä työtehtävät ovat tällöin usein samankaltaisia. Kun ohjeistukset on laadittu, tulisi ne kouluttaa koko henkilöstölle.⁵⁰

⁴⁷ Andreasson ym. 2019, 110-111.

⁴⁸ Andreasson ym. 2019, 111.

⁴⁹ Andreasson ym. 2019, 109-112.

⁵⁰ Andreasson ym. 2019, 115.

Uuden työntekijän saapuessa töihin, tulisi huolehtia riittävästä perehdytyksestä myös tietosuojan ja tietoturvan osalta. Työntekijän on tärkeää ymmärtää tietosuojan ja tietoturvan merkitys työssään. Perehdyttäminen saattaa olla joissakin organisaatioissa pintapuolista esimerkiksi ajanpuutteen vuoksi, mutta olisi todella tärkeää käydä ainakin salassapitoasiat lävitse. Työntekijän syyllystyessä tietosuojarikkomukseen, saattaa hän vedota siihen, että ei sitä ole käyty perehdytyksessä läpi. Työntekijällä on kuitenkin velvollisuus ottaa asioista selvää, mikäli jokin asia on epäselvä hänelle.⁵¹

Tietosuoja-asetuksen 5 artiklassa on säädetty rekisterinpitäjälle velvollisuus, jossa henkilötietoja tulee suojata luvattomalta sekä lainvastaiselta käsittelyltä, mutta myös vahingossa tapahtuvalta häviämislä, tuhoutumiselta tai vahingoittumiselta käyttäen tarpeellisia organisatorisia ja teknisiä toimia. Organisatorisilla toimenpiteillä tarkoitetaan esimerkiksi käyttövaltuuden antamisen yhteydessä käytyä ohjeistusta tai salassapitosopimusta. Tekninen toimi on puolestaan esimerkiksi käyttäjän tunnistaminen. Rekisterinpitäjälle on asetettu myös velvollisuus seurata, että asetettuja suojaustoimenpiteitä noudatetaan. Organisaatiot voivat ylläpitää esimerkiksi käyttö- ja luovutusrekisterilokia, joita rekisterinpitäjä seuraa jälkikäteisesti. Lokien tarkoitus on tukea käyttäjien eli työntekijöiden oikeusturvaa. Asiakas voi esimerkiksi väittää, että hänen tietojansa on katseltu ilman asiakassuhdetta, jolloin käyttövalvontalokista voidaan tarkastaa onko näin käynyt. Lokirekisterien valvonta kuuluu yleensä tietosuojavastavan tehtäviin.⁵²

8.3 Tietosuojavastaava ja valvontaviranomainen

Suomen valvontaviranomaisena toimii tietosuojavaltuutetun toimisto. Tietosuojavastaan tehtävänä on toimia valvontaviranomaisen yhteyspisteenä käsittelyyn liittyvissä kysymyksissä sekä tehdä valvontaviranomaisen kanssa yhteistyötä. Tähän luetaan mukaan myös tietosuoja-asetuksen 36 artiklan mukainen ennakkokuuleminen sekä kuuleminen muista kysymyksistä. Tietosuojavastaava toimii organisaation yhteyshenkilönä ja auttaa valvontaviranomaista saamaan käyttöönsä tarvittavat asiakirjat ja tiedot.⁵³

⁵¹ Andreasson ym. 2019, 116-117.

⁵² Andreasson ym. 125-127.

⁵³ WP 243, 20.

8.4 Tietosuojavastaava ja rekisteröidyt

Tietosuoja-asetuksen 38 artiklan 4 kohdan mukaan rekisteröity voi ottaa yhteyttä tietosuoja-vastaavaan kaikissa henkilötietojen käsittelyyn liittyvissä asioissa mukaan lukien tietosuoja-asetuksen tuomien oikeuksien käytössä. Tietosuoja-asetuksen 13 ja 14 artiklassa säädetään rekisteröidyn informoinnista. Rekisteröityä tulee informoida hänen henkilötietojensa käsitte-lystä, mutta rekisteröidyllä on muita tietosuojoikeudellisia oikeuksia. Rekisteröidyn oikeuk-sista säädetään tietosuoja-asetuksen 3 luvussa. Tietosuoja-asetuksen 15 artiklan mukaan re-kisteröidyllä on oikeus tietää mitä henkilötietoja hänestä käsitellään sekä oikeus tietää mikäli hänen henkilötietojaan ei käsitellä. Rekisteröidyn oikeuksiin kuuluvat myös tietosuoja-asetuk-sen 15 artiklan mukainen oikeus saada henkilötiedot itselle, 16 artiklan mukainen oikeus vaa-tia tietojen korjaamista ja 17 artiklan mukainen oikeus vaatia tietojen poistamista. Rekiste-röidyllä on myös tietosuoja-asetuksen 18 artiklan mukainen oikeus käsittelyn rajoittamiseen, 20 artiklan mukainen oikeus siirtää tiedot järjestelmästä toiseen, 21 artiklan mukainen vas-tustamisoikeus sekä 22 artiklan mukainen oikeus olla joutumatta automaattisen päätöksen kohteeksi. Henkilö voi tehdä tietosuoja-asetuksen 77 artiklan mukaan valituksen valvontavi-ranomaiselle jos hän katsoo, että henkilötietojen käsittelyssä rikotaan tietosuoja-asetusta. Henkilö voi käyttää myös muita hallinnollisia muutoksenhaku- ja oikeussuojakeinoja. Tieto-suoja-asetuksen 79 artiklan mukainen tehokas oikeussuojakeino on nostaa kanne tuomioistui-messa rekisterinpitäjää tai henkilötietojen käsittelijää vastaan, jos hän katsoo, että hänen oikeuksiaan on loukattu sen takia, ettei ole noudatettu tietosuoja-asetusta.⁵⁴ Kuviossa 4 on lueteltu rekisteröidyn oikeudet, joita hän voi käyttää olemalla yhteydessä suoraan rekisterin-pitäjään tai mahdolliseen tietosuojavastaavaan.

Tietosuoja-asetuksen 12 artiklan mukaan rekisterinpitäjän tulee toimimittaa rekisteröidylle informointivelvollisuutta koskevat tiedot sekä 15-22 artiklan mukaiset käsittelyä koskevat tie-dot kirjallisesti, paitsi jos rekisteröity pyytää saada ne suullisesti edellyttäen kuitenkin henki-löllisyyden tarkastamista muulla tavoin. Tiedot tulee olla tiiviit, läpinäkyvät ja helposti ym-märrettävät. Rekisterinpitäjällä on oikeus kieltäytyä toimittamasta tietoja vain, jos hän pys-tyy osoittamaan, että ei pysty tunnistamaan rekisteröityä. Rekisterinpitäjän tulee vastata re-kisteröidylle viimeistään kuukauden kuluessa mihin toimenpiteisiin se on ryhtynyt rekiste-röidyn pyynnön toteuttamiseksi. Jos pyyntöjä on monta tai ne ovat monimutkaisia, voidaan määräaika jatkaa kahdella kuukaudella, mutta tällöinkin rekisteröidylle on ilmoitettava kuu-kauden kuluessa viivästyksestä sekä kerrottava viivästyksen syyt. Tietosuoja-asetuksen 12 ar-tiklan 4 kohdan mukaan jos rekisterinpitäjä kieltäytyy toteuttamasta rekisteröidyn pyyntöä,

⁵⁴ Ks. Andreasson ym. 2019, 166-170.

tulee rekisterinpitäjän antaa perustelu kieltäytymiselle. Tämän jälkeen rekisteröity voi laittaa asian vireille valvontaviranomaiselle tai käyttää muita oikeussuojakeinoja.

15 artikla	•Oikeus saada pääsy tietoihin
16 artikla	•Oikeus tietojen oikaisemiseen
17 artikla	•Oikeus tietojen poistamiseen
18 artikla	•Oikeus käsittelyn rajoittamiseen
20 artikla	•Oikeus siirtää tiedot järjestelmästä toiseen
21 artikla	•Vastustamisoikeus
22 artikla	•Oikeus olla joutumatta automaattisen päätöksen teon kohteeksi

Kuvio 4: Rekisteröidyn oikeudet

9 Tietosuojavastaavien yhteystiedot tietosuojavaltuutetun toimistolla

Tietosuoja-asetuksen 37 artiklan 7 kohdan mukaan tietosuojavastaavan yhteystiedot tulee ilmoittaa valvontaviranomaiselle, joka Suomessa on tietosuojavaltuutettu.⁵⁵ Tietosuojavaltuutetun toimisto julkaisi tietosuoja-asetuksen soveltamisen alkaessa uudistetut kotisivut, jotka löytyvät osoitteesta tietosuoja.fi. Uudistettujen kotisivujen on tarkoitus vastata erilaisen käyttäjien tarpeisiin ja lomakkeiden avulla pyritään helpottamaan asiointia tietosuojavaltuutetun kanssa.⁵⁶ Kotisivuilla on ilmoitus tietosuojavastaavasta -lomake niin suomeksi, ruotsiksi kuin englanniksi. Mikäli rekisterinpitäjän, henkilötietojen käsittelijän tai tietosuojavastaavan tiedoissa tapahtuu muutoksia, tulee niistä ilmoittaa myös tietosuojavaltuutetun toimistolle.

⁵⁵ Ks. Korpisaari ym. 2018, 357.

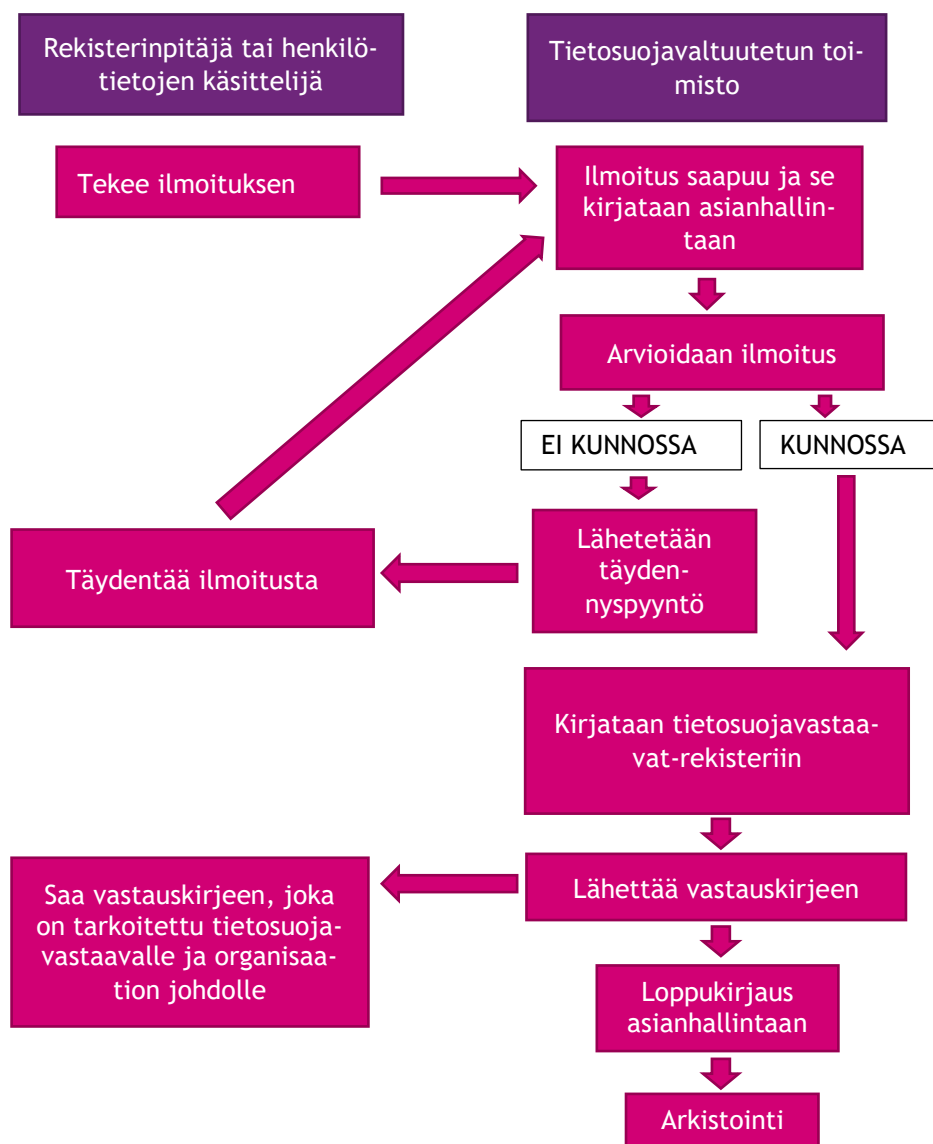
⁵⁶ Tietosuojavaltuutetun toimisto. Ajankohtaista. Tietosuojavaltuutetun toimiston verkkosivut uudistuivat.

Kotisivuille on luotu tätä varten myös muutoslomake kieliversioineen. Edellä mainitut lomakkeet ovat liitteinä 1-6.

9.1 Ilmoitusten käsittely tietosuojavaltuutetun toimistolla

Ilmoitus tietosuojavastaavasta saapuu useimmiten tietosuojavaltuutetun toimiston kotisivujen kautta täytetyllä lomakkeella. Täytetty lomake saapuu virastopostiin aivan niin kuin muutkin sähköisesti vireille saatetut asiat. Kokemuksen mukaan ilmoituksia tuli vuonna 2018 lomakkeiden lisäksi jonkin verran myös postitse tai tavallisella sähköpostiviestillä. Vuonna 2019 rekisterinpitäjät ovat hyvin löytäneet lomakkeen kotisivuilta ja muulla tavalla tehtyjä ilmoituksia tulee enää harvakseltaan. Tämä on hyvä juttu, koska silloin rekisterinpitäjät ja henkilötietojen käsittelijät ilmoittavat tietosuojavaltuutetun toimistolle kaikki tarpeelliset tiedot. Ilmoituksen ollessa kuitenkin epäselvä tai puutteellinen, pyydetään organisaatiota täydentämään ilmoitusta.

Tietosuojavaltuutetun toimistoon saapuneet ilmoitukset tietosuojavastaavista kirjataan asianhallintaan kuten muutkin vireille saatetut asiat. Asianhallinnasta se saa oman diaarinumeron, jolla kyseisen organisaation tietosuojavastaava-ilmoituksia käsitellään myös jatkossa. Tietosuojavastaavan yhteystiedot kirjataan myös erilliseen tietosuojavastaavat-rekisteriin, jota päivitetään aina muutosten tullessa. Tietosuojavaltuutetun toimistosta lähetetään tietosuojavastaavalle sähköpostitse vastaus ilmoituksen saapumisesta ja se pyydetään toimittamaan myös organisaation johdolle. Vastaus sisältää infokirjeen, jossa on tärkeää tietoa tietosuojavastaavana toimimisesta. Vastauskirje lähetetään suomeksi, ruotsiksi ja englanniksi. Täten varmistetaan, että tietosuojavastaava sekä organisaation johto ymmärtävät lukemansa. Asia päätetään tietosuojavaltuutetun toimistossa vastauskirjeen myötä ja arkistoidaan. Tietosuojavastaavan vaihtuessa organisaatiossa, kirjataan uusi tietosuojavastaava diaarinumeron yhteyteen ja tiedot päivitetään tietosuojavastaavat-rekisteriin. Rekisterissä on täten aina ajantasainen tieto. Kuviossa 5 on kuvattu tietosuojavastaavien ilmoitusten käsittelyprosessi tietosuojavaltuutetun toimistolla.

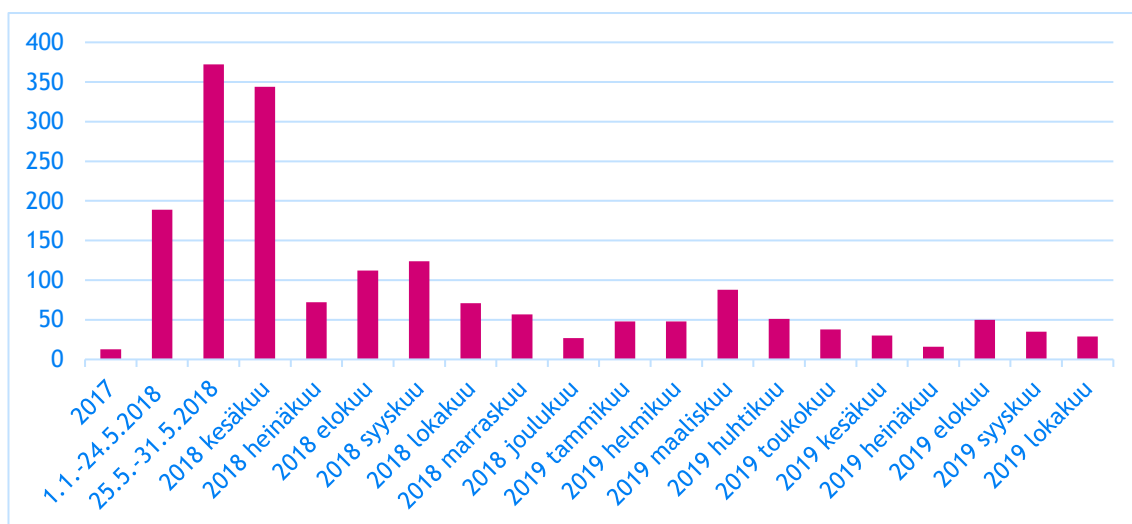


Kuvio 5: Tietosuojavastaavien ilmoitusten käsittelyprosessi

9.2 Tilastoja tietosuojavastaava-ilmoituksista

Tietosuojavaltuutetun toimistolle on saapunut 1814 ilmoitusta nimetyistä tietosuojavastavista vuoden 2019 lokakuun loppuun mennessä. Luku ei kuitenkaan ole verrannollinen tietosuojavastaavien lukumäärään, sillä ilmoitukset ovat rekisterinpitäjä/henkilötietojen käsittelijä -kohtaisia. Tämä tarkoittaa sitä, että tietosuojavastaava voi toimia esimerkiksi viiden yrityksen tietosuojavastaavana. Tällöin jokainen yritys on ilmoittanut tietosuojavastaavan tietosuojavaltuutetun toimistolle, joten ilmoituksia on täten saapunut viisi. Ensimmäinen ilmoitus nimetyistä tietosuojavastavista on saapunut tietosuojavaltuutetun toimistolle toukokuussa 2017. Vuonna 2017 ilmoituksia tietosuojavastavista tuli yhteensä 13 kappaletta. Vuonna 2018

ennen tietosuoja-asetuksen soveltamisen aloittamista 25.5.2018 tietosuojavaltuutetun toimistolle oli saapunut 189 kappaletta ilmoituksia nimetyistä tietosuojavastaavista. Toukokuun lopussa vuonna 2018 tietosuoja-asetuksen soveltamisen alkaessa ilmoituksia tuli 372 kappaletta, 177 niistä on tullut vireille tietosuojavaltuutetun toimistossa päivänä, jolloin tietosuoja-asetusta alettiin soveltamaan.⁵⁷ Vuoden 2018 kesäkuun jälkeen tilanne rauhoittui ja ilmoituksia tietosuojavastaavista tulee tasaisesti. Vuoden vaihteessa sekä kesälomakautena ilmoitusten lukumäärä hiukan pienenee. Hiukan enemmän ilmoituksia saattaa tulla silloin kun jokin taho on pitänyt tietosuojakoulutusta. Tämän voi päätellä siitä, kun saapuneet ilmoitukset tulevat samalta sektorilta muutaman päivän sisällä. Taulukossa 1 on kuvattu tietosuojavaltuutetun toimistolle kuukausittain saapuneiden ilmoitusten lukumäärää tietosuoja-asetuksen soveltamisajankohdan jälkeen. Taulukossa on kuitenkin ilmoitettu vuoden 2017, toukokuu ennen tietosuoja-asetuksen soveltamisen aloitusta ja toukokuu, kun tietosuoja-asetusta alettiin soveltamaan omina pylväinään verrannollisuuden vuoksi.



Taulukko 1: Tilasto ilmoitetuista tietosuojavastaavista

⁵⁷ Tietosuojavaltuutetun toimisto. Tilastotiedot.

9.3 Huomiot ja korjausehdotukset

Yli vuoden kokemus tietosuojavastaava-ilmoitusten käsittelijänä on tuonut mukanaan näemyksen, että rekisterinpitäjät ja henkilötietojen käsittelijät eivät välttämättä tunne termejä rekisterinpitäjä tai henkilötietojen käsittelijä. Ilmoituksiin saatetaan kirjoittaa organisaation yksittäisen henkilön nimi kun kysytään rekisterinpitäjän tai henkilötietojen käsittelijän nimeä. Lomakkeessa lukee ”Rekisterinpitäjäksi kutsutaan yritystä, viranomaista, yhteisöä tai henkilöä, joka määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot. Henkilötietojen käsittelijäksi kutsutaan rekisterinpitäjältä ulkopuolista tahoa, joka käsittelee henkilötietoja rekisterinpitäjän puolesta”. Rekisterinpitäjällä tarkoitetaan siis organisaatiota, eikä yksittäistä henkilöä organisaatiossa.

Tietosuojavaltuutetun toimisto on kiinnittänyt huomiota siihen, että suuri osa organisaatioista, joiden tulisi nimittää tietosuojavastaava, ei ole tehnyt ilmoitusta tietosuojavaltuutetun toimistolle. Monet organisaatiot ovat luultavasti kuitenkin nimittäneet tietosuojavastaavan, mutta eivät ole ymmärtäneet välttämättä sitä, että heidän tulisi ilmoittaa siitä myös valvontaviranomaiselle. Tietosuojavaltuutetun toimisto on lisännyt asiasta muistutuksen uutiskirjeisiin ja miettinyt, jos sidosryhmäyhteistyön kautta saisi muistutettua asiasta.

Organisaatiot, jotka ovat tietosuoja-asetuksen mukaan ilmoittaneet tietosuojavastaavasta tietosuojavaltuutetun toimistolle, eivät välttämättä ole muistaneet ilmoittaa tietosuojavastaavan vaihtumista tai muusta muutoksesta. Tällöin tietosuojavaltuutetun toimistolla ei ole ajantasaista tietoa organisaation tietosuojavastaavasta ja yhteydenpito valvontaviranomaisen ja tietosuojavastaavan välillä saattaa vaikeutua. Osa organisaatiosta puolestaan on tehnyt muutoksen ilmoituksen, mutta tietosuojavaltuutettu ei ole saanut aiemmin ilmoitusta tietosuojavastaavasta. Tällöin tietosuojavaltuutetun toimisto pyytää organisaatiota täydentämään ilmoitusta puuttuvien tietojen osalta, sillä muutos ilmoituksessa ilmoitetaan vain muuttuneet tiedot.

Kun tietosuoja-asetusta alettiin soveltamaan toukokuussa 2018, tuli tietosuojavastaava-ilmoituksia todella suuri määrä. Osa rekisterinpitäjistä ja henkilötietojen käsittelijöistä ilmoitti tietosuojavastaavan useampaan kertaan. Tällöin tuli olla tarkkana, että ei kirjaa samaa organisaatiota koskevaa ilmoitusta useammalle diaarinumerolle. Edelleen tulee uusia ilmoituksia tietosuojavastaavasta, vaikka tarkoitus on ilmoittaa muutoksesta. Tämän vuoksi tietosuojavastaava-ilmoitusten käsittelijän tulee tarkistaa onko organisaatio ilmoittanut jo aikaisemmin tietosuojavastaavan yhteystiedot tietosuojavaltuutetun toimistolle.

Tietosuojavaltuutetun toimistossa on myös ehdotettu sitä, että ilmoitus tietosuojavastaavasta -lomake ja muutos ilmoituksesta tietosuojavastaavasta -lomake yhdistettäisiin yhdeksi lomakkeeksi. Tällöin lomakkeessa olisi valintaruutu sille, onko kyseessä uusi ilmoitus vai kyse muutoksen ilmoittamisesta valvontaviranomaiselle. Yhdistetyllä lomakkeella rekisterinpitäjät ja

henkilötietojen käsittelijät löytäisivät aina siihen tarkoitettun lomakkeen. Tuloksena väärin lomakkeiden käyttö vähenisi, sillä organisaatioiden pitäisi lomaketta täyttäessä miettiä onko kyseessä uusi ilmoitus vai kyse muutoksen ilmoittamisesta.

Tilastojen ottamista tulisi myös kehittää. Tällä hetkellä tietosuojavastaavat-rekisteristä saadaan vaan tietosuojavastaava-ilmoitusten kokonaislukumäärä. Yksityiskohtaisemmat haut ovat todella vaikeita suorittaa. Esimerkiksi kuntien tekemien ilmoitusten lukumäärää on vaikeata seurata, koska kunnat ovat nimellä ”kunta” tai ”kaupunki”. Hakusanalla haettaessa ”kaupunki” haku onnistuu hyvin. ”Kunta”-haulla tulokseen tulevat mukaan myös seurakuntayhtymät, koska se sisältää sanan kunta.

Lähteet

Kirjallisuus

Aarnio, A. 2011. Luentoja lainopillisen tutkimuksen teoriasta. Helsinki: Unigrafia Oy Yliopistopaino.

Andreasson, A., Koivisto, J. & Ylipartanen, A. 2014. Tietosuojavastaavan käsikirja 2. Tallinna: Printon.

Andreasson, A., Koivisto, J. & Ylipartanen, A. 2015. Tietosuojakäsikirja johdolle. Tallinna: Printon.

Andreasson, A., Riikonen, J. & Ylipartanen, A. 2019. Osaava tietosuojavastaava ja EU:n yleinen tietosuoja-asetus. Tallinna: Printon.

Hanninen, M., Laine, E., Rantala, K., Rusi, M. & Varhela, Markku. 2017. Henkilötietojen käsittely: EU-tietosuoja-asetuksen vaatimukset. Vantaa: Hansaprint Oy.

Korpisaari, P., 9 artikla. teoksessa Korpisaari, P., Pitkänen, O. & Warma-Lehtinen, E. 2018. Uusi tietosuojalainsäädäntö. Helsinki: Alma Talent.

Korpisaari, P., 99 artikla. teoksessa Korpisaari, P., Pitkänen, O. & Warma-Lehtinen, E. 2018. Uusi tietosuojalainsäädäntö. Helsinki: Alma Talent.

Nykänen, P., Osa 1. teoksessa Lämsineva, P., Nykänen, P., Rautiainen, P., Ruohonen, J., Urpilainen, M. & Virtanen, P. 2013. Johdatus oikeusjärjestykseen. Tampere: Tampereen yliopisto, Johtamiskorkeakoulu.

Ojanen, T. 2016. EU-oikeuden perusteita; 3., uudistettu laitos. Helsinki: Edita Publishing Oy.

Warma-Lehtinen, E., artikla 37. teoksessa Korpisaari, P., Pitkänen, O. & Warma-Lehtinen, E. 2018. Uusi tietosuojalainsäädäntö. Helsinki: Alma Talent.

Warma-Lehtinen, E., artikla 38. teoksessa Korpisaari, P., Pitkänen, O. & Warma-Lehtinen, E. 2018. Uusi tietosuojalainsäädäntö. Helsinki: Alma Talent.

Warma-Lehtinen, E., artikla 39. teoksessa Korpisaari, P., Pitkänen, O. & Warma-Lehtinen, E. 2018. Uusi tietosuojalainsäädäntö. Helsinki: Alma Talent.

Virallislähteet

EU:n yleisen tietosuoja-asetuksen täytäntöönpanoryhmän (TATTI) mietintö. Oikeusministeriö, Helsinki 2017.

Euroopan parlamentin ja neuvoston asetus (2016/679) luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus).

Euroopan parlamentin ja neuvoston direktiivi (2016/680) luonnollisten henkilöiden suojelusta toimivaltaisten viranomaisten suorittamassa henkilötietojen käsittelyssä rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten sekä näiden tietojen vapaasta liikkuvuudesta ja neuvoston puitepäättökseen 2008/977/YOS kumoamisesta.

Euroopan parlamentin ja neuvoston direktiivi (95/46/EY) yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta.

Euroopan unionin neuvosto. Toimielinten välinen asia: 2012/0011 (COD).

Hallituksen esitys eduskunnalle EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi (HE 9/2018).

Puitepäättös (2008/977/YOS) rikosasioissa tehtävissä sekä poliisi- ja oikeudellisessa yhteistyössä käsiteltävien henkilötietojen suojaamisesta.

Tietosuojaryhmä (WP29-työryhmä) 16/FI WP 243 rev.01. Tietosuojavastaavia koskevat ohjeet.

Hallintolaki (434/2003)

Henkilörekisterilaki (471/1987)

Henkilötietolaki (523/1999)

Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/2007)

Laki sähköisen viestinnän palveluista (917/2014)

Laki sähköisestä lääkemääräyksestä (61/2007)

Laki tietosuojalautakunnasta ja tietosuojavaltuutetusta (389/1994)

Laki yksityisyyden suojasta työelämässä (759/2014)

Luottotietolaki (527/2007)

Tietosuojalaki (1050/2018)

Muut lähteet

Eduskunta. EU:n yleisen tietosuoja-asetuksen (GDPR) täytäntöönpano - Uusi tietosuojalaki. https://www.eduskunta.fi/FI/tietoaeduskunnasta/kirjasto/aineistot/kotimainen_oikeus/LATI/EUn-tietosuojauudistus/Sivut/EUn-yleinen-tietosuoja-asetus.aspx Viitattu 8.11.2019.

Eduskunta. https://www.eduskunta.fi/FI/tietoaeduskunnasta/kirjasto/aineistot/kotimainen_oikeus/LATI/Sivut/EUn-tietosuojauudistus.aspx Viitattu 5.11.2019.

Euroopan unioni. Euroopan komissio. https://europa.eu/european-union/about-eu/institutions-bodies/european-commission_fi Viitattu 25.11.2019.

Euroopan unioni. Euroopan parlamentti. <https://www.europarl.europa.eu/portal/fi> Viitattu 25.11.2019.

Euroopan unioni. Euroopan unionin neuvosto. https://europa.eu/european-union/about-eu/institutions-bodies/council-eu_fi Viitattu 25.11.2019.

Euroopan unioni. Perustietoa Euroopan unionista. https://europa.eu/european-union/about-eu/eu-in-brief_fi Viitattu 8.12.2019.

Lakimiesuutiset. <https://lakimiesuutiset.fi/gdpr-on-edelleen-monelle-vieras/>. Viitattu 2.12.2019.

Opitietosuoja.fi. <https://opitietosuoja.fi/index.php/fi/56-lainsaadaentoe/lait/eun-tietosuoja-asetus/23-tuleva-eu-n-tietosuoja-asetus> Viitattu 7.11.2019.

Tietosuojavaltuutetun toimisto. <https://tietosuoja.fi/lainsaadanto>. Viitattu 13.11.2019.

Tietosuojavaltuutetun toimisto. <https://tietosuoja.fi/tietosuojavaltuutetun-toimisto> Viitattu 3.11.2019.

Tietosuojavaltuutetun toimisto. https://tietosuoja.fi/artikkeli/-/asset_publisher/tietosuoja-valtuutetun-toimiston-verkkosivut-uudistuivat Viitattu 5.11.2019.

Tietosuojavaltuutetun toimiston tilastotiedot tietosuojavastaavista. 4.11.2019.

Tietosuojavastaava. <https://www.protietosuojavastaava.fi/> Viitattu 2.12.2019.

Kuviot

Kuvio 1: Tietosuoja-asetuksen valmistelu	14
Kuvio 2: Tietosuojavastaavalle tarjottavat resurssit	21
Kuvio 3: Tietosuojavastaavan roolit	23
Kuvio 4: Rekisteröidyn oikeudet.....	27
Kuvio 5: Tietosuojavastaavien ilmoitusten käsittelyprosessi.....	29

Taulukot

Taulukko 1: Tilasto ilmoitetuista tietosuojavastaavista	30
---	----

Liitteet

Liite 1: Ilmoitus tietosuojavastaavasta -lomake.....	39
Liite 2: Muutos ilmoitukseen tietosuojavastaavasta -lomake	40
Liite 3: Anmälan on dataskyddombud -blankett.....	41
Liite 4: Ändring av anmälan om dataskyddombud -blankett.....	42
Liite 5: Declaration of Data Protection Officer -form	43
Liite 6: Change to Data Protection Officer declaration -form	44
Liite 7:Vastauskirje	45
Liite 8: Svar	47
Liite 9: Reply	49

Liite 1: Ilmoitus tietosuojavastaavasta -lomake

Ilmoitus tietosuojavastaavasta

Rekisterinpitäjän tai henkilötietojen käsitteijän nimi *

Rekisterinpitäjäksi katsutaan yrityksiä, viranomaisia, yhteisöitä tai henkilöitä, jotka määrittävät henkilötietojen käsittelyn tarkoituksen ja keinot. Henkilötietojen käsitteijäksi katsutaan rekisterinpitäjältä ulkopuolista tahoa, joka käsittelee henkilötietoja rekisterinpitäjän puolesta.

Ilmoittaja on *

- Rekisterinpitäjä
 Henkilötietojen käsitteijä

Yritys- ja yhteisötunnus (Y-tunnus)

Sähköpostiosoitte *

Puhelinnumero *

Osoite *

Tietosuojavastaava ilmoitetaan *

- Tietosuoja-asetuksen perusteella
 Erityislainsäädännön perusteella
 Vapaaehtoisesti

Vapaaehtoisesti nimettyä tietosuojavastaavaa koskevat aineet nimelläisperustetta, saamaa ja tehtäviä koskevat vastinmuksot kuin leikkauksella nimettyä.

Tietosuojavastaavan nimi

Tietosuojavastaavan nimen ilmoittaminen on vapaaehtoinen, mutta nimen ilmoittamista tietosuojavastuutalon toimialalle pidetään suositeltavana yritystyon helpottamiseksi. Tietosuojavastaavaksi ei saa nimetä henkilöä, jolla on eturistiriitoja.

Tietosuojavastaavan sähköpostiosoitte *

Sähköpostiosoitteen on hyvä olla sellainen, että vastaanottajan suostuvuus tietosuojavastaavan kanssa voidaan varmistaa etnis, myös esimerkiksi potaalojen ja henkilöviestien yhteydessä. Hyvä vaihtoehto sähköpostiositteeksi on esimerkiksi tietosuojavastaava@organisaatio.fi

Tietosuojavastaavan puhelinnumero *

Tietosuojavastaavan osoite *

Pajonko on yksi plus kaksi numerona? *

Kysymys on tehty osakopostiin esittämisellä.

Lähetä lomake

Liite 2: Muutos ilmoitukseen tietosuojavastaavasta -lomake

Muutos ilmoitukseen tietosuojavastaavasta

Rekisterinpitäjän tai henkilötietojen käsittelijän nimi *

Rekisterinpitäjäksi kutsutaan yritystä, viranomasta, yhteisöä tai henkilöä, joka määrittelee henkilötietojen käsittelyn tarkoituksen ja keinot. Henkilötietojen käsittelijäksi kutsutaan rekisterinpitäjistä ulkopuolista tahoa, joka käsittelee henkilötietoja rekisterinpitäjän puolesta.

Tietosuojavastaavailmoituksen diaarinumero

Muutos tietosuojavastaavan tietoihin

Tietosuojavastaavan nimi

Tietosuojavastaavan nimen ilmoittaminen on vapaaehtoista, mutta nimen ilmoittamista tietosuojavaltuutetun toimistolle pidetään suositeltavana yhteistyön helpottamiseksi. Tietosuojavastaavaksi ei saa nimetä henkilöä, jolla on eturistiriittoa.

Tietosuojavastaavan sähköpostiosoite

Sähköpostiosoitteen on hyvä olla sellainen, että välttämättä sujuvuus tietosuojavastaavan kanssa voidaan varmistaa aina, myös esimerkiksi poissaolojen ja henkilövaihdosten yhteydessä. Hyvä vaihtoehto sähköpostiosoitteeksi on esimerkiksi tietosuojavastaava@organisaatio.fi

Tietosuojavastaavan puhelinnumero

Tietosuojavastaavan osoite

Lisätietoja

Muutos rekisterinpitäjän tai henkilötietojen käsittelijän tietoihin

Sähköpostiosoite

Puhelinnumero

Osoite

Lisätietoja rekisterinpitäjistä

Muu muutos

Paljonko on yksi plus kaksi numerona? *

Kysymys on tehty roskapostin estämiseksi.

[Lähetä lomake](#)

Liite 3: Anmälan on dataskyddombud -blankett

Anmälan om dataskyddombud

Namnet på den personuppgiftsansvarige eller personuppgiftsbiträdet *

Med personuppgiftsansvarig avses ett företag, en myndighet, ett samfund eller en person som fastställer syftet och metoderna för behandling av personuppgifter. Med personuppgiftsbiträde avses en aktör som är utomstående i förhållande till den personuppgiftsansvarige, vilken behandlar personuppgifter för den personuppgiftsansvariges räkning.

Anmälan är *

- Personuppgiftsansvarig
 Personuppgiftsbiträde

FO-nummer

E-postadress *

Telefonnummer *

Adress *

Dataskyddombud anmäls *

- Utifrån dataskyddsförordningen
 Utifrån speciallagstiftningen
 Frivilligt

Ett dataskyddombud som utnämns frivilligt omfattas av samma krav på utnämninggrund, ställning och utgifter som ett ombud som utnämns på lagstadgat sätt.

Dataskyddombudets namn

Det är frivilligt att anmäla dataskyddombudets namn, men det rekommenderas att namnet meddelas till dataskyddombudens byrå för ett underlätta samarbetet. En person med intressekonflikter får inte utnämnas till dataskyddombud.

Dataskyddombudets e-postadress *

Det finns skäl att erbjuda adressen är sådan att ändligheten i kommunikationen med dataskyddombudet alltid kan säkerställas, också till exempel vid frånvaro och personalomsättning. Ett bra alternativ till e-postadress är till exempel dataskyddombud@organisation.fi.

Dataskyddombudets telefonnummer *

Dataskyddombudets adress *

Vad är ett plus två som siffror? *

Frågan ställa för ett undvika skräppost.

Liite 4: Ändring av anmälan om dataskyddsbud -blankett

Ändring av anmälan om dataskyddsbud

Namnet på den personuppgiftsskyldige eller personuppgiftsbiträdet *

Med personuppgiftsansvarig avses ett företag, en myndighet, ett samfund eller en person som fastställer syftet och metoderna för behandling av personuppgifter. Med personuppgiftsbiträde avses en aktör som är utomstående i förhållande till den personuppgiftsansvarige, vilken behandlar personuppgifter för den personuppgiftsansvariges räkning.

Diarienummer på anmälan om dataskyddsbud

Ändring i uppgifterna om dataskyddsbudet

Dataskyddsbudets namn

Det är frivilligt att anmäla dataskyddsbudets namn, men det rekommenderas att namnet meddelas till dataombudsmannens byrå för att underlätta samarbetet. En person med intrasskonflikter får inte utnåmnas till dataskyddsbud.

Dataskyddsbudets e-postadress

Det finns skäl att e-postadressen är sådan att omedelheten i kommunikationen med dataskyddsbudet alltid kan säkerställas, också till exempel vid frånvaro och personalomsättning. Ett bra alternativ till e-postadress är till exempel dataskyddsbud@organisation.fi.

Dataskyddsbudets telefonnummer

Dataskyddsbudets adress

Närmare uppgifter

Ändring av uppgifterna om den personuppgiftsskyldige eller personuppgiftsbiträdet

E-postadress

Telefonnummer

Adress

Närmare uppgifter

Annan ändring

Vad är ett plus två som siffra? *

Frågan ställs för att undvika skräppost.

Send form

Liite 5: Declaration of Data Protection Officer -form

Declaration of Data Protection Officer

Name of controller or processor *

A controller is a company, authority, community or person that defines the purposes and methods of processing personal data. A processor is a third-party processing personal data on behalf of a controller.

The notifier is *

- A controller
 A processor

Business ID

E-mail *

Telephone number *

Address *

The Data Protection Officer is being declared *

- By virtue of the GDPR
 By virtue of special legislation
 Voluntarily

The appointment basis, position and duties of Data Protection Officers appointed voluntarily are subject to the same requirements as those appointed on a statutory basis.

Name of Data Protection Officer

Declaring the name of the Data Protection Officer is voluntary, but communicating the name to the Office of the Data Protection Ombudsman is recommended to facilitate cooperation. Persons with conflicts of interest may not be appointed as Data Protection Officers.

E-mail address of the Data Protection Officer *

The email address should be one that enables uninterrupted communication with Data Protection Officer, also during absences and personnel changes. For example, dataprotectionofficer@organisation.fi would be a good choice.

Telephone number of the Data Protection Officer *

Address of the Data Protection Officer *

How much is one plus two (please enter a digit)? *

This question helps us to prevent spam.

Liite 6: Change to Data Protection Officer declaration -form

Change to Data Protection Officer declaration

Name of controller or processor *

A controller is a company, authority, community or person that defines the purposes and methods of processing personal data. A processor is a third-party processing personal data on behalf of a controller.

Record number of the Data Protection Officer declaration

Changes to the details of the Data Protection Officer

Name of Data Protection Officer

Declaring the name of the Data Protection Officer is voluntary, but communicating the name to the Office of the Data Protection Ombudsman is recommended to facilitate cooperation. Persons with conflicts of interest may not be appointed as Data Protection Officers.

E-mail address of the Data Protection Officer

The e-mail address should be one that enables uninterrupted communication with Data Protection Officer, also during absences and personnel changes. For example, dataprotectionofficer@organisation.fi would be a good choice.

Telephone number of the Data Protection Officer

Address of the Data Protection Officer

Additional information

Changes to the details of the controller or processor

E-mail address

Telephone number

Address

Additional information

Other change

How much is one plus two (please enter a digit)? *

This question helps us to prevent spam.

[Send form](#)

Liite 7:Vastauskirje



Vastaus ilmoitukseen tietosuojavastaavasta

Arvoisa vastaanottaja,

kiitos ilmoituksesta ja onnea tietosuojavastaavan nimittämisestä!

Tietosuojavaltuutetun toimisto on vastaanottanut ilmoituksesi ja kirjannut toimitetut tiedot tietosuojavastaavien rekisteriin. Tietosuojavaltuutetun toimisto ylläpitää valtakunnallista henkilörekisteriä sille ilmoitettuihin tietosuojavastaavista. Verkkosivuiltamme löydät tietoa [lähettämiesi tietojen käsittelystä](#) ja [oj-keuksista](#) muun muassa saada pääsy tietoihisi.

Jos tietosuojavastaava vaihtuu tai muut tiedot muuttuvat, ilmoita päivitetty tiedot tietosuojavaltuutetun toimistolle [muutoslomakkeella](#).

Tämä kirje on tarkoitettu organisaation johdolle ja tiedoksi annettavaksi myös nimitetyille tietosuojavastaavalle. Kirjeessä on tiivistetty tietoa ja ohjausta tietosuojavastaavan asemasta ja tehtävistä.

Tietosuojavastaavan asema ja tarvittavat resurssit

Tehtäväsi rekisterinpitäjänä tai henkilötietojen käsittelijänä on tukea tietosuojavastaavaa työssään. Tietosuojavastaavalla on oltava riittävästi työaikaa, -välineitä ja osaamista tehtävän suorittamiseen sekä mahdollisuus koulutusta.

Tietosuojavastaava hoitaa tehtäviään itsenäisesti, ja häntä sitoo salassapitovelvollisuus. Tietosuojavastaava voi hoitaa myös muita tehtäviä, kunhan rekisterinpitäjä ja henkilötietojen käsittelijä ovat varmistaneet, ettei siitä aiheudu eturistiriitoja.

Tietosuojavastaavan nimittäneen organisaation on noudatettava seuraavia periaatteita

- Tietosuojavastaava tai hänen tiiminsä on otettava mahdollisimman aikaisessa vaiheessa mukaan kaikkien tietosuojakysymysten käsittelyyn.
- Tietosuojavastaavalla on oltava mahdollisuus raportoida suoraan johdolle. Tietosuojavastaava kutsutaan säännöllisesti ylempään tai keskitason johdon kokouksiin.
- Kun tehdään päätöksiä, joilla on vaikutuksia tietosuojaan, tietosuojavastaavan suositellaan olevan paikalla. Kaikki olennaiset tiedot toimitetaan tietosuojavastaavalle viipymättä, jotta hän voi antaa asianmukaisia neuvoja.
- Tietosuojavastaavan näkemykselle annetaan aina asianmukainen painoarvo. Mahdollisissa erimielisyystilanteissa on hyvä dokumentoida perusteet, joiden vuoksi tietosuojavastaavan neuvoa ei noudateta.
- Jos tietoturvaloukkaus tai muu tietosuojaan liittyvä ongelma ilmenee, tietosuojavastaavaa kuullaan mahdollisimman nopeasti.

Tietosuojavastaavat eivät ole henkilökohtaisesti vastuussa yleisen tietosuoja-asetuksen rikkomisesta. Tietosuoja säännösten noudattaminen on rekisterinpitäjän tai henkilötietojen käsittelijän vastuulla.



Tietosuojavastaavan yhteystiedot yleisön saataville

Tietosuojavastaavan yhteystietojen on oltava suoraan ja helposti yleisön saatavilla. Rekisteröidyt voivat ottaa yhteyttä tietosuojavastaavaan kaikissa asioissa, jotka liittyvät heidän henkilötietojensa käsittelyyn tai [tietosuoja-asetukseen perustuvien oikeuksien](#) käyttöön. Tietosuojavastaavalla voi olla esimerkiksi oma asiakaspalvelunumero tai yhteydenottolomake organisaation verkkosivuilla.

Tietosuojavastaavan tehtävät

Tietosuojavastaava on organisaation sisäinen asiantuntija tietosuoja-asioissa sekä rekisteröityjen ja valvontaviranomaisen yhteyshenkilö. Tietosuojavastaavan on tehtäviään suorittaessaan otettava huomioon henkilötietojen käsittelytoimiin liittyvät riskit, käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset.

Tietosuojavastaava

- seuraa tietosuojasääntöjen noudattamista koko organisaatiossa ja tuo esiin havaitsemiaan puutteita
- antaa tietoja ja neuvoja tietosuojasääntöjen mukaisista velvollisuuksista johdolle ja henkilötietoja käsitteleville työntekijöille
- antaa pyydettyä neuvoja tietosuojan vaikutustenarvioinnin (DPIA) tekemisestä ja valvoo vaikutustenarvioinnin toteutusta
- on rekisteröityjen yhteyshenkilö henkilötietojen käsittelyyn liittyvissä asioissa
- tekee yhteistyötä valvontaviranomaisen kanssa ja toimii valvontaviranomaisen yhteyshenkilönä.

Rekisterinpitäjä ja henkilötietojen käsittelijä voivat halutessaan ulkoistaa tietosuojavastaavan tehtävän organisaation ulkopuoliselle palveluntarjoajalle.

Lue lisää:

Tietosuojavaltuutetun toimiston verkkosivut: [Tietosuojavastaavat](#)

[Tietosuoja-asetus](#): artikkelit 37–39, johdanto-osan kohta 97

[Tietosuojavastaavia koskevat ohjeet](#) (pdf)

[Usein kysytyt kysymykset: Tietosuojavastaavat](#) (pdf)

Liite 8: Svar



Svar på anmälan av dataskyddsbud

Bästa mottagare,

tack för anmälan och grattis till utnämningen av ett dataskyddsbud!

Dataombudsmannens byrå har tagit emot din anmälan och registrerat de överlämnade uppgifterna i registret över dataskyddsbud. Dataombudsmannens byrå administrerar ett riksomfattande personregister över dataskyddsbud som anmälts till byrån. På vår webbplats hittar du information om [behandlingen av de uppgifter som du lämnat in](#) och [dina rättigheter](#), bland annat om tillgången till dina uppgifter.

Om dataskyddsbudet byts eller om andra uppgifter ändras, vänligen meddela de uppdaterade uppgifterna till dataombudsmannens byrå med [ändringsblanketten](#).

Detta brev är avsett för organisationsledningen och för delgivning också till det utnämnda dataskyddsbudet. Brevet innehåller koncis information och handledning om dataskyddsbudets ställning och uppgifter.

Ställningen som dataskyddsbud och nödvändiga resurser

Din uppgift som personuppgiftsansvarig eller personuppgiftsbiträde är att stöda dataskyddsbudet i sitt arbete. Ett dataskyddsbud ska ha tillräckligt med arbetstid, arbetsredskap och kompetens samt möjlighet att utbildas sig för att utföra uppgiften.

Dataskyddsbudet sköter sina uppgifter på egen hand och han eller hon är bunden av tystnadsplikt. Dataskyddsbudet kan också sköta andra uppgifter, så länge som den personuppgiftsansvarige och personuppgiftsbiträdet förvissat sig om att detta inte leder till intressekonflikter.

Den organisation som utnämnt dataskyddsbudet ska iakta följande principer

- Dataskyddsbudet eller hans eller hennes team ska tas med i ett så tidigt skede som möjligt i all behandling av dataskyddsfrågor.
- Dataskyddsbudet ska ha en möjlighet att rapportera direkt till ledningen. Dataskyddsbudet kallas regelbundet till möten för ledningen på den översta nivån eller mellannivån.
- När beslut som inverkar på dataskyddet fattas, rekommenderas det att dataskyddsbudet är på plats. Alla väsentliga uppgifter överlämnas till dataskyddsbudet utan dröjsmål, så att ombudet kan ge ändamålsenliga råd.
- Dataskyddsbudets syn ska alltid ges behörig vikt. Vid eventuella meningsskiljaktigheter finns det skäl att dokumentera grunderna till att dataskyddsbudets råd inte följs.
- Om en dataskyddsincident eller ett annat problem som anknyter till dataskyddet uppkommer, ska dataskyddsbudet höras så fort som möjligt.

Dataskyddsbuden ansvarar inte personligen för brott mot den allmänna dataskyddsförordningen. Efterlevnaden av dataskyddsbestämmelserna ligger på den personuppgiftsansvariges och personuppgiftsbiträdets ansvar.

Dataombudsmannens byrå

PB 800, 00521 Helsingfors – tfn 020 566 6700 (växel) – tietosuoja@om.fi – www.tietosuoja.fi

Dataskyddsbudets kontaktuppgifter ska vara tillgängliga för allmänheten

Dataskyddsbudets kontaktuppgifter ska direkt och enkelt stå till allmänhetens förfogande. De registrerade kan ta kontakt med dataskyddsbudet i alla ärenden som gäller behandlingen av deras personuppgifter eller utövandet av rättigheter som grundar sig på dataskyddsförordningen. Ett dataskyddsbud kan ha till exempel ett eget kundbetjäningnummer eller ett kontaktformulär på organisationens webbsidor.

Dataskyddsbudets uppgifter

Dataskyddsbudet är organisationens interna expert på dataskyddsfrågor och kontaktperson för de registrerade och tillsynsmyndigheten. Dataskyddsbudet ska vid utförande av sina uppgifter beakta de risker som är förknippade med behandlingsåtgärder som gäller personuppgifter, behandlingens karaktär, omfattning, kontexten och syftena.

Dataskyddsbudet

- följer efterlevnaden av dataskyddsbestämmelserna i hela organisationen och lyfter fram brister som det upptäckt
- ger information och råd om skyldigheterna enligt dataskyddsbestämmelserna till ledningen och arbetstagare som behandlar personuppgifter
- ger på begäran råd om hur konsekvensbedömningen (DPIA) ska göras och övervakar genomförandet av denna
- är kontaktperson för de registrerade i ärenden som gäller behandling av personuppgifter
- samarbetar med tillsynsmyndigheten och fungerar som kontaktperson för tillsynsmyndigheten.

Den personuppgiftsansvarige och personuppgiftsbiträdet kan om de så önskar lägga ut uppgiften som dataskyddsbud på entreprenad till tjänstetillhandahållare utanför organisationen.

Läs mer:

Webbplatsen för dataombudsmannens byrå: [Dataskyddsbud](#)
[Dataskyddsförordningen](#): artiklarna 37–39, punkt 97 i introduktionsdelen
[Riktlinjer om dataskyddsbud](#) (pdf)

Liite 9: Reply



OFFICE OF
THE DATA PROTECTION OMBUDSMAN

1 (2)

Reply to Data Protection Officer declaration

Dear recipient,

thank you for your declaration and for designating a Data Protection Officer!

The Office of the Data Protection Ombudsman has received your declaration and entered the information in the register of Data Protection Officers. The Office of the Data Protection Ombudsman maintains a national personal data file of the Data Protection Officers communicated to it. Our website contains information [on the processing of the data you submitted to us](#) and [your rights](#), such as the right of access to personal data concerning you.

If the Data Protection Officer or his or her contact details change, communicate the changes to the Office of the Data Protection Ombudsman with the [change form](#).

This letter is addressed to the management of the organisation and for the information of the designated Data Protection Officer. The letter contains information and advice on the position and duties of the Data Protection Officer in a concise form.

Position of the Data Protection Officer and the required resources

As a controller or processor, your duty is to support the Data Protection Officer in his or her work. The Data Protection Officer must be provided with sufficient time, tools and competencies for performing his or her duties and with a chance to obtain training.

The Data Protection Officer performs his or her duties independently and is bound by a secrecy obligation. The Data Protection Officer can also have other duties, as long as the controller and processor have ensured that they will pose no conflicts of interest.

The organisation that designated the Data Protection Officer is required to observe the following principles

- The Data Protection Officer or his or her team shall be involved in the handling of all questions related to data protection at the earliest stage possible.
- The Data Protection Officer must have the possibility to report directly to the management. The Data Protection Officer shall be regularly invited to high- and mid-level meetings.
- The Data Protection Officer should be present when decisions affecting data protection are made. All relevant information shall be delivered to the Data Protection Officer immediately so that he or she can give appropriate advice.
- The opinion of the Data Protection Officer shall be given the appropriate weight. In case of a difference of opinion, the grounds on which the advice of the Data Protection Officer was not followed should be documented.
- The Data Protection Officer shall be consulted as soon as possible on any personal data breaches or other issues concerning data protection.

Data Protection Officers are not personally responsible for infringements of the General Data Protection Regulation. Compliance with data protection regulations is the responsibility of the controller or processor.

Office of the Data Protection Ombudsman

P.O. Box 800, 00521 Helsinki, Finland – tel. +358 29 566 8700 (switchboard) – tietosuoja@om.fi – www.tietosuoja.fi

Public availability of the Data Protection Officer's contact details

The Data Protection Officer's contact details must be directly and easily accessible to the public. Data subjects can contact the Data Protection Officer in all matters related to the processing of their personal data or the exercise of rights based on the GDPR. For example, the Data Protection Officer can have a dedicated customer service telephone number or contact form on the company's website.

Tasks of the Data Protection Officer

The Data Protection Officer is the organisation's internal expert in matters involving data protection and the contact person for data subjects and the supervisory authority. In the course of his or her duties, the Data Protection Officer is required to take into account the risks involved in processing activities as well as the scope, context and purposes of the processing.

The Data Protection Officer

- monitors compliance with data protection rules across the organisation and highlights any deficiencies
- provides management and the employees that process personal data with information and advice on their duties specified in the data protection rules
- gives advice on carrying out the data protection impact assessment (DPIA) and monitors its implementation
- serves as the contact person for data subjects in matters related to the processing of personal data and
- cooperates with the supervisory authority and serves as its contact person.

The controller and processor are free to outsource the duties of the Data Protection Officer to an external service provider.

Read more:

Website of the Office of the Data Protection Ombudsman: [Data Protection Officers](#)
[General Data Protection Regulation](#); Articles 37–39, recital 97
[Guidelines on Data Protection Officers](#) (pdf)