EUROOPAN UNIONIN YLEISEN TIETOSUOJA-ASETUKSEN SOPIMUSVAATIMUKSISTA JOHTUVAT YRITYSVAIKUTUKSET

Niina Tukia
Lapin yliopisto
Oikeustieteiden tiedekunta
Pro Gradu - tutkielma
2019

Lapin yliopisto, oikeustieteiden tiedekunta

Työn nimi: Yleisen tietosuoja-asetuksen sopimusvaatimuksista johtuvat yritysvaikutukset
Tekijä: Niina Tukia
Opintokokonaisuus ja oppiaine: Kauppaoikeus
Työn laji: Tutkielma X Laudaturtyö __ Lisensiaattityö __ Kirjallinen työ __
Sivumäärä: XIV + 93 + liitteet xvii
Vuosi: 2019

Tiivistelmä

Tietojenkäsittelysopimusten päivittäminen, uusien neuvotteleminen, valvonta ja hallinta vaativat yrityksiltä huomattavaa perehtymistä ja tietotaitoa. EU:n yleisen tietosuoja-asetuksen Sopimusvaatimusten noudattaminen aiheuttaa siten merkittäviä vaikutuksia yritysten toiminnalle. Tässä tutkielmassa selvitetään mainitun tietosuoja-asetuksen artikla 28 asettamien sopimusvaatimusten keskeisimmät yritysvaikutukset Suomessa toimiville yrityksille. Lisäksi, tutkielmassa kartoitetaan, miksi yritysvaikutusten vaikutusarvioinnit ovat tärkeä osa lainsäädäntöhankkeiden valmistelua ja täytäntöönpanoa, sekä selvitetään tutkielmalle soveltuvin osin tietosuoja-asetuksesta tehtyjen vaikutusarviointien ja jälkiseurannan tuloksia. Tutkielman ohessa toteutettiin myös kyselytutkimus sopimusvaatimusten vaikutuksista Suomessa toimiville yrityksille.

Tutkielman tutkimusmetodi oli oikeusdogmaattinen eli lainopillinen. Lainopillinen tutkimusmenetelmä toimi niin sanottuna pääasiallisena tutkimusmenetelmänä, jonka rinnalla tutkielmassa hyödynnettiin täydentävinä menetelminä empiiristä tutkimusmenetelmää, sekä soveltuvin osin sääntelyteoriaa. Tutkielman pääasialliset lähteet koostuivat aihetta käsittelevästä lainsäädännöstä, oikeuskirjallisuudesta, artikkeleista, hallituksen ja Euroopan komission esityksistä ja selvityksistä, sekä oikeuskäytännöstä ja asiantuntijalausunnoista. Näin pyrittiin saamaan kattava selvitys Sopimusvaatimusten tämän hetken velvoittavuudesta Suomessa toimiville yrityksille. Tutkielma pohjautui siten voimassa olevaan lainsäädäntöön. Tutkielman johtopäätösten kannanotot Sopimusvaatimusten tosiasiallisista vaikutuksista perustuivat suurissa määrin tutkielman kyselytutkimukseen osallistuneiden yritysten antamiin vastauksiin sekä viranomaisten toteuttamiin selvityksiin tietosuoja-asetuksen vaikutuksista.

Selvitysten perusteella sopimusvaatimukset kuormittivat Suomessa toimivien yritysten toimintaa ja kasvattivat yrityksiin kohdistunutta hallinnollista taakkaa ja compliance-kustannuksia. Tietojenkäsittelysopimuksia koskevat sopimusneuvottelut ilmoitettiin olevan aikaa vieviä ja pitkiä prosesseja, sekä rekisterinpitäjä-käsittelijäsuhteiden määrittely aiheutti runsaasti epäselvyyttä. Lisäksi, yritysten vanhojen sopimusten päivittäminen sopimusvaatimuksia vastaaviksi koettiin työlääksi. Tietosuoja-asetuksen ja sopimusvaatimusten yritysvaikutukset ovat selvitysten valossa merkittäviä, joiden kustannukset yrityksille ovat luultavasti huomattavia. Tutkielman rajallisuudesta johtuen, saaduista tuloksista ei ole kuitenkaan tehtävissä yleistettävissä olevia johtopäätöksiä. Jotta Sopimusvaatimusten vaikutukset kilpailukykyyn ja markkinoiden toimivuuteen voitaisiin selvittää riittävällä tasolla, toteutuneiden yritysvaikutusten selvittäminen vaatisi kattavampaa määrällistä selvitystä.

Avainsanat:
yleinen tietosuoja-asetus, henkilötietojen käsittely, henkilötietojen käsittelijä, tietosuoja, vaikutusarviointi, yritysvaikutus, sopimusvaatimukset, tietojenkäsittelysopimus.

Muita tietoja: (vain Lappia koskevat)
Suostun tutkielman luovuttamiseen Rovaniemen hovioikeuden käyttöön X
Suostun tutkielman luovuttamiseen kirjastossa käytettäväksi X
Suostun tutkielman luovuttamiseen Lapin maakuntakirjastossa käytettäväksi X

SISÄLLYS

LÄHTEET

Kirjallisuus ja artikkelit

Aalto-Setälä, Minna – Viitaila, Mikko: Tietosuoja pähkinänkuoressa. Tietosuojaopas yrityksille. Helsinki 2018.

Baldwin, Robert – Cave, Martin – Lodge, Martin: Understanding Regulation: theory, strategy and practise. Oxford University Press 2012.

Enroth, Timo – Neuvonen, Riku: EU:n tietosuoja-asetuksen (EU 2016/679) yritysvaikutukset. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 41/2017. Helsinki 2017. *(Valtioneuvoston selvitys 2017)*

Erlund, Kai – Lilja, Johanna – Lindfors, Arto – Salminen, Janne – Turunen, Jaakko: IT2018 – Käytännön käsikirja. Viro 2019.

Ervasti, Kaijus: Empiirinen oikeustutkimus. Teoksessa: Oikeuspoliittisen tutkimuslaitoksen tutkimustiedonantoja 64, Empiirinen tutkimus oikeustieteessä, toim. Heidi Lindfors, Helsinki 2004, s. 9-15.

Harjunheimo, Niina: Muistio eduskunnan hallintovaliokunnalle; (U 21/2012) valtioneuvoston jatkokirjelmä eduskunnalle ehdotuksesta yleiseksi tietosuoja-asetukseksi. Elinkeinoelämän keskusliitto EK ry 2015. *(Elinkeinoelämän keskusliitto 2015)*

Heikinsalmi, Minna: Kilpailunrikkomismaksu kartellitapauksissa Suomessa, määräytymisperusteet ja seuraamusmaksun taso. Kilpailuviraston selvityksiä 1/2009. Helsinki 2009.

Henriksson, Anu: Yritystoiminta Helsingissä, Tilastoja 2018:17. Helsinki 2018.

Huikko, Katariina - Hämäläinen, Jukka - Juntunen, Pauliina - Lehto, Karolina - Sulin, Ida: Tietosuoja-asetuksen huomioiminen kilpailutettaessa julkisia hankintoja. Versio 1.0 Toukokuu 2017. *(Huikko ym. 2017)*

Kainulainen, Heini: Teemahaastattelut kriminologisessa tutkimuksessa. Teoksessa: Oikeuspoliittisen tutkimuslaitoksen tutkimustiedonantoja 64, Empiirinen tutkimus oikeustieteessä, toim. Heidi Lindfors, Helsinki 2004, s. 16–26.

Kangasharju, Aki – Rauhanen, Timo: Lainsäädännön hallinnollinen taakka yrityksille – raskaimmat säädösalueet. Työ- ja elinkeinoministeriön julkaisuja, Kilpailukyky, 13/2008. Helsinki 2008.

Keinänen, Anssi – Halonen, Miia: Mikä vaivaa vaikutusten arviointia? – Vaikutusten arvioinnin puutteet lainsäädännön arviointineuvoston havaitsemana ja lausuntojen huomioiminen hallituksen esityksissä. Edilex 2017, s. 6-14.

Keinänen, Anssi – Lonka, Harriet – Pajuoja, Jussi – Vartiainen, Niko – Tuominen, Risto – Halonen, Miia – Koskela, Tarja: Lainsäädännön arviointineuvoston toiminnan vaikuttavuuden arviointi. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 2019:12. Helsinki 2019. *(Valtioneuvoston selvitys 2019)*

Korkea-aho, Emilia: Empiirisen oikeustutkimuksen käytäntö. Teoksessa: Oikeuspoliittisen tutkimuslaitoksen tutkimustiedonantoja 64, Empiirinen tutkimus oikeustieteessä, toim. Heidi Lindfors, Helsinki 2004, s. 81–90.

Korpisaari, Päivi – Pitkänen, Olli – Warma-Lehtinen, Eija: Uusi tietosuojalainsäädäntö. Alma Talent. Helsinki 2018.

Lång, Jukka – Taka, Anni-Maria: Personal Data – Finland. Ius Laboris, 7.6.2019.

Lång, Jukka: EU:n yleisen tietosuoja-asetuksen vaikutukset suomalaisiin yrityksiin. Dittmar & Indrenius; Oikeusministeriön pyytämä selvitys. Helsinki 2016.

Moerel, Lokke: CNIL's decision fining Google violates one-stop-shop. 19.2.2019.

Mäenpää, Olli: Asiantuntijalausunto EDK-2018-AK-178898; Hallituksen esitys EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi (HE 9/2018vp). Helsinki 2018.

Määttä, Kalle:

- Oikeustaloustieteen perusteet. 2. uudistettu painos. Helsinki 2016.
- Elinkeinotoiminnan sääntelystä Suomessa. Edilex 2011, s. 25–28.
- Mihin indeksiehtolakia tarvitaan? Kansantaloudellinen aikakauskirja – 99. vsk. – 1/2003, s. 72–77.

Määttä, Tapio: Metodinen pluralismi oikeustieteessä – ympäristöoikeudellisen tutkimuksen suuntaukset ja menetelmät. Edilex 2015.

Sulin, Ida – Tainio, Hanna: Suomen Kuntaliiton yleiskirje (14/2017) kunnan- ja kaupunginhallituksille yleisestä tietosuoja-asetuksesta. Helsinki 2017.

Tala, Jyrki: Lainvalmistelu ja sääntelyn vaihtoehdot. Helsinki 2012.

Talus, Anu - Autio, Elina - Hänninen, Anna - Pihamaa, Heljä-Tuulia – Kantonen, Silja: Miten valmistautua EU:n tietosuoja-asetukseen? Oikeusministeriön julkaisu 4/2017. Helsinki 2017. *(Talus ym. 2017)*

Tohmo, Timo – Littunen, Hannu: Toimialoittainen keskittyminen ja siinä tapahtuneet muutokset Suomen teollisuudessa vuosina. Kansantaloudellinen aikakauskirja – 99. vsk. – 4/2003, s. 424–430.

Warma, Eija – Nieminen, Jussi: Tietosuoja ja kilpailuoikeus – määräävässä markkina-asemassa olevan yrityksen toimitusvelvollisuudesta ja tietosuojalainsäädännöstä. Defensor Legis 4/2016, s. 549 – 569.

Wasastjerna, Maria: Blurred lines: the German Facebook case and the interlink between competition law and data protection. Kilpailuoikeudellinen vuosikirja 2018, Vantaa 2019, s. 23–34.

Wennäkoski, Anna Aurora: Tietosuojaoikeudellinen vahingonkorvaus murroksessa. Edilex 2017, s. 68–93.

Virallisaineisto

Finanssivalvonta: Hallinnollisten sakkojen ja seuraamusmaksujen vakuuttamiskelpoisuus. Tulkinta 16.10.2018 – 2/2018 (FIVA 3/01.02/2018). *(Finanssivalvonta 2018)*

HaVL 25/2015 vp: Valtioneuvoston kirjelmä eduskunnalle ehdotuksesta asetukseksi yksilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta (Yleinen tietosuoja-asetus) sekä direktiiviksi yksilöiden suojelusta toimivaltaisten viranomaisten henkilötietojen käsittelyssä rikosten torjumiseksi, tutkimiseksi, selvittämiseksi tai niistä syyttämiseksi tai rikosoikeudellisten seuraamusten täytäntöönpanemiseksi ja näiden tietojen vapaasta liikkuvuudesta (Tietosuojadirektiivi).

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

Kilpailu- ja kuluttajavirasto: Kilpailun ja kuluttajansuojan kysymyksiä datataloudessa. Kilpailu- ja kuluttajaviraston selvityksiä 1/2019. Helsinki 2019.

Työ- ja elinkeinoministeriö: Selvitys yritysten hallinnollisen taakan kehityksestä. TEM raportteja 15/2012. Helsinki 2012. *(Työ- ja elinkeinoministeriö 2012)*

Valtiontalouden tarkastusvirasto: Tarkastuskertomus 18/2012, Hallituksen lainsäädäntösuunnitelma. Jälkiseurantaraportti - Dnro 045/54/2011. Helsinki 2018.

Euroopan komissio:

Better regulation "Toolbox" (SWD (2017) 350). Bryssel 2017. *(Euroopan komissio- Toolbox)*

COM (2016) 615, lopull. Komission tiedonanto Euroopan parlamentille, Eurooppa neuvostolle ja neuvostolle, 14.9.2016. Parempi sääntely: paremmilla tuloksilla saadaan aikaan vahvempi unioni. Bryssel 2016. *(COM (2016) 615, lopull.)*

COM (2018) 43, lopull. Komission tiedonanto Euroopan parlamentille ja neuvostolle, 24.1.2018. Vahvempi suoja, uudet mahdollisuudet – komission ohjeet yleisen tietosuoja-asetuksen suorasta soveltamisesta 25. toukokuuta 2018 lähtien. Bryssel 2018. *(COM (2018) 43, lopull.)*

COM (2019) 374, lopull. Komission tiedonanto Euroopan parlamentille ja neuvostolle, 24.7.2019. Tietosuojasäännöt luottamuksen rakentajana EU:ssa ja sen ulkopuolella – tilannekatsaus. Bryssel 2019. *(COM (2019) 374, lopull.)*

Commission Staff Working Document, Better Regulation Guidelines (SWD (2017) 350). Bryssel 2017. *(Euroopan komissio - Better Regulation Guidelines)*

Erityisbarometri 487a. Bryssel 2019. Saatavissa: https://tietosuoja.fi/documents/6927448/10882171/Erityiseurobarometri+487+a+Suomi (Luettu 9.7.2019). *(Euroopan komission erityisbarometri 2019b)*

How the EU determines if a non-EU country has an adequate level of data protection. Bryssel 2019. *(Euroopan komission päätös tietosuojan tason riittävyydestä 2019)*

Keynote Speech by European Commissioner *Jourová* at the University of Chile: "EU-Chile: Challenges and Opportunities in the Digital Era. Shared values and common responses". Päivitetty 17.10.2019. Saatavissa: https://europa.eu/rapid/press-release_SPEECH-19-3991_en.htm (Luettu 9.7.2019). *(Jourová 2019)*

Komission asiantuntijaryhmä: Report – contribution from the Multistakeholder Expert Group to the stock-taking exercise of June 2019 on one year of GDPR application. 11.6.2019. Saatavissa:

https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=31527 (Luettu 10.8.2019). *(Komission asiantuntijaryhmän raportti 2019)*

Komission asiantuntijaryhmien ja muiden vastaavanlaisten elinten rekisteri. Päivitetty 5.8.2019. Saatavissa: https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3537&NewSearch=1&NewSearch=1&Lang=FI (Luettu 10.8.2019). *(Komission asiantuntijaryhmä 2019)*

Komission asiantuntijaryhmien ja muiden vastaavanlaisten elinten rekisteri / Report from the Multistakeholder Expert Group on the GDPR application and the Annex (Questionnaire used). 11.6.2019. Saatavissa: https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeeting&meetingId=15670 (Luettu 10.8.2019). *(Komission asiantuntijaryhmälle tehty selvitys 2019)*

Mitä sääntöjä sovelletaan, jos yritys siirtää tietoja EU:n ulkopuolelle? 2017. Saatavissa: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-rules-apply-if-my-organisation-transfers-data-outside-eu_fi (Luettu 5.8.2019). *(Euroopan komission suojatoimet 2019)*

SEC (2012) 72, lopull. Commission Staff Working Paper, Impact Assessment Accompanying the Document: Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) and Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data. 25.1.2012. *(SEC (2012) 72, lopull.)*

Special Eurobarometer 487a – Data annex. Bryssel 2019. Saatavissa: https://tietosuoja.fi/documents/6927448/10882171/Special+Eurobarometer+487a+EN.pdf (Luettu 9.7.2019). *(Euroopan komission erityisbarometri 2019a)*

Special Eurobarometer 487a – Report. Bryssel 2019. Saatavissa: https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/survey/getsurveydetail/instruments/special/surveyky/2222 (Luettu 20.6.2019). *(Euroopan komission erityisbarometri 2019c)*

Standard Contractual Clauses (SCC). Bryssel 2019. Saatavissa: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en (Luettu 8.9.2019). *(Euroopan komissio (SCC) 2019)*

Oikeusministeriö:

Vaikutusten arviointi. 2019. Saatavissa: https://oikeusministerio.fi/vaikutusten-arviointi (Luettu 9.7.2019). *(Oikeusministeriö 2019)*

Hallituksen esitysten laatimisohjeet, HELO-työryhmän mietintö. Selvityksiä ja ohjeita 49/2018. Helsinki 2018. *(Oikeusministeriö 2018)*

EU:n yleinen tietosuoja-asetus; kolmansien maiden tietosuojan riittävyyttä koskevat päätökset. Perusmuistio OM2018-00505, Helsinki 2018. *(Oikeusministeriön perusmuistio (OM2018-00505)) 2018)*

Eduskunnan ja valtioneuvoston yhteistoiminta Euroopan unionin asioiden kansallisessa valmistelussa. Selvityksiä ja ohjeita 57/2011. Helsinki 2012. *(Oikeusministeriö 2011)*

Oikeusministeriön EU-valmistelun opas. Toiminta ja hallinto 79/2010. Helsinki 2010. *(Oikeusministeriö 2010)*

Säädösehdotusten vaikutusten arviointi, ohjeet. Oikeusministeriön julkaisu 2007:6. Helsinki 2007. *(Oikeusministeriö 2007)*

Lainsäädännön arviointineuvosto:

Aloite valtioneuvoston kanslialle lainsäädännön jälkiarviointijärjestelmän luomiseksi. Helsinki 2019. *(Lainsäädännön arviointineuvosto 2019)*

Lainsäädännön arviointineuvoston vuosikatsaus 2018. Helsinki 2019. *(Lainsäädännön arviointineuvosto 2018)*

Lainsäädännön arviointineuvoston vuosikatsaus 2017. Helsinki 2018. *(Lainsäädännön arviointineuvosto 2017)*

Lainsäädännön arviointineuvoston vuosikatsaus 2016. Helsinki 2017. *(Lainsäädännön arviointineuvosto 2016)*

Lainsäädännön arviointineuvoston lausunto luonnoksesta hallituksen esitykseksi eduskunnalle EU:n yleistä tietosuoja-asetusta täydentäväksi yleiseksi lainsäädännöksi. Lausunto Dnro: VNK/133/32/2018. Helsinki 2018. *(Lainsäädännön arviointineuvoston lausunto (VNK/133/32/2018))*

Lainsäädännön arviointineuvoston lausunto luonnoksesta esitykseksi eduskunnalle yrittäjävähennyksen säätämiseksi. Lausunto Dnro: VNK/1644/03.02.00/2016. Helsinki 2016. *(Lainsäädännön arviointineuvoston lausunto (VNK/1644/03.02.00/2016))*

Lainsäädännön arviointineuvoston lausunto luonnoksesta hallituksen esitykseksi eduskunnalle laeiksi sairasvakuutuslain, lääkelain 57 b ja 102 §:n sekä terveydenhuollon ammattihenkilöstöstä annetun lain 22 ja 23 §:n muuttamisesta. Lausunto Dnro: VNK/1641/03.02.00/2016. Helsinki 2016. *(Lainsäädännön arviointineuvoston lausunto (VNK/1641/03.02.00/2016))*

Lainsäädännön arviointineuvoston lausunto luonnoksesta hallituksen esitykseksi eduskunnalle laiksi valtion yhtiöomistuksesta ja omistajaohjauksesta annetun lainmuuttamisesta. Lausunto Dnro: VNK/1581/30/2016. Helsinki 2016. *(Lainsäädännön arviointineuvoston lausunto (VNK/1581/30/2016))*

Lainsäädännön arviointineuvoston lausunto luonnoksesta hallituksen esitykseksi eduskunnalle liikennekaaresta. Lausunto Dnro: VNK/1189/03.02.00/2016. Helsinki 2016. *(Lainsäädännön arviointineuvoston lausunto (VNK/1189/03.02.00/2016))*

Tietosuojaviranomaisten tuottama aineisto

Euroopan tietosuojaneuvosto:

First overview on the implementation of the GDPR and the roles and means of the national supervisory authorities – 26.2.2019. Saatavissa: http://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2019/02-25/9_EDPB_report_EN.pdf (Luettu 2.4.2019). *(Euroopan tietosuojaneuvoston katsaus 2019)*

Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation - version 3.0. 4.6.2019. *(EDPB Guidelines (1/2018) 2019)*

Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679 - version 2.0. 4.6.2019. *(EDPB Guidelines (1/2019) 2019)*

Tietoa Euroopan tietosuojaneuvostosta. Saatavissa: https://edpb.europa.eu/about-edpb/about-edpb_fi (Luettu 1.8.2019). *(Euroopan tietosuojaneuvosto 2019)*

Tietosuojatyöryhmä:

Esimerkkejä henkilötietojen tietoturvaloukkauksista ja siitä, kenelle niistä ilmoitetaan. Bryssel 2019. Saatavissa: https://tietosuoja.fi/documents/6927448/8214536/Esimerkkej%C3%A4+tietoturvaloukkauksista (Luettu 9.4.2019). *(Tietosuojatyöryhmä 2019)*

Article 29 Data Protection Working Party: Guidelines on consent under Regulation 2016/679. WP259 rev.01. Bryssel 2018. *(Article 29 Working Party 2017)*

Ohjeet tietosuojaa koskevasta vaikutustenarvioinnista ja keinoista selvittää ”liittyykö käsittelyyn todennäköisesti” asetuksessa (EU) 2016/679 tarkoitettu "korkea riski". Bryssel 2017. *(Tietosuojatyöryhmä 2017)*

Lausunto 1/2010 rekisterinpitäjän ja henkilötietojen käsittelijän käsitteistä. Bryssel 2010. *(Tietosuojatyöryhmä 2010)*

Information Commissioner`s Office:

Intention to fine British Airways £183.39m under GDPR for data breach. Päivitetty 8.7.2019. Saatavissa: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-announces-intention-to-fine-british-airways/ (Luettu 13.8.2019). *(ICO – British Airways 2019)*

Intention to fine Marriott International, Inc. more than £99 million under GDPR for data breach. Päivitetty 9.7.2019. Saatavilla: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/intention-to-fine-marriott-international-inc-more-than-99-million-under-gdpr-for-data-breach/ (Luettu 13.8.2019). *(ICO – Marriot 2019)*

Tietosuojavaltuutetun toimisto:

Tietosuojavaltuutetun päätös. Henkilötietojen rekisterinpitäjästä ja käsittelijästä. Diaarinumero: 5036/183/2019. Annettu 2.9.2019. *(Tietosuojavaltuutetun päätös (5036/183/2019) 2019)*

Apulaistietosuojavaltuutetuiksi Anu Talus ja Jari Råman. Päivitetty 25.4.2019. Saatavissa: https://tietosuoja.fi/artikkeli/-/asset_publisher/apulaistietosuojavaltuutetuiksi-anu-talus-ja-jari-raman (Luettu 29.5.2019). *(Tietosuojavaltuutetun toimiston tiedote 2019)*

Ennakkokuuleminen. 2019. Saatavissa: https://tietosuoja.fi/ennakkokuuleminen (Luettu 6.4.2019). *(Tietosuojavaltuutetun toimisto 2019d)*

Euroopan tietosuojaneuvoston ohjeet. Saatavissa: https://tietosuoja.fi/euroopan-tietosuojaneuvoston-ohjeet (Luettu 15.8.2019). *(Euroopan tietosuojaneuvoston ohjeet 2019).*

Milloin henkilötietoja saa käsitellä? 2019. Saatavissa: https://tietosuoja.fi/kasittelyperusteet (Luettu 6.4.2019). *(Tietosuojavaltuutetun toimisto 2019b)*

Mitä oikeuksia rekisteröidyllä on eri tilanteissa. 2019. Saatavissa: https://tietosuoja.fi/rekisteroidyn-oikeudet-eri-tilanteissa (Luettu 6.4.2019). *(Tietosuojavaltuutetun toimisto 2019a)*

Osoita noudattavasi tietosuojasäännöksiä. 2019. Saatavissa: https://tietosuoja.fi/osoitusvelvollisuus (Luettu 8.4.2019). *(Tietosuojavaltuutetun toimisto 2019c)*

Reijo Aarnion blogi: Mitä GDPR:n jälkeen? Päivitetty 4.6.2018. Saatavissa: https://tietosuoja.fi/artikkeli/-/asset_publisher/mita-gdpr-n-jalkeen- (Luettu 20.4.2019). *(Aarnio 2018)*

Reijo Aarnion blogi: Seuraamuksista 2.Päivitetty 30.11.2016. Saatavissa: https://tietosuoja.fi/artikkeli/-/asset_publisher/seuraamuksista-2 (Luettu 20.4.2019). *(Aarnio 2016)*

Reijo Aarnion blogi: Totuus hallinnollisista sanktioista. Päivitetty 1.3.2017. Saatavissa: https://tietosuoja.fi/artikkeli/-/asset_publisher/totuus-hallinnollisista-sanktioista (Luettu 20.4.2019). *(Aarnio 2017)*

Tietosuojavaltuutetun päätös luetteloksi käsittelytoimista, joiden yhteydessä on tehtävä vaikutustenarviointi. Päivitetty 21.12.2018. Saatavissa: https://tietosuoja.fi/luettelo-vaikutustenarviointia-edellyttavista-kasittelytoimista (Luettu 8.4.2019). *(Tietosuojavaltuutetun toimisto 2018b)*

Tietosuojavaltuutetun toimiston toimintakertomus 2018. Helsinki 2019. Saatavissa: https://tietosuoja.fi/documents/6927448/10717840/Toimintakertomus+2018 (Luettu 9.7.2019). *(Tietosuojavaltuutetun toimisto 2018a)*

Tietoturvaloukkaukset. 2019. Saatavissa: https://tietosuoja.fi/tietoturvaloukkaukset (Luettu 7.4.2019). *(Tietosuojavaltuutetun toimisto 2019e)*

Vaikutustenarviointi. 2019. Saatavissa: https://tietosuoja.fi/fi/vaikutustenarviointi (Luettu 7.4.2019). *(Tietosuojavaltuutetun toimisto 2019f)*

Oikeustapaukset

Kansalliset tuomioistuimet

KHO 2018:112

Euroopan unionin tuomioistuin

C-507/17 *Google v CNIL - Commission Nationale de l'Informatique et des Libertés* ECLI:EU:C:2019:772

C-40/17 *Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV Oberlandesgericht Düsseldorf* ECLI:EU:C:2019:629

C-25/17 *Tietosuojavaltuutettu v Jehovan todistajat — uskonnollinen yhdyskunta* ECLI:EU:C:2018:551

C-210/16 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein vastaan Wirtschaftsakademie Schleswig-Holstein GmbH* ECLI:EU:C:2018:388

Euroopan komissio

M.8179 *Canon / Toshiba Medical Systems Corporation* (Art. 14(2) Procedure)

Internet-aineisto

Acubiz: Compliance as a competitive advantage or a risk factor? 2019. Saatavissa: https://www.acubiz.com/compliance-as-a-competitive-advantage-or-a-risk-factor/(Luettu 15.7.2019).

Castrén & Snellman: Mikko-Pekka Partasen blogi: Täyttävätkö yrityksesi palvelusopimukset tietosuoja-asetuksen vaatimukset? Päivitetty 1.3.2018. Saatavissa: https://www.castren.fi/fi/blogijauutiset/blogi-2018/tayttavatko-yrityksesi-palvelusopimukset-tietosuoja-asetuksen-vaatimukset/ (Luettu 15.7.2019). *(Partanen 2018)*

Eduskunta - Erika Bergström: Ruotsi – oikeudellisia tiedonlähteitä. Päivitetty 21.2.2019. Saatavissa: https://www.eduskunta.fi/FI/tietoaeduskunnasta/kirjasto/aineistot/ulkomainen_oikeus/Sivut/Ruotsi.aspx (Luettu 18.6.2019). *(Eduskunta 2019b)*

Eduskunta: Lainsäädäntö. 2019. Saatavissa: https://www.eduskunta.fi/FI/tietoaeduskunnasta/kirjasto/aineistot/kotimainen_oikeus/kotimaiset-oikeuslahteet/Sivut/Lainsaadanto.aspx (Luettu 13.1.2019). *(Eduskunta 2019a)*

Elinkeinoelämän keskusliitto: Nyyssölä bloggaa: Tietosuoja-asetus tuo työnantajille käännetyn todistustaakan. Päivitetty 16.11.2017. Saatavissa: https://ek.fi/blogi/2017/11/16/nyyssola-bloggaa-tietosuoja-asetus-tuo-tyonantajille-kaannetyn-todistustaakan/ (Luettu 5.7.2019). *(Nyyssölä 2017)*

Elinkeinoelämän keskusliitto: Tietopaketti yrityksille: EU:n yleinen tietosuoja-asetus ja tietosuojalaki. 2019. Saatavissa: https://ek.fi/mita-

teemme/yrityslainsaadanto/tietosuojalainsaadanto/tietopaketti-yrityksille-on-aika-valmistautua-eun-yleiseen-tietosuoja-asetukseen/#5-2--Rekisterinpit-j-n-velvollisuudet (Luettu 13.9.2019). *(Elinkeinoelämän keskusliitto 2019)*

Finanssiala: Henkilötietojen käsittelyä finanssialalla koskevat käytännesäännöt. Helsinki 2017. Saatavissa: http://www.hypo.fi/wp-content/uploads/2018/05/Finanssilala_Henkil%C3%B6tietojen-k%C3%A4sittely%C3%A4-finanssialalla-koskevat-k%C3%A4yt%C3%A4nnes%C3%A4%C3%A4nn%C3%B6t_01122017.pdf (Luettu 1.9.2019).

Finlex-julkaisut: Lainvalmistelun prosessiopas. 2013. Saatavissa: http://lainvalmistelu.finlex.fi/taytantoonpano/#esittely (Luettu 13.1.2019). *(Lainvalmistelun prosessiopas 2013)*

Heise online – *Joerg, Heidrich*: DSGVO: 5000 Euro Bußgeld für fehlenden Auftragsverarbeitungsvertrag. Päivitetty 20.1.2019. Saatavissa: https://www.heise.de/newsticker/meldung/DSGVO-5000-Euro-Bussgeld-fuer-fehlenden-Auftragsverarbeitungsvertrag-4282737.html (Luettu 5.8.2019). *(Kolibri Image Regina und Dirk Maass GbR vs Data Protection Authority of Hamburg 2019)*

i-SCOOP: GDPR and approved codes of conduct – demonstrating compliance. 2019. Saatavissa: https://www.i-scoop.eu/gdpr/gdpr-codes-conduct/ (Luettu 1.6.2019).

Korkein oikeus: Oikeudenkäyntimenettelyä koskevia periaatteita. 2014. Saatavissa: https://korkeinoikeus.fi/fi/index/muutoksenhakijalle/oikeudenkayntimenettelyakoskeviaperiaatteita.html (Luettu 4.7.2019). *(Korkein oikeus 2019)*

Lausuntopalvelu.fi: Lausuntopyyntö yleisen tietosuoja-asetuksen toimivuudesta ja sen soveltamiseen liittyvistä kokemuksista. Lausuntopyynnön diaarinumero: VN/5281/2019. Saatavissa: https://www.lausuntopalvelu.fi/FI/Proposal/ShowAllProposalAnswers?proposalId=2df6ebd7-975e-4169-a0de-edd9ab3d7217 (Luettu 25.9.2019). *(Oikeusministeriön selvitys 2019)*

Pietikäinen, Suvi: Rekisterinpitäjän ja käsittelijän väliset sopimukset. Valtionvarainministeriö 2016. Saatavissa: https://www.vahtiohje.fi/web/guest/rekisterinpitajan-velvollisuudet (Luettu 1.5.2019).

Suojelupoliisi: Turvallisuusselvitys on ennaltaehkäisevää turvallisuustyötä. Helsinki 2019. Saatavissa: https://www.supo.fi/turvallisuusselvitykset (Luettu 5.7.2019).

Suomen tulli: EU-, Eta-, Efta- ja Schengen-maat. 2019. Saatavissa: https://tulli.fi/tietoa-tullista/tullin-toiminta/eu-eta-efta-ja-schengen-maat (Luettu 20.7.2019).

Suomen Yrittäjät: Yrittäjyys Suomessa. Päivitetty 28.3.2019. Saatavissa: https://www.yrittajat.fi/suomen-yrittajat/yrittajyys-suomessa-316363 (Luettu 6.4.2019).

Valtioneuvoston kanslia: Lainsäädännön arviointineuvosto, Tehtävät ja toimintatavat. 2019. Saatavissa: https://vnk.fi/arviointineuvosto/tehtavat-ja-toimintatavat (Luettu 14.1.2019).

LYHENTEET

Asetus	Euroopan unionin yleinen tietosuoja-asetus (EU 679/2016)
EDPB	Euroopan tietosuojaneuvosto
ETA	Euroopan talousalue
EU	Euroopan unioni
HE	Hallituksen esitys
HeTL	Henkilötietolaki (523/1999)
ICO	Ison-Britannian tietosuojaviranomainen
KHO	Korkein hallinto-oikeus
SEU	Sopimus Euroopan unionista
SEUT	Sopimus Euroopan unionin toiminnasta

KUVAT

TAULUKOT

1 JOHDANTO

1.1 Tutkielman aihepiiri ja kysymysten asettelu

Digitaalisessa maailmassa henkilötiedoista ja kuluttajien tuottamasta datasta on tullut markkinoilla hyödynnettävä valuutta. Kilpailu- ja kuluttajaviraston mukaan yksinään Euroopan unionin (EU) *datatalouden* arvo oli 300 miljardia euroa vuonna 2016, ja sen uskotaan nousevan vuoteen 2020 mennessä jopa 739 miljardiin euroon.[1] *Digitalisaation* muutospaineiden myötä, myös unionin lainsäädäntö vaati uudistusta. EU:n yleinen tietosuoja-asetus[2] (jäljempänä ”*Asetus*”) tuli voimaan 25.5.2016 ja edelleen sovellettavaksi jäsenvaltioissa 25.5.2018 alkaen. Asetuksen täytäntöönpano on vaikuttanut ja tullee vaikuttamaan enenevissä määrin erityisesti yritysten toimintaan. Kyseessä ei ole uuden asian sääntely, mutta Asetuksen myötä yritysten on tullut huolehtia käsittelemistään henkilötiedoistaan entistä tarkemmin. Toimimalla Asetuksen vaatimusten mukaisesti yritys voi pyrkiä saavuttamaan kilpailuetua markkinoilla osoittamalla ulospäin olevansa luotettava ja ottavansa tietosuojan vakavasti. Euroopan komission komissaari *Věra Jourová* näkee Asetuksen mahdollisuutena talouden kehitykselle:

> *”Studies indicate that companies benefit from their privacy investments. These benefits include fewer losses from data breaches, quicker sales and innovation through the offer on the market of new products and services with novel privacy and data security solutions. We see these products often developed by smaller and medium-sized companies. In short, the Europe's data protection law, the GDPR, is an opportunity for business and a means for individuals to build trust.”*[3]

Tietosuojasääntelyn kokonaisuudistuksen tavoitteena oli saada aikaan koko unionin kattava ajanmukainen, vahva ja yhtenäinen tietosuojakehys.[4] Sääntelyuudistuksen taustalla vaikutti informaatioteknologian nopea kehitys ja tarve saada lievitettyä jäsenvaltioiden epäyhtenäisestä henkilötietodirektiivin[5] implementoinnista aiheutuneita haasteita.[6] Asetuksen johdantolauseen (166) mukaan, Asetuksella suojataan luonnollisten henkilöiden oikeutta henkilötietojen suojaan sekä varmistetaan henkilötietojen vapaa liikkuvuus jäsenmaiden välillä.

---

[1] Ks. *Kilpailu- ja kuluttajavirasto* 2019, s. 9 ja 11.
[2] Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta (yleinen tietosuoja-asetus).
[3] *Jourová* 2019, kohta Data protection and privacy.
[4] *COM (2018) 43, lopull.*, kohta 1. EU:n uusi tietosuojakehys – vahvempi suoja ja uusia mahdollisuuksia.
[5] Euroopan parlamentin ja neuvoston direktiivi 95/46/EY annettu 24 päivänä lokakuuta 1995, yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta.
[6] *HE 9/2018 vp*, s. 4.

Asetuksen voimaantulosta, velvoitteista ja yksityishenkilöiden asemasta on tiedotettu julkisuudessa runsaasti[7], jonka seurauksena henkilötietojen arkaluonteisuus ja oikeus henkilötietojen suojaan ovat tulleet laajasti tiedostetuksi[8]. Yritykset ovat täytäntöönpanneet merkittävän määrän uusia käytänteitä sekä teknisiä ja organisatorisia toimia vastatakseen Asetuksen vaatimuksiin. Asetuksen artiklan 28 määrittelemät tietojenkäsittelysopimuksia koskevat sopimusvaatimukset ovat yksi mainituista uusista velvoitteista (jäljempänä ”*Sopimusvaatimus*”). Sopimusvaatimusten yrityksille aiheuttama taakka ilmenee yritysten ulkoistaessa *henkilötietojen käsittelyn* kokonaan tai osin toiselle yritykselle.[9] Sopimusvaatimusten taakka kohdistunee erityisesti sopimuskumppaneiden välisiin neuvotteluihin, yritysten pyrkiessä löytämään yhteisen ymmärryksen tietojenkäsittelysopimuksen sisällöstä, tarpeesta ja soveltuvuudesta.

1.1.1 Asetuksen asettamien Sopimusvaatimusten merkitys yrityksille

Yritykset keräävät *henkilötietoja* lukuisiin eri tarpeisiin, kuten asiakasrekisteriä, markkinointia, profilointia tai lain erikseen määräämiä velvoitteita varten. Henkilötiedoilla tarkoitetaan Asetuksen artiklan 4.1 mukaisesti kaikkia tunnistettuun tai tunnistettavissa olevaan henkilöön liittyviä tietoja (jäljempänä ”*Rekisteröity*”). Henkilötietoja ovat esimerkiksi asiakkaan nimi, henkilötunnus, sijaintitiedot, verkkotunnistetiedot, taikka sairauksia koskevat tiedot. Yritykset käsittelevät henkilötietoja monesti hallinnollisen toiminnan vuoksi, muun muassa palkanlaskennan ja henkilöstörekistereiden muodossa. Yrityksen henkilötietojen käsittelyn laajuus riippuu yrityksen toimialasta, kansainvälisyydestä, koosta sekä yhtiömuodosta[10]. Asetuksen myötä yritysten on tullut pystyä osoittamaan käsittelevänsä henkilötietoja lainmukaisesti. Mainittu *osoitusvelvollisuus* on Asetuksen yksi merkittävimmistä periaatteista. Osoitusvelvollisuus konkretisoituu myös Asetuksen 28 artiklan Sopimusvaatimuksissa. Yritysten tulee varmistaa, että myös kyseisen yrityksen lukuun toimivat tahot, kuten ulkoistettu palkanlaskenta, täyttävät Asetuksen vaatimukset toiminnassaan. Sopimusvaatimusten vaikutukset markkinoille on siten huomattava, sillä teknologian kehityksen ja digitalisaation myötä on oletettavaa, että lähes kaikki yritykset keräävät tai käsittelevät jopa huomattavia määriä henkilötietoja. Vastatakseen

[7] Esimerkiksi tietosuojavaltuutetun toimiston toimintakertomuksen mukaan, Asetuksesta kirjoitettiin lähes 2 200 artikkelissa ja tietosuojavaltuutettu esiintyi hakusanana lähes tuhannessa artikkelissa. *Tietosuojavaltuutetun toimisto* 2018a, s. 22.

[8] Komission teettämän eurobarometrin mukaan suomalaisista 66 % oli kuullut Asetuksesta, mutta vain 35 % tiesi mitä Asetus käsittää. *Euroopan komission erityisbarometri* 2019a, s. T2.

[9] Henkilötietojen käsittelyllä tarkoitetaan Asetuksen artiklan 4.2 mukaisesti mm. henkilötietojen keräämistä, säilyttämistä, käyttöä, siirtämistä ja luovuttamista. Kaikki henkilötietoihin kohdistuvat toimenpiteet henkilötietojen käsittelyn suunnittelusta henkilötietojen poistamiseen ovat henkilötietojen käsittelyä.

[10] *Lång* 2016, s. 2.

markkinoiden kysyntään, yhä useampi toimii yhteistyössä muiden yritysten kanssa tai ulkoistaa käsittelyn tehostaakseen toimintaansa.

Sopimusvaatimusten mukaan, yritysten on solmittava kirjallinen sopimus, kun henkilötietojen käsittely suoritetaan toisen yrityksen lukuun (jäljempänä ”*Tietojenkäsittelysopimus*”). Tietojenkäsittelysopimuksessa tulee vahvistaa muun muassa käsittelyn kohde ja kesto, käsittelyn luonne ja tarkoitus, henkilötietojen tyyppi ja Rekisteröityjen ryhmät, sekä rekisterinpitäjänä toimivan yrityksen velvollisuudet ja oikeudet. Rekisterinpitäjällä tarkoitetaan Asetuksen 4.7 artiklan mukaisesti yhtä tai useampaa oikeushenkilöä – kuten yrityksiä, jotka yksin tai yhdessä määrittelevät henkilötietojen käyttötarkoituksen sekä miten niitä käsitellään (jäljempänä ”*Rekisterinpitäjä*” tai ”*yritys*”).[11] Yrityksille, jotka ovat tottuneesti solmineet kirjalliset sopimukset henkilötietojen käsittelystä palveluntuottajiensa kanssa jo ennen Asetuksen voimaan tuloa, Sopimusvaatimusten sisältö ei välttämättä tarkoita käytännöntason muutoksia. Artikla 28 voi toimia näissä tapauksissa myös hyvänä muistilistana ja runkona, sen antaessa eräänlaisen minimitason sopimuksen sisällölle. Oletettavaa kuitenkin on, että vaatimustason noustessa, huomattava osa yrityksistä on Sopimusvaatimusten kanssa uuden edessä. Myös Sopimusvaatimusten tulkinta ja oikea täytäntöönpano voi sitoa yritysten resursseja erityisesti sopimusneuvotteluissa ja henkilötietoja käsittelevän tietoteknologian päivittämisessä. Huomattavaa on, että Asetuksen voimaantulon myötä, yritysten kaikki ulkoistetut sopimukset, jotka koskevat henkilötietojen käsittelyä, tulee täyttää Sopimusvaatimukset, tarkoittaen niin uusia kuin olemassa olevia sopimuksia. Osa Sopimusvaatimusten aiheuttamasta kuormasta, johtuneekin mittavasta vanhojen mutta voimassaolevien sopimusarkistojen päivittämisestä.

Henkilötietojen käsittelyn lainmukaisen käsittelyn merkittävyyttä korostaa Asetuksen asettama sanktiouhka. Yritykset ovat vastuussa Sopimusvaatimusten rikkomisesta, mikä voi tarkoittaa vahingonkorvausvastuun lisäksi velvollisuutta maksaa hallinnollista sakkoa 10 miljoonaa euroa tai 2 % yhtiön maailmanlaajuisesta liikevaihdosta.

Parhaimmillaan Sopimusvaatimukset luovat yritysten toiminnalle selkeät suuntaviivat henkilötietojen käsittelylle sekä yhtenäistää ja edistää eri jäsenmaihin sijoittautuneiden yritysten välisiä sopimusneuvotteluita. Yleisellä tasolla tietosuojasääntelyn voi myös nähdä vahvistavan kansalaisten luottamusta yrityksiä kohtaan, heidän ollessaan paremmin tietoisia oikeuk-

[11] Rekisterinpitäjänä voi olla esimerkiksi luonnollinen henkilö, oikeushenkilö, virasto tai organisaatio. Mm. sairaalat, erilaiset yhdistykset, myös verkkokaupat toimivat usein rekisterinpitäjinä.

sistaan ja pystyessään paremmin vaikuttamaan omien henkilötietojensa käsittelyyn. Käsittelyn ennustettavuus luonee taas oikeusvarmuutta ja edistänee palveluiden vapaata liikkuvuutta.

Sopimusvaatimusten kuormittavuus jakautunee kuitenkin eri yritysten välillä eri tavalla. Sääntelyn velvoitteet kuormittavat yritysten jokapäiväistä toimintaa ja riskienhallintaa riippuen toimialasta, kansainvälisyydestä, koosta sekä yhtiömuodosta[12]. On myös huomattavaa, että tällöin yritysten resurssit ja lähtökohdat täytäntöönpanna sääntelyn velvoitteet vaihtelevat. Yritysten valmiudet henkilötietojen käsittelijöinä eroavat siis suuresti; osa yrityksistä, erityisesti isommat ja monikansalliset yritykset, ovat panostaneet ja investoineet henkilötietojen käsittelyyn jo ennen tietosuojasääntelyn uudistusta, kun taas pienemmät ja ”ei-henkilötietosensitiiveillä aloilla” toimivat yritykset saattavat olla epävarmoja Asetuksen vaatimista uusista toimista.

1.1.2 Sopimusvaatimusten ennakointi

Jotta Asetuksen tavoite vahvistaa sisämarkkinoita ja varmistaa henkilötietojen vapaa liikkuvuus jäsenvaltioiden välillä olisi toteutettavissa, tulee Asetuksen täytäntöönpanon selkeyteen kiinnittää huomiota. Hallituksen esityksen (HE) mukaan vapaan liikkuvuuden esteenä mainitaan muun muassa henkilötietojen käsittelylle asetetut ylimääräiset edellytykset.[13] Vaikka henkilötietojen käsittelyyn liittyvää byrokratiaa on saatu Asetuksen myötä kevennettyä, on se tuonut mukanaan joukon uusia vaatimuksia. Jotta henkilötietojen suojasta on mahdollista saada erottamaton osa yritysten organisatorisia toimia, tulee yritysten huomioida sitä koskevat tietosuojavelvoitteet kaikessa toiminnassaan. Sopimusvaatimusten ollessa yrityksiin nähden uusi velvoite, viranomaisten antama ohjeistus ja velvoitetta tukevien mekanismien tarjoaminen keventänee yrityksille siitä aiheutuvaa taakkaa. Valmistautuminen ennakolta, riittävä ja oikea-aikainen tiedottaminen, sekä yritysten tukeminen olisikin ollut erityisen tärkeää Sopimusvaatimusten kuormittavuuden vähentämiseksi. Sopimusvaatimusten yritysvaikutusten kattava kartoittaminen olisi siten myös edesauttanut Asetuksen tavoitteisiin pääsemistä. Yritystasolla Sopimusvaatimusten täytäntöönpanoon paneutuminen ja valmistautuminen saattaisi ennalta estää yrityksiä syyllistymästä sääntelyn sisältämille sanktioille ja sen tuomille mahdollisille mainehaitoille.

[12] *Lång* 2016, s. 2.
[13] *HE 9/2018 vp*, s. 27

1.2 Tutkielman tavoitteet

Tutkielman tarkoituksena on kartoittaa Asetuksen artikla 28 velvoitteet ja vaikutukset yritysten toiminnassa sekä selvittää kyseisten Sopimusvaatimusten keskeisimmät yritysvaikutukset Suomessa toimiville yrityksille. Tutkielmassa toteutetaan myös empiirinen kyselytutkimus rajatulle yritysjoukolle. Tutkielma ei erittele Sopimusvaatimusten vaikuttavuutta yritysten eri markkina-alojen välillä, vaan käsittelee kaikkia yrityksiä yhtenä joukkona. Yritysten joukko on lisäksi rajattu Suomessa toimiviin yksityisiin yrityksiin, jättäen ulkopuolelle muun muassa julkisessa omistuksessa olevat yritykset sekä kansainvälisen vertailun – vaikkakin aihetta sivutaan lyhyesti. Tietosuojasääntelyllä on Asetuksen lisäksi paljon liittymiä myös muuhun lainsäädäntöön, muun muassa lukuisiin kansallisiin erityislakeihin, mutta tämä tutkielma rajautuu käsittelemään vain Asetusta, tarkemmin rajattuna artiklan 28 Sopimusvaatimusten yritysvaikutuksia.

Tutkielman tarkoituksen ja rajausten myötä, tutkimuskysymys on muotoutunut seuraavasti:

> ”Mitä yritysvaikutuksia Sopimusvaatimuksilla on Suomessa toimivien yritysten toiminnassa?”.

Haasteen tutkielmalle luo sääntelyn tuoreus, jonka vuoksi voi olla liian aikaista lähteä selvittämään Sopimusvaatimusten toteutuneita yritysvaikutuksia, sillä kaikki vaikutukset eivät todennäköisesti ole vielä ilmenneet. Toiseksi, yritysten käytännöt eivät ole välttämättä vielä vakiintuneet, jonka vuoksi Sopimusvaatimusten tunnistaminen yritysten taakkaa lisäävänä tekijänä voi alussa tuntua korostuneesti. Yritysvaikutusten arviointia heikentää myös Sopimusvaatimusten velvoittavuutta koskeva laaja yritysten joukko; sääntely velvoittaa kaikkia yrityksiä solmimaan kirjallisen sopimuksen Sopimusvaatimusten mukaisesti, kun kyse on ulkoistetusta henkilötietojen käsittelystä, koskien niin yksityistä kuin julkista sektoria, kattaen toisin sanoen kaikki yrityssektorit. Laaja yritysten joukko taas vaikeuttaa vaikutusten vertailtavuutta toisiinsa, sillä lähtökohdat sääntelyn vaatimuksille saatavat erota paljonkin toisistaan jo olemassa olevan ja vanhemman erityislainsäädännön vuoksi. Tämän vuoksi sääntelyn kuormittavuus voi vaihdella yritysten ja eri markkina-alojen välillä suurestikin. Yritysvaikutusten selvittäminen vaatisi merkittävästi laajempaa tutkimusta, jossa eri yrityssektorit arvioitaisiin erikseen. Tietosuojasääntelyn todellisten ja toteutuneiden yritysvaikutusten selvittäminen vaatisi markkina-alojen mukaan eriteltyä empiiristä tutkimusta, jolloin yritysten hallinnolliset velvoitteet ja kuormittavuus olisivat vertailukelpoisia keskenään.

1.3 Tutkimusmenetelmät

1.3.1 Oikeusdogmatiikka

Asetettujen tutkimuskysymysten myötä, on ilmeistä, että tutkielman laadukas toteutus vaatii kirjoittajaltaan monitieteistä tutkimusta. Monitieteisyyden tuoma metodinen avoimuus[14] mahdollistaa normatiivisen oikeustieteen eli lainopin ja ei-normatiivisen tutkimusmenetelmien yhdistämisen, antaen lopullisille tutkimustuloksille monimuotoisuutta, moniarvoisuutta ja avoimuutta.[15] Tutkielman tutkimusmenetelmiksi on tämän myötä valikoitunut oikeustieteelliselle tutkimukselle tyypillinen lainopillinen eli oikeusdogmaattinen tutkimusmenetelmä, joka toimii niin sanottuna pääasiallisena tutkimusmenetelmänä. Monitieteisyyden nimissä, lainopillisen menetelmän rinnalla, tutkielmassa hyödynnetään täydentävinä menetelminä empiiristä tutkimusmenetelmää sekä soveltuvin osin sääntelyteoriaa.

Tutkielman pääasialliset lähteet koostuvat menetelmälle tyypillisesti aihetta käsittelevästä lainsäädännöstä, oikeuskirjallisuudesta, artikkeleista, hallituksen ja komission esityksistä ja selvityksistä, sekä oikeuskäytännöstä ja asiantuntijalausunnoista. Näin pyritään saamaan kattava selvitys Sopimusvaatimusten tämän hetken velvoittavuudesta Suomessa toimiville yrityksille. Tutkielma pohjautuu siten voimassa olevaan lainsäädäntöön (*de lege lata*), huomioiden kuitenkin kirjoittajan *de lege ferenda* – kannanotot pohdinnoissaan. Lainsäädännön ollessa tuoretta, tutkielman johtopäätösten kannanotot Sopimusvaatimusten tosiasiallisista vaikutuksista perustuvat kuitenkin suurissa määrin tutkielman kyselytutkimukseen osallistuneiden yritysten antamiin vastauksiin.

1.3.2 Empiirinen tutkimusmenetelmä

Sopimusvaatimusten toteutuneiden yritysvaikutusten selvittämiseksi, tutkielmassa toteutettiin kysely erikseen rajatulle yritysjoukolle. Empiirisen tutkimuksen liittäminen osaksi tutkielmaa mahdollistaa todellisten yritysvaikutusten selvittämisen. Empiirisen tutkimuksen avulla saadut vastaukset edesauttavat tutkielman tulosten kattavuutta ja antavat välittömän vastauksen, miten Sopimusvaatimukset ovat käytännössä vaikuttaneet yrityksiin.[16] Kyselyn tulokset muo-

[14] Määttä kuvaa metodista avoimuutta valmiutena yhdistää ennakkoluulottomasti erilaisia tutkimuksellisia näkökulmia ja lähestymistapoja. Metodisen avoimuuden rinnalla puhutaan myös metodisesta pluralismista, joka tarkoittaa Määtän mukaan menetelmällistä avoimuutta, monimuotoisuutta ja -arvoisuutta. *Määttä* 2015, s. 2.
[15] *Ervasti* 2004, s. 10–11.
[16] *Korkea-aho* 2004, s. 83.

dostavat kuitenkin vain osan suurempaa tutkielma-aiheen yritysvaikutuksia käsittelevää kokonaisuutta. Oikeustieteiden tohtori, dosentti *Emilia Korkea-aho* on todennut 2004 pidetyssä tutkijaseminaarissa, että tutkielman empiirisen tutkimusosion voidaan katsoa olevan osin sekä määrällistä, että laadullista.[17] Määrällistä, kvantitatiivista tutkimusta tutkielmassa ilmentää etukäteen laaditut kyselylomakkeet, joissa yrityksen vastausvaihtoehdot olivat pääsääntöisesti rajattu valmiiksi annettuihin vaihtoehtoihin. Laadullista, kvalitatiivista tutkimusta tutkielmassa olisi ilmentänyt erityisesti yrityksissä tehdyt haastattelut. Vastanneille yrityksille tarjottiin mahdollisuutta vastata kyselyn sijaan haastatteluna, mutta yksikään kyselyyn vastannut ei valinnut tätä vaihtoehtoa. Haastattelut olisivat voineet edelleen rikastuttaa empiirisen tutkimuksen tuloksia, kun haastateltavat olisivat saaneet mahdollisuuden kertoa omin sanoin mielipiteitään ja kokemuksiaan, ja tarvittaessa jakaa uusia omasta mielestään olennaisia huomioita käsiteltävistä aihealueista.[18]

1.3.3 Sääntelyteoria

Jotta tutkielman teoriapohja on ymmärrettävää ja riittävä, sovelletaan tutkielmassa lainopillisen ja empiirisen tutkimusmenetelmien rinnalla sääntelyteoriaa[19]. Sääntelyteorian avulla soveltuvaa sääntelyä analysoidaan yritysten näkökulmasta, jonka avulla tutkimukseen saadaan osin oikeustaloustieteellistä vivahdetta. Positiivisen oikeustaloustieteen tavoin tutkielmassa analysoidaan myös Sopimusvaatimusten tehokkuutta ja lainsäätäjän mahdollisia motiiveja koskien lailla yrityksiin kohdistettuja velvoitteita ja toimintaa tukevia mekanismeja.[20] Sääntelyteoriaan nojaten, tutkielmassa tuodaan myös esille, miten Sopimusvaatimusten yritysvaikutukset on huomioitu tietosuojasääntelyn valmistelussa ja kuinka jälkiseurannan tarve on huomioitu. Tutkielman sääntelyteoreettinen analyysi ei kuitenkaan ota kantaa onko kyseinen sääntely riittävää tai voisiko sitä vähentää.

1.4 Lähdeaineisto ja rakenne

Tutkielmassa Sopimusvaatimusten yritysvaikutuksia selvitetään lainsäädäntöä, oikeustapauksia, oikeuskirjallisuutta sekä viranomaislähteitä hyödyntäen. Lainsäädännön tutkiminen keskittyy Asetuksen tuomiin velvoitteisiin, keskittyen erityisesti artiklan 28 määrittelemiin Sopimusvaatimuksiin. Tutkielman rajauksista ja tietosuojasääntelyn rakenteista johtuen, tut-

[17] *Korkea-aho* 2004, s. 89–90.
[18] *Kainulainen* 2004, s. 17–18.
[19] Ks. sääntelyteoriasta lähemmin *Baldwin – Cave – Lodge* 2012, luvut 1–8 ja 11–14.
[20] *Määttä* 2016, s. 32–31.

kielmassa ei ole ollut tarvetta selvittää kansallista tietosuojalainsäädäntöä muutamia mainintoja tarkemmin. Sopimusvaatimusten yritysvaikutusten selvittämiseksi, tutkielmassa käsitellään kattavasti eri viranomaisten ohjeita ja kannanottoja lainsäädännön ja Asetuksen sisällöstä sekä yritysvaikutusten kartoittamisesta ja jälkiseurannasta. Henkilötietojen suojasta löytyy paljon kirjallisuutta, sittemmin myös suomalaista oikeuskirjallisuutta, mutta varsinaisesti Tietojenkäsittelysopimuksia koskien vielä melko vähän. Lisäksi tutkielmassa on hyödynnetty sähköisiä artikkeleita sekä blogeja rikastuttamaan tutkielman kriittistä pohdintaa, vaikka yksittäisten henkilöiden tai asianajajatoimistojen kirjoitusten tieteellinen arvo lieneekin kyseenalaistettavissa. Koska tutkielman aiheesta ei ole vielä tutkielman kirjoitushetkellä julkaistua suomalaista oikeuskäytäntöä, on selvityksessä hyödynnetty muiden jäsenmaiden sekä komission antamia tulkintoja ja oikeustapauksia.

Tutkielma jakautuu kuuteen eri lukuun. Luvuissa kaksi, kolme ja neljä keskitytään aiheen teoreettiseen viitekehykseen. Toisessa luvussa selvitetään mitä yritysvaikutuksilla tarkoitetaan ja yritysvaikutusten kartoittamisen merkitystä yhteiskunnassa. Kolmannessa luvussa käydään läpi Asetuksen yrityksille aiheuttamia velvoitteita ja kustannuksia yleisellä tasolla. Neljännessä luvussa keskitytään Asetuksen artiklaan 28, selvittäen kattavasti Sopimusvaatimusten sisältöä. Neljäs luku nivoo myös käsitetasolla yhteen aikaisempien lukujen sisältöä koskien yritysvaikutusten selvittämisen sekä Asetuksen aiheuttamat kustannukset ja niiden vaikutukset yritysten toimintaan. Kattavan teorian jälkeen, viidennessä luvussa käydään läpi tutkielmassa toteutettu kyselytutkimus ja siitä saadut tulokset. Tutkielman kuudennessa, eli viimeisessä luvussa esitellään johtopäätökset Sopimusvaatimusten yritysvaikutuksista Suomessa toimiville yrityksille. Johtopäätösten osana hyödynnetään kyselytutkimuksen merkittävimpiä tuloksia.

2 MITÄ YRITYSVAIKUTUKSILLA TARKOITETAAN JA MITEN NIITÄ SELVITETÄÄN

2.1 Vaikutusarvioinnin tavoitteet yleisesti

Sääntelyn *vaikutusarvioinnin* perimmäinen tarkoitus on tarjota tietoa lain valmistelijoille, päättäjille sekä sidosryhmille, esimerkiksi yrityksille ja yksityisille henkilöille. Parhaimmillaan tehty arvio kertoo selkeästi sääntelyn tulevista vaikutuksista, merkittävyydestä, sekä sen tuomista hyödyistä ja haitoista. Merkittävä osa vaikutusarviointia on myös voimaan saatetun sääntelyn vaikutusten seuranta. Jotta asetettuihin tavoitteisiin päästäisiin ja mahdolliset yllättävätkin haitalliset vaikutukset voitaisiin korjata, on sääntelyn jälkikäteinen seuranta erityisen tärkeä vaihe vaikutusarviointia.

Tässä luvussa käsitellään sääntelyn vaikutusarviointia yleisesti; mistä vaikutusarvioinnissa on kyse sekä mitä arvioinnin toteuttamisessa tulisi huomioida. Tutkielman rajauksesta johtuen, luvun painotus asian käsittelyssä tulee kuitenkin olemaan *yritysvaikutusten arvioinnissa*.

2.2 Sääntelyn vaikutusarviointi

2.2.1 Vaikutusarviointia koskeva ohjeistus

Säädösehdotusten vaikutusarviointi tulee toteuttaa valtioneuvoston antamien ohjeiden mukaisesti. Säädösehdotusten vaikutusten arviointiohjeet (jäljempänä *”Valtioneuvoston ohjeet”)*[21] toimivat rinnan *hallituksen esityksen laatimisohjeiden* kanssa, joissa tuodaan esille vaikutusarvioinnin tärkeys ja edellytetään vaikutuksenarvioinnin sisällyttämistä hallituksen esityksiin.[22] Valtioneuvoston ohjeet käsittelevät vaikutusarvioinnin toteutusta hallituksen esityksen laatimisohjeita yksityiskohtaisemmin ja kattavammin. Näin ollen, säädösehdotusten vaikutusarvioinnin tulee käsitellä niin taloudelliset vaikutukset, vaikutukset viranomaisten toimintaan, ympäristövaikutukset, sekä muut yhteiskunnalliset vaikutukset.[23] Vaikutusarvioinnin keskeisimmät tulokset kuvataan hallituksen esitysten perusteluosissa. Jokaisesta mainitusta

[21] Valtioneuvosto antoi 1.11.2007 oikeusministeriön esityksestä ohjeet säädösehdotusten vaikutusten arvioinnista. Ohjeilla korvattiin aikaisemmat ohjeet koskien taloudellisten vaikutusten arviointia (1998), ympäristövaikutusten arviointia (1998), yritysvaikutusten arviointia (1999), sekä aluekehitysvaikutusten arviointia (2003). *Oikeusministeriö* 2007, kohta Esipuhe.

[22] *Oikeusministeriö* 2018, s. 23–24, 57 ja 36.

[23] Mainitut vaikutusalueet pitävät sisällään mm. vaikutukset yrityksille, kotitalouksille, kansantaloudelle, ympäristön kehitykselle, ihmisten terveydelle, kansalaisten perusoikeuksille ja tietoyhteiskunnalle. Ks. tarkemmin vaikutusarvioinnin kattavuudesta *Oikeusministeriö* 2007, s. 8.

vaikutusalasta löytyy ohjeita täydentävää tietoaineistoa tukemaan arvioinnin toteuttamista.[24] Valtioneuvoston ohjeita sovelletaan lakien valmistelun lisäksi myös asetusten ja oikeussäännöjen valmistelussa. Valtioneuvoston ohjeet ovat hyödynnettävissä myös kansainvälisten velvoitteiden hyväksyntä-prosesseissa, mukaan lukien EU liitännäisissä asioissa kuten direktiivien implementoinneissa sekä EU asetusten voimaan saattamisissa.[25]

Vaikutusarviointi toteutetaan osana ministeriöiden säädösvalmistelua, tarkoittaen sitä, että kulloinkin säädösvalmistelusta vastuussa oleva ministeriö laatii ja vastaa vaikutusarvioinnin toteuttamisesta.[26] Vaikutusarvioinnin avulla päätöksentekijät saavat riittävästi tietoa, siitä millaisia vaikutuksia uudella sääntelyllä olisi. Vaikutusarvioinnin tuleekin esitellä tulevan sääntelyn tavoitteet ja hyödyt, kustannukset, haitat ja riskit sekä mahdolliset odottamattomat vaikutukset.[27] Lisäksi, vaikutuksissa tulee ottaa huomioon sääntelyä koskevat välittömät sekä mahdolliset välilliset vaikutukset[28]. Kyseisten tietojen avulla päätöksentekijät voivat tehdä tarvittavia muutoksia tai lisäyksiä lain sisältöön tai keskeyttää hankkeen etenemisen kannattamattomana uudistuksena. Vaikutusarviointi voi siten parantaa lainsäädännön laatua, millä on merkittävä vaikutus yhteiskuntaan; sääntelyllä vaikutetaan niin ihmisten perusoikeuksien turvaamiseen, kuin viranomaisten juridiseen päätöksentekoon esimerkiksi tuomioistuimissa ja virastoissa. Vaikutusarvioinnin ehdottomana hyötynä on myös sen tarjoama informaatio sidosryhmille, sillä etukäteen saatu tieto tulevista muutoksista ja vaatimuksista keventää ja edesauttaa kohderyhmien valmistautumista ja sääntelyn täytäntöönpanoa.[29]

Se, miten laajana ja yksityiskohtaisena kyseisiä vaikutuksia arvioidaan, on aina riippuvainen kyseessä olevasta lakiehdotuksesta, sekä sen tuomien vaikutusten merkittävyydestä. Kaikissa tilanteissa tärkeää on monipuolinen ja kattava kartoitus, joka ottaa huomioon myös mahdolliset vaikutukset, jos sääntelyehdotus jää toteuttamatta. Pääasiallisena tavoitteena kuitenkin on, että toteutettu arviointi antaa päätöksentekijöille riittävästi luotettavaa tietoa eri ratkaisuvaih-

[24] Ks. *Oikeusministeriö* 2019, kohdat Taloudelliset vaikutukset; Viranomaisvaikutukset; Ympäristövaikutukset; Muut yhteiskunnalliset vaikutukset.
[25] *Oikeusministeriö* 2007, kohta Esipuhe.
[26] Esimerkiksi oikeusministeriön teettämät selvitykset tietosuojalain (1050/2018) valmistelussa. Ks. *HE 9/2018 vp*, s. 64–69.
[27] *Oikeusministeriö* 2007, s. 8.
[28] Valtioneuvoston ohjeissa mainitaan esimerkkejä sääntelyn välillisistä ja välittömistä vaikutuksista. Välittömiä taloudellisia vaikutuksia voivat olla mm. työ- ja kalustokustannukset, kun taas välillisesti vaikutukset voivat näkyä mm. sairaanhoitokuluissa tai ihmisten työkyvyssä. *Oikeusministeriö* 2007, s. 8.
[29] *Oikeusministeriö* 2007, s. 7.

toehdoista ja näiden seurauksista, kattaen niin ennakollisen ”*ex-ante*”- kuin jälkikäteisen ”*ex-post*”- arvioinnin.[30]

2.2.2 Vaikutusarvioinnin huomiointi säädösvalmistelussa

Alla olevassa kuvassa 1, havainnollistuu hyvin vaikutusarvioinnin vaiheet säädösvalmistelussa. Kyseinen Valtioneuvoston ohjeissa esitetty kaavio[31] voi elää ja vaihdella säädösvalmistelun edetessä ja eri säädösvalmisteluiden välillä.[32]

Kuva 1. Vaikutusarviointi säädösvalmistelun eri vaiheissa.

Säädösvalmistelun ensivaiheessa eli lainsäädännön valmistelun alussa, esiselvitysten ja esivalmistelun ohessa, kartoitetaan millaiset vaikutukset kyseisellä sääntelyvaihtoehdolla olisi. Sääntelyvaihtoehtoja voi olla myös useampi, riippuen sääntelyn tarpeesta ja tavoitteista.[33] Uusi säädös[34] ei aina ole kaikkein tehokkain[35] ratkaisuvaihtoehto, vaan asiantilan ratkaisemiseksi voi olla myös muita kevyempiä vaihtoehtoja.[36] Valtioneuvoston ohjeet sisältävät vaiku-

[30] *Oikeusministeriö* 2007, s. 9.
[31] *Oikeusministeriö* 2007, s. 10.
[32] *Oikeusministeriö* 2007, s. 10.
[33] *Oikeusministeriö* 2007, s. 10.
[34] Suomessa säädöksiin luetaan esimerkiksi lait, tasavallan presidentin ja valtioneuvoston asetukset, viranomaisten määräykset sekä Ahvenanmaan maakuntalait. Tämän lisäksi, kansallisesti voimassa oleviin säädöksiin luetaan myös EU sääntely sekä Suomea sitovat kansainväliset sopimukset ja velvoitteet. *Eduskunta* 2019a, kohta Oikeusjärjestyksestä, säädöksistä ja säädöshierarkiasta.
[35] Ks. sääntelyn tehokkuudesta tarkemmin *Määttä* 2011, s. 25–28.
[36] Sääntelyvaihtoehtoina ymmärretään monesti toimet, jotka eivät edellytä oikeudellista sääntelyä. *Jyrki Talan* mukaan yksi sääntelyvaihtoehdoista olisi informaatio-ohjaus. Tarkoittaen neuvonantoa ja ohjeistamista joilla

tusarviointia helpottavan ”*vaikutusten tunnistamisen tarkistuslistan*”.[37] Vaihtoehtojen vaikutusten huolellinen kirjaaminen tuo selkeästi esille eri vaihtoehtojen vaikutusten erot. Kerätyn tiedon avulla valmistelusta siirrytään säädösvalmistelun seuraaviin vaiheisiin; perusvalmisteluun, lausuntovaiheeseen sekä jatkovalmisteluun.

Perusvalmistelussa toteutettu vaikutusarviointi menee valmistelun kartoittamista syvemmälle. Kattava vaikutusarvioinnin toteutus vaatiikin laajempaa selvittämistä, kuten kuulemisia ja lausuntoja asiantuntijoilta, sidosryhmiltä ja viranomaisilta. Saadut vaikutusarvioinnin tulokset tulee saattaa ministeriön tietoon, jotta sen tuoma informaatio on käytettävissä säädösvalmistelussa ja siihen liittyvässä päätöksenteossa.[38] Vaikutusarvioinnin keskeiset tulokset sisällytetään hallituksen esityksen perusteluihin. Perusteluissa tulee mainita lyhyesti ainakin seuraavat vaikutukset: vaikutusarvioinnin keskeiset tulokset eli merkittävimmät vaikutukset, miten vaikutukset on arvioitu, mihin tietolähteisiin ja oletuksiin arviointi perustuu, onko arviointia tehtäessä pyydetty lausuntoja tai järjestetty kuulemisia ja miten *jälkiseuranta* aiotaan toteuttaa.[39] Vaikutusarvioinnin merkittävyyttä kuvastaa myös sen huomiointi *laintarkastusvaiheessa*. Jos oikeusministeriö toteaa laintarkastusvaiheessa, että vaikutusarviointi on toteutettu puutteellisesti, voi sääntelyä valmistellut ministeriö saada asiasta huomautuksen.[40]

Säädösvalmistelusta vastannut ministeriö laatii käsiteltävästä asiasta edellä kuvatulla tavoin hallituksen esityksen – vaikutusarviointeineen - valtioneuvostolle ja eduskunnalle. Esityksen perusteella ratkaistaan, hyväksytäänkö ehdotettu sääntely. Vaikka hallituksen esitykseen ei sisällytetä kaikkea kerättyä aineistoa vaikutusarvioinnin toteutuksesta ja tuloksista, on kaikki kerätty tieto tarvittaessa mahdollista saattaa päätöksenteon tueksi.[41]

Hyväksytyn säännöksen jälkeen seuraa viimeinen vaihe; seurantavaihe. Jälkiseuranta onkin vaikutusarvioinnin yksi merkittävimmistä tehtävistä[42], vaikka se on käytännössä usein jäänytkin toteuttamatta.[43] Jälkiseurannalla tarkoitetaan uuden lain täytäntöönpanon vaikutusten seu-

---

vaikutettaisiin eri tahojen toimintatapoihin. Muina vaihtoehtoina Tala mainitsee mm. itsesääntelyn, kuten sopimusjärjestelyt julkisten ja yksityisten toimijoiden kesken. *Tala* 2012, s. 5.

[37] *Oikeusministeriö* 2007, s. 43–55.

[38] *Oikeusministeriö* 2007, s. 11.

[39] *Oikeusministeriö* 2007, s. 11; *Oikeusministeriö* 2018, s. 23–24.

[40] *Oikeusministeriö* 2007, s. 12.

[41] *Oikeusministeriö* 2007, s. 12.

[42] Ks. lainsäädännön arviointineuvoston aloite lainsäädännön jälkiarviointijärjestelmästä. Valtioneuvostotasoinen järjestelmä määrittäisi lait mistä jälkiarvioinnit tehtäisiin, sekä jälkiarvioinnin yleiset periaatteet, miten niitä laadittaisiin, kenen toimesta, rahoituksesta ja valvonnasta. *Lainsäädännön arviointineuvosto* 2019, s. 1.

[43] Ks. *Määttä* 2003, s. 77.

rantaa; jälkiseurannan tarkoituksena on selvittää miten asetettuihin tavoitteisiin on päästy, ovatko vaikutukset olleet odotetunlaiset, arvioidaan lain toimivuutta, onko mahdollisesti ilmennyt jotain odottamatonta ja millaisia muutostarpeita uusi sääntely on mahdollisesti tuonut. *Lainvalmistelun prosessioppaassa* jälkiseurannan keinoina mainitaan muun muassa tutkimukset ja selvitykset, tilastot, tuomioistuinten ratkaisut hallintoviranomaisten päätökset ja käytännöt, kuulemis- ja keskustelutilaisuudet sekä kyselyt ja muu palautteen kerääminen.[44] Seurannan tuloksista kootaan jälkiseurantaraportti, jota voidaan hyödyntää myös tulevien säädösvalmisteluiden yhteydessä.[45] Seurannasta vastaa säädösvalmistelusta vastannut ministeriö.[46] Myös lainvalmistelun prosessiopas ottaa kantaa lain täytäntöönpanoon ja vaikutusten seurantaan. Lainvalmistelun prosessioppaan mukaan, lain täytäntöönpano ja vaikutusten seuranta tulee toteuttaa kattavasti, oikea-aikaisesti ja järjestelmällisesti, lisäksi saaduissa tuloksissa on huomioitava laille asetetut tavoitteet ja arvot. Saadut tulokset on kirjattava siten, että ne ovat myös myöhemmin todennettavissa.[47]

2.3 Yritysvaikutusten arviointi

2.3.1 Yritysvaikutusten arviointi osana taloudellisia vaikutuksia

Yritysvaikutusten arviointi on osa taloudellisten vaikutusten arviointia. Muita taloudellisen arvioinnin osa-alueita ovat kotitalouksien asema, julkinen talous ja kansatalous. Taloudellisia vaikutuksia arvioidaan, jotta säädöshankkeelle asetetut tavoitteet toteutuisivat. Säädöshankkeen tavoitteina voi olla muun muassa talouskasvu, työllisyyden kehittäminen, yritysten toiminnan ja kilpailukyvyn tukeminen ja kansalaisten hyvinvointi. Valtioneuvoston ohjeiden mukaisesti, taloudelliset vaikutukset voidaan jakaa edelleen välittömiin sekä välillisiin vaikutuksiin. Esimerkkinä välittömistä vaikutuksista mainittakoon sääntelyn aiheuttamat muutokset yritysten verotuksessa, ja välillisinä vaikutuksina muun muassa erilaiset käyttäytymisvaikutukset johtuen sääntelyn aiheuttamien hintojen muutoksista - vaikuttaen edelleen kulutustottumuksiin sekä investointeihin.[48]

Yritysvaikutusten arvioinnin päämääränä on tavoitella yrityksille suotuisaa ja kilpailukykyistä säädösympäristöä. Jotta tämä toteutuisi, arvioinneissa on huomioitava miten säädösehdotus

[44] *Lainvalmistelun prosessiopas* 2013, kohta Seuranta.
[45] Ks. esimerkki jälkiseurantaraportista *Valtiontalouden tarkastusvirasto* 2018.
[46] *Lainvalmistelun prosessiopas* 2013, kohta Täytäntöönpano ja Seuranta.
[47] *Lainvalmistelun prosessiopas* 2013, kohta Täytäntöönpano ja Seuranta.
[48] *Oikeusministeriö* 2007, s. 16.

toteutuessaan tulisi vaikuttamaan yrityksiin niin lyhyen kuin pitkän ajan kuluessa, sekä huomioida näiden hyöty- että haittavaikutukset.[49]

2.3.2 Yritysvaikutusten kartoittaminen ja sisältö

Yritysvaikutusten merkittävyyden arviointi on keskeistä vaikutusten kokonaiskuvan saamiseksi. Yritysvaikutukset katsotaan merkittäviksi silloin kun ne kattavat kaikki yritykset, huomattavan osan yrityksistä, tai silloin kun ne kohdistuvat rajatun yritysjoukon toimintaan, toimintaedellytyksiin, markkinoihin, tai kansantalouteen. Jotta merkittävyyttä on mahdollista arvioida, tulee selvittää, minkälaisia yrityksiä sääntely koskee, paljonko sääntelyn alaisia yrityksiä on ja eroaako sääntelyn vaikutukset erilaisten yritysten välillä. Jos tulokset osoittavat sääntelyn yritysvaikutuksiltaan merkittäväksi, niiden mahdolliset vaikutukset tulee selvittää perusteellisesti.[50] Merkittävyyden kannalta on myös ensiarvoisen tärkeää kartoittaa yritysten nykyinen toimintaympäristö sekä markkinat; yritysten asiakaskunta, tyypilliset sopimuskumppanit, tuotannon hinnoittelu, markkinoille pääsy, sekä alan vallitseva kilpailutilanne. Mikäli nykytilaa ei selvitetä, tulevien muutosten vaikutuksia ei voida luotettavasti arvioida, eivätkä yritykset pysty ennakoimaan tulevia muutoksia yritystoiminnassaan.[51] Yritysvaikutusten vaikutusarvioinneissa tulisikin tuoda selkeästi esille hyöty-kustannussuhde sekä lakiesityksen keskeiset vaikutukset. Lainsäädännön arviointineuvoston lausunto valtion yhtiöomistuksesta toimii asiasta hyvänä esimerkkinä:

> *”esitysluonnoksen yritysvaikutuksista ei käy ilmi, mitä taloudellisia vaikutuksia lakiesityksellä on kehitysyhtiöön siirrettäville yrityksille. Luonnoksessa ei myöskään käsitellä sitä, millaisia laajempia kokonaistaloudellisia hyötyjä tai kustannuksia seuraa kehitysyhtiön ta*[52]*.”*[53]

Välittömien ja välillisten vaikutusten lisäksi sääntelymuutosten myötä yrityksille voi aiheutua sekä liiketoiminnallisia että hallinnollisia kustannuksia. *Liiketoiminnallisilla kustannuksilla* tarkoitetaan kertaluontoisia tai jatkuvia investointeja, jotka voivat kohdistua esimerkiksi tietojärjestelmiin tai henkilöstöön. Toisaalta sääntelymuutos voi vaikuttaa myös yrityksen liiketoiminnan tutkimus- ja kehitystoimintaan, joko vähentämällä tai lisäämällä investointeja -

[49] *Oikeusministeriö* 2007, s. 9–8.
[50] Joskus voi olla myös tarpeen tehdä tarkastelu tietyntyyppisiä kohdeyrityksiä silmälläpitäen, erityisesti silloin kun kysymyksessä on pieniin yrityksiin kohdistuva uusi sääntely. *Oikeusministeriö* 2007, s. 18.
[51] *Oikeusministeriö* 2007, s. 18 ja 20.
[52] *Lainsäädännön arviointineuvoston lausunto (VNK/1581/30/2016)* 2016, s. 1.
[53] Ks. myös *Keinänen – Halonen* 2017, s. 10.

vaikuttaen esimerkiksi uusiin innovaatioihin.[54] *Hallinnollisilla kustannuksilla* tarkoitetaan yritysten jatkuvaluonteisia kustannuksia, joita ovat muun muassa viranomaisille tai kolmansille osapuolille toimitetut tiedot yrityksen toiminnasta tai tuotantotavoista. Hallinnollisten kustannusten selvittäminen on tärkeää, jotta voidaan nähdä minkälaista *hallinnollista taakkaa* ne aiheuttavat yritysten kokoon nähden.[55] Sääntelyn hallinnollinen taakka korostuu yleensä eniten pienien ja uusien yritysten kohdalla[56], kohdistuen siten valtaosaan suomalaisista yrityksistä (Suomen yrityksistä pieniä ja keskisuuria yrityksiä (jäljempänä ”*pk-yritys*”)[57] on 99,8 %).[58]

Sääntelyllä voi olla yrityksille kilpailuoikeudellisia vaikutuksia, jonka vuoksi vaikutusarvioinnissa tulee tunnistaa sääntelyn mahdolliset vaikutukset yritysten väliseen kilpailuun. Jos tulevan lain katsotaan estävän, rajoittavan tai vääristävän kilpailua, se tulee huomioida sääntelyn toteutuksessa.[59] Sääntelyn tulisi kannustaa yrittäjyyteen ja yritysten kasvumahdollisuuksiin. Kilpailuoikeudelliset vaikutukset kattavat myös kansainvälisen näkökulman. Kansallisella sääntelyllä voidaan vaikuttaa yritysten rajatylittävään kilpailuun, niin EU:ssa kuin kolmansissa maissa. Lisäksi on erityisen tärkeää huomioida, etteivät eri maiden yritykset joudu keskenään eriarvoiseen asemaan Suomen sääntelystä johtuen, ja toisaalta siihen, että suomalaiset markkinat toimintaympäristönä pysyisivät kiinnostavina ja mahdollisina myös ulkomaalaisille yrityksille.[60]

2.3.3 Yritysvaikutusten esittäminen ja tiedonlähteet

Yritysvaikutuksia on mahdollista arvioida sekä määrällisesti että laadullisesti. Lähtökohtaisesti arviot tulisi esittää euromääräisesti silloin, kun siihen on mahdollisuus, esimerkiksi hallinnollisia kustannuksia esitettäessä.[61] Euromääräisyyden tarpeeseen on kiinnittänyt huomiota

[54] *Oikeusministeriö* 2007, s. 20.
[55] Hallinnollinen taakka koostuu yrityksen toimista, jotka tehdään vain lainsäädännön velvoittamina. Vaikka hallinnollinen taakka on osa hallinnollisia kustannuksia, on huomattava etteivät kaikki hallinnolliset kustannukset ole hallinnollista taakkaa, vaan ns. *business-as-usual- kustannuksia*, mitkä aiheutuvat tavanomaisen liiketoiminnan järjestämisestä. *Työ- ja elinkeinoministeriö* 2012, s. 7; *Kangasharju – Rauhanen* 2008, s. 12–16.
[56] *Oikeusministeriö* 2007, s. 19.
[57] Mikroyritysten sekä pienten ja keskisuurten yritysten (”pk-yritysten”) luokka koostuu yrityksistä, joiden palveluksessa on vähemmän kuin 250 työntekijää ja joiden vuosiliikevaihto on enintään 50 miljoonaa euroa; Komission suositus mikroyritysten sekä pienten ja keskisuurten yritysten määritelmästä (2003/361/EY) artikla 2.
[58] Tilastokeskuksen yritysrekisterin mukaan, Suomessa oli vuonna 2017 mikroyrityksiä 264 519 (93,2 %), pienyrityksiä 15 989 (5,6 %), keskisuuria 2 883 (1,0 %) ja suuryrityksiä 615 (0,2 %). *Suomen Yrittäjät* 2019, kohta Yrittäjyys Suomessa.
[59] *Oikeusministeriö* 2007, s. 19.
[60] *Oikeusministeriö* 2007, s. 21.
[61] *Oikeusministeriö* 2007, s. 25.

myös lainsäädännön arviointineuvosto useissa lausunnoissaan.[62] Jos määrällisen arvion tekeminen ei ole mahdollista, kuten käsiteltäessä yritysten kilpailukykyä tai markkinoiden toimivuutta, tulee arvio tehdä laadullisesti. Yritysvaikutusten arvioinnissa tiedonlähteinä voi Valtioneuvoston ohjeiden mukaan hyödyntää esimerkiksi Tilastokeskuksen yritysrekisteriä, elinkeinoelämän järjestöjä, yrityskyselyjä sekä kilpailuviranomaisten asiantuntijuutta.[63]

2.4 Vaikutusarvioinneista yleisesti

2.4.1 Vaikutusarvioinnin huomiointi EU sääntelyssä ja kansainvälisten velvoitteiden hyväksynnässä

Unionin jäsenmaana, Suomen lainsäädäntö rakentuu sekä kansallisesta että unionin tason säännöksistä. EU sääntelyn lisäksi, myös kansainväliset monen maan väliset sopimukset ovat Suomessa voimassa olevaa oikeutta. Vaikutusarvioinnit ovat siten merkittävä osa myös unionin säännösten sekä kansainvälisten velvoitteiden valmistelua ja täytäntöönpanoa.[64] Vaikutusarviointi on sisällytetty myös unionin toimielinten väliseen sopimukseen paremmasta lainsäädännöstä.[65] Paremman sääntelyn avulla toimielimet tavoittelevat yksinkertaisempia sääntöjä saadakseen tehokkaampia tuloksia, esimerkiksi vähentämällä *sääntelytaakkaa* ja liiallista byrokratiaa[66]. Vaikutusarviointia käsitelläänkin sopimuksessa paremman lainsäädännön välineenä. Sopimuksen 3 luvun kohta 12 mukaan, vaikutusarvioinnit edesauttavat tietoon perustuvan päätöksen teossa sekä parantavat unionin lainsäädännön laatua. Vaikutusarviointien avulla varmistetaan korkealaatuinen unionin lainsäädäntö, ja vahvistetaan unionin talouden kilpailukykyä ja kestävyyttä[67]. Komission vaikutusarvioinnissa korostuvat kaksi tärkeää Euroopan unionin toiminnasta tehdyn sopimuksen (SEUT)[68] mukaista periaatetta; *toissijaisuusperiaate* sekä *suhteellisuusperiaate*.[69] Toissijaisuusperiaatteen mukaan jäsenmaat hoitavat kansallisesti kaiken sen mihin EU tason toimia ei tarvita. Suhteellisuusperiaatteen mukaan

[62] Ks. jäljempänä kappale 2.4.3. Lainsäädännön arviointineuvosto.
[63] *Oikeusministeriö* 2007, s. 26.
[64] Vuoden 2003 jälkeen komissiossa on valmisteltu 975 vaikutusarviointia. *COM (2016) 615, lopull.*, s. 8.
[65] Euroopan parlamentin, Euroopan unionin neuvoston ja Euroopan komission välinen toimielinten sopimus paremmasta lainsäädännöstä (EUVL L 123, 12.5.2016, s. 1–14)
[66] mm. tietosuoja-asetuksen korvatessa 28 eri jäsenvaltion lakia, uskottiin sen vähentävän hallinnollista taakkaa ja helpottavan yritysten pääsyä markkinoille. Hyötyjen arvioitiin olevan vuosittain noin 2,3 miljardia euroa. *COM (2016) 615, lopull.*, s. 7.
[67] Ks. Sopimus paremmasta lainsäädännöstä johdantolause 2 ja 6.
[68] Sopimus Euroopan unionin toiminnasta, tehty 13 päivänä joulukuuta 2007 (Konsolidoitu toisinto 2016; EUVL *C 202, 7.6.2016, s. 1–388*).
[69] SEUT Pöytäkirja (N:o 2): Toissijaisuus- ja suhteellisuusperiaatteen soveltamisesta (Konsolidoitu toisinto 2016; EUVL C 202, 7.6.2016, s. 206–209).

EU:n toimet tulee toteuttaa siten, ettei tehdä enempää kuin on tarpeen tavoitteiden toteuttamiseksi.

Komission laatimien paremman sääntelyn oheistuksissa (”*Better Regulation Guidelines*”) käsitellään yleisellä tasolla vaikutusarvioinnin tarvetta ja sisältöä.[70] Vaikutusarviointiohjeistusten soveltamisen tulkintaa on täydennetty komission erillisillä ohjeilla (”*Better regulation Toolbox*”), joissa kuvataan seikkaperäisemmin vaikutusarvioinnin tarpeen arviointia ja toteutusta.[71] Ohjeet ovat tarkoitettu lainsäädäntötyötä valmisteleville ja täytäntöönpanon valvontaa toteuttaville komission viranomaisille, mutta niissä on huomattavan paljon yhdenmukaisuutta kansallisten valtioneuvoston antamien ohjeiden kanssa. Komission ohjeiden mukaan vaikutusarviointeja tulee tehdä lainsäädäntöaloitteista, joista on odotettavissa merkittäviä taloudellisia, sosiaalisia tai ympäristövaikutuksia.

Vaikutusarvioinneissa on esitettävä selkeästi, johdonmukaisesti ja kokonaisvaltaisesti keihin vaikutukset kohdistuisivat ja mitä vaikutuksia lainsäädäntöehdotuksella olisi. Arvioinneissa on huomioitava niin suorat kuin epäsuorat vaikutukset, sekä eriteltävä oletettavat olennaiset vaikutukset kohdistettuna taloudelle, yhteiskunnalle ja ympäristölle. Arvioinneissa on lisäksi nimenomaisesti mainittava, jos jollekin osa-alueista ei ole odotettavissa merkittäviä vaikutuksia. Vaikutusarviointiraportissa on huomioitava myös mahdolliset vaikutukset pk-yrityksille, sekä vaikutukset kilpailukykyyn. Vaikutusarviointien tarkoituksena on selvittää mahdollisten ongelmien laajuus, niiden mahdolliset seuraukset ja kartoittaa unionilta vaadittavat toimet ongelmien pienentämiseksi. Lisäksi arviointien avulla selvitetään ratkaisuja, ja kartoitetaan mahdollisimman yksityiskohtaisesti esityksen aiheuttamat lyhyen ja pitkän aikavälin kustannukset.[72] Vaikutusarviointeja toteutettaessa olisi huomioitava, että pienet haitalliset vaikutukset saattavat olla merkittäviä tai kulminoitua merkittäviksi esimerkiksi jonkin tietyn sektorin olemassa olevien olosuhteiden vuoksi tai pk-yritysten kohdalla.[73] Arvioinnit tuleekin siten tehdä aina tapauskohtaisesti, eikä niiden toteuttamista varten voi tämän vuoksi antaa kaikkiin tilanteisiin sopivia määräyksiä.[74] Komission ohjeiden mukaan, vaikutusarviointien tulisikin

[70] Ks. ohjeistuksia tarkemmin *Euroopan komissio - Better Regulation Guidelines* 2017, s. 23–28 ja 30.
[71] Ks. ohjeistuksia tarkemmin *Euroopan komissio- Toolbox* 2017, luvut 2 ja 3.
[72] Ks. Sopimus paremmasta lainsäädännöstä kohta 12; *Euroopan komissio - Better Regulation Guidelines* 2017, s. 14–15.
[73] *Euroopan komissio - Toolbox* 2017, s. 48–51.
[74] *Euroopan komissio - Better Regulation Guidelines* 2017, s. 16–17.

olla oikein toteutettuna kattavia, oikeasuhteisia, näyttöön perustuvia, avoimia sidosryhmien näkemyksille sekä puolueettomia.[75]

Paremman sääntelyn toteuttamiseksi, toimielinten välisessä sopimuksessa huomioidaan myös lainsäädännön jälkiseuranta, eli niin sanotut toimivuustarkastukset (”*fitness checks*”). EU:n toimivuustarkastuksilla edistetään lainsäädännön tavoitteisiin pääsemistä ja toteutetaan unionin lainsäädännön tuloksellisuuden arviointia.[76]

Suomen valtioneuvosto ja ministeriöt seuraavat vireillä olevia EU - säädöshankkeita ja pyrkivät arvioimaan niiden vaikutuksia Suomelle. Kansallisissa EU liitännäisissä säädöshankkeissa vaikutusarvioinnin laatimisen tukena hyödynnetään soveltuvin osin komission laatimaa vaikutusarviointia[77]. EU säännösten kansallinen vaikutusarviointi on tärkeää, sillä komission laatima arvio vaikutuksista on harvoin riittävä huomioimaan sääntelyn tuomia mahdollisia erityisvaikutuksia Suomelle tai muille pienille jäsenvaltioille[78]. Säädösvalmistelusta vastuussa oleva ministeriö laatii komission ehdotuksesta perusmuistion[79], sekä U- tai E – kirjelmän[80]. Kansainvälisten velvoitteiden täytäntöönpanossa hyödynnetään siten säädösvalmistelua koskevia Valtioneuvoston ohjeita soveltuvin osin.[81]

2.4.2 Tiedonlähteet ja menetelmät

Riittävän kattava ja laaja-alainen vaikutusarvio vaatii toteutuakseen paljon taustatyötä. Lähteinä vaikutusarvioinneissa voidaan käyttää samoja keinoja kuin jälkiseurannassa; tutkimuksia ja selvityksiä, tilastoja, tuomioistuinten ratkaisuja, hallintoviranomaisten päätöksiä ja seurantatietoja. Myös kuulemis- ja keskustelutilaisuuksien järjestäminen, sekä lausuntopyyntöjen esittäminen sääntelyn kohderyhmiltä ja asiantuntijoilta on tärkeää. Hyödyllisiä ovat myös aikaisemmat vastaavat hankkeet, niitä koskevat tutkimukset sekä komission ja muiden maiden tekemät vaikutusarvioinnit – erityisesti EU liitännäisissä asioissa.[82]

---

[75] *Euroopan komissio - Better Regulation Guidelines* 2017, s. 30.
[76] Ks. Sopimus paremmasta lainsäädännöstä kohta 6 ja 20; Ks. myös tarkemmat elementit toimivuustarkastuksen vaatimuksista *Euroopan komissio - Better Regulation Guidelines* 2017, s. 50–67.
[77] Esimerkiksi komission vaikutusarviointi tietosuoja-asetuksesta huomioitiin kansallisen tietosuojasääntelyn kokonaisuudistuksessa. Ks. *HE 9/2018 vp*, s. 66.
[78] Ks. *Lång* 2016, s. 5 ja 8.
[79] *Oikeusministeriö* 2007, s. 14.
[80] Ks. mainituista U- ja E-asioista tarkemmin *Oikeusministeriö* 2011, s. 14–35. Ks. myös perusmuistion laatimisesta tarkemmin *Oikeusministeriö* 2010, s. 17–18 ja 62–65.
[81] *Oikeusministeriö* 2007, s. 14.
[82] *Lainvalmistelun prosessiopas* 2013, kohta Täytäntöönpano ja Seuranta; *Oikeusministeriö* 2007, s. 14.

2.4.3 Lainsäädännön arviointineuvosto

15.4.2016 alkaen vaikutusarviointien laadun varmistamiseksi, valtioneuvoston kanslian yhteydessä on toiminut riippumaton ja itsenäinen *lainsäädännön arviointineuvosto*. Arviointineuvoston toiminnasta säätää valtioneuvoston asetus lainsäädännön arviointineuvostosta (1735/2015 vp). Lainsäädännön arviointineuvoston toimenkuvaan kuuluu sen toiminnasta säätävän asetuksen 2 §:n mukaisesti lausuntojen antaminen hallituksen esitysluonnoksista ja niitä koskevista vaikutusarvioinneista sekä arvioida lainsäädännön vaikutusten toteutumista. Huomattavaa on, ettei arviointineuvoston toimenkuvaan kuulu antaa uusia ohjeita tai vaatimuksia vaikutusarviointien toteuttamiseksi, vaan se tukeutuu arvioinneissaan vahvasti Valtioneuvoston ohjeisiin koskien hallituksen esityksen laatimista sekä säädösehdotusten vaikutusarviointeja.[83]

Arviointineuvoston lausunnot voidaankin nähdä ministeriöiden toimintaa tukevana ja neuvoa antavana toimintana. Lisäksi, itsenäisenä toimijana, arviointineuvosto valitsee itse lausuttavat esitykset ja säädösluonnokset, joista se antaa kehittämisehdotuksensa ja kommenttinsa. Valinnoissaan arviointineuvosto kertoo painottavansa esityksen taloudellista ja yhteiskunnallista merkittävyyttä[84]. Käytännössä arvioitaviksi päätyvät usein yhteiskunnallisesti merkittävimmät säädöshankkeet, jotka lienevät myös tavanomaista haastavimpia.[85] Ministeriöt eivät kuitenkaan ole sidottuja arviointineuvosto antamille lausunnoille, vaan ne voivat harkintansa mukaan huomioida ja hyödyntää saamiaan arviointeja. Jos käsittelyssä oleva säädösehdotus on ollut arviointineuvoston käsittelyssä, tulee tämä kuitenkin mainita hallituksen esityksessä, mainittava on myös, miten arviointineuvoston lausunto on huomioitu. Lainsäädännön arviointineuvoston tekemän selvityksen mukaan, noin kaksi kolmasosaa sen antamista parannusehdotuksista oli huomioitu[86]. Valitettavaa oli, ettei esityksistä ilmennyt, kuinka lausunnot oli huomioitu[87]. Tämä voidaan nähdä merkittävänä puutteena säädösvalmistelun avoimuudelle.

Muun muassa lausunto luonnoksesta hallituksen esitykseksi eduskunnalle koskien uutta tietosuojalakia (1050/2018) arviointineuvosto katsoi esitysluonnoksen sisältävän merkittäviä

[83] *Keinänen – Halonen* 2017, s. 6.
[84] *Lainsäädännön arviointineuvosto* 2017, s. 9.
[85] *Keinänen – Halonen* 2017, s. 22.
[86] *Lainsäädännön arviointineuvosto* 2016, s. 11.
[87] *Keinänen – Halonen* 2017, s. 18–19.

puutteita[88]. Arviointineuvoston antamista kymmenestä korjauskehotuksesta lopullisessa esityksessä oli huomioitu kuusi ja neljä vain osittain. Annettuihin huomioihin perustuen, lopullisessa hallituksen esityksessä esitellään laajemmin ja monipuolisesti myös Asetuksen yritysvaikutuksia, sekä Asetuksen yrityksille aiheuttamia hyötyjä ja haittoja. Lopullisesta esityksestä jäi vielä puuttumaan selkeät sääntelyn kohdetahot.[89]

Arviointineuvosto laatii vuosittain vuosikatsauksen, joissa on esitettynä arviointineuvoston arvio hallituksen esitysluonnoksista. Yleisimmät esitysluonnosten puutteet ovat koskeneet vaikutusten määrällistä arviointia, toteuttamisvaihtoehtojen kuvausta, kustannusten ja hyötyjen kuvausta, sekä vaikutusten ryhmittelyä vaikutusarvio-ohjeiden mukaisesti.[90] Arviointineuvoston mukaan vuonna 2017 merkittävä osa esitysluonnoksista sisälsi huomattavia puutteita[91]. Vuotta myöhemmin esitysluonnosten taso näyttää parantuneen[92], mutta uusina korostuneina haasteina, edellisistä vuosista poiketen, nousi esille riskien ja ongelmien kuvaus, vaikutusmekanismit sekä välilliset vaikutukset.[93]

On kuitenkin huomattava, että eri esitysluonnosten välillä voi olla merkittäviä eroja, laadukkaista kokonaisuuksista esityksiin, joissa on todettu merkittäviä puutteita.[94] Kaikissa tapauksissa, arviointineuvoston lausunnot toimisivat parhaimmillaan ministeriöille oikein hyödynnettäessä arvokkaina palautteina ja tiedonlähteinä.[95] Arviointineuvostolla on myös tärkeä rooli

[88] Merkittävimpinä puutteina mainittiin mm. tietosuoja-asetuksen sisällön puuttuminen, kohderyhmien erittelyn vajavaisuus, osin vaikealukuisuus, ja vaikutusarvioiden riittämätön käsittely. *Lainsäädännön arviointineuvoston lausunto (VNK/133/32/2018)* 2018, s. 1.
[89] *Valtioneuvoston selvitys* 2019, s. 64–65 ja 111–112.
[90] Ks. lainsäädännön arviointineuvoston vuosikatsaukset *Lainsäädännön arviointineuvosto* 2016, s. 6; *Lainsäädännön arviointineuvosto* 2017, s. 15; *Lainsäädännön arviointineuvosto* 2018, s. 17.
[91] Vrt. STM:n esitysluonnos laiksi vakuutusten tarjoamisesta. *Lainsäädännön arviointineuvosto* 2017, s. 11.
[92] Lainsäädännön arviointineuvosto antoi vuonna 2018 yhteensä 28 lausuntoa, joista 9 vastasi pääosin valtioneuvoston ohjeita säädösehdotuksen vaikutusarvioinnista. *Lainsäädännön arviointineuvosto* 2018, s. 12 ja 16.
[93] *Lainsäädännön arviointineuvosto* 2018, s. 17; Ks. myös *Keinänen – Halonen* 2017, s. 6-15, jossa esitysluonnosten ja arviointineuvoston antamien lausuntojen tarkempi selvitys osoittaa, että lausunnoissa korostuu myös erityisesti perusteluiden kestävyys, esitystekniset seikat, vaikutusten kohdentuminen, sekä laaja-alaisuus ja suunnitelmallisuus.
[94] Ks. esim. Lausunto luonnoksesta hallituksen esitykseksi eduskunnalle yrittäjävähennyksen säätämiseksi *Lainsäädännön arviointineuvoston lausunto (VNK/1644/03.02.00/2016)* 2016, s.2; Ks. myös lausunto luonnoksesta hallituksen esitykseksi eduskunnalle laeiksi sairasvakuutuslain, lääkelain 57 b ja 102 §:n sekä terveydenhuollonammattihenkilöstöstä annetun lain 22 ja 23 §:n muuttamisesta *Lainsäädännön arviointineuvoston lausunto (VNK/1641/03.02.00/2016)* 2016, s. 3; Ks. myös lausunto luonnoksesta hallituksen esitykseksi eduskunnalle liikennekaaresta *Lainsäädännön arviointineuvoston lausunto (VNK/1189/03.02.00/2016)* 2016, s. 4.
[95] Vrt. jos hallituksen lopullinen esitys julkaistaan jo kuukauden päästä lainsäädännön arviointineuvoston lausunnon antamisesta, on oletettavaa ettei lausuntoa ole oletettavasti keritty huomioimaan esityksessä. Ks. *Lainsäädännön arviointineuvosto* 2016, s. 11.

sääntelyn jälkiseurannassa; se voi omasta aloitteestaan arvioida, miten hyvin voimaan saatetun säädöksen vaikutukset ovat toteutuneet.[96]

2.5 Yhteenveto

Yritysvaikutusten arviointi osana sääntelyä voi parantaa lainsäädännön laatua ja edistää sille asetettujen tavoitteiden toteutumista. Taustalla vaikuttavat niin oikeusvaltioperiaatteiden kuin perusoikeuksien turvaaminen, mutta myös yhteiskunnan kehittäminen ja uudistaminen ajantasaiseksi. Hyvissä ajoin toteutettu vaikutusarviointi antaa yrityksille mahdollisuuden vaikuttaa lain sisältöön asiantuntijalausuntojen muodossa. Saatu etukäteistieto yritysvaikutuksista auttaa yrityksiä myös valmistautumaan tuleviin muutoksiin, mikä edesauttanee edelleen lain velvoitteiden täytäntöönpanoa. Lisäksi arvioitujen yritysvaikutusten julkaiseminen jo valmisteluvaiheessa helpottaa tulevien muutosten ymmärrettävyyttä ja merkittävyyttä, sekä luo luottamusta ja varmuutta lain täytäntöönpanoa kohtaan.[97]

Komission esittämät vaikutusarvioinnit kattavat luonnollisesti kaikki jäsenmaat. Kaikkia jäsenmaita koskevina, komission vaikutusarvioinnit voidaan katsoa olevan melko yleisellä tasolla toteutettuja, eivätkä ne välttämättä palvele yksittäisissä jäsenmaissa toimivia yrityksiä. Tämän vuoksi Suomen kansallisten viranomaisten ja oikeusministeriön rooli sääntelyn täytäntöönpanon arvioinnissa, valvonnassa ja yritysten ohjaamisessa korostuu.[98] Sääntelyn kansallisen jälkiseurannan merkitys yrityksille onkin huomattava. Jos sääntelyn täytäntöönpanossa havaitaan haasteita, joita ei ole sääntelyä suunnitellessa otettu huomioon tai mikäli asetettuihin tavoitteisiin ei ole päästy, lainsäädäntöviranomaiset voivat aloittaa toimenpiteet tilanteen korjaamiseksi. Ilman vaikutusten toteutumisen arviointia, moni epäkohta lainsäädännön toteutuksessa voisi jäädä huomaamatta ja siten myös korjaamatta. Epätoivottujen vaikutusten huomioimattomuus voi pahimmillaan aiheuttaa yrityksille tarpeetonta hallinnollista taakkaa tai markkinahäiriöitä yritysten väliseen kilpailuun.[99]

---

[96] *Valtioneuvoston kanslia*, kohta Tehtävät ja toimintatavat.
[97] *Oikeusministeriö* 2007, s. 7–9.
[98] *Oikeusministeriö* 2007, s. 13–14.
[99] *Määttä*, 2016. s. 33–51.

3 REKISTERINPITÄJÄN VELVOLLISUUKSISTA JA NIIDEN AIHEUTTAMISTA KUSTANNUKSISTA YLEENSÄ

3.1 Asetuksen vaikutus yritysten toimintaan

Luonnollisten henkilöiden oikeus henkilötietojen suojaan ja mahdollisuus siirtää henkilötietojaan vapaasti ja turvallisesti unionissa taataan Euroopan unionin perusoikeuskirjan[100] artiklassa 8 sekä SEUT artiklassa16. Asetuksen tarkoituksena on artiklan 1 mukaisesti toteuttaa näitä perusoikeuksia ja siten suojella ja parantaa luonnollisten henkilöiden oikeutta turvalliseen henkilötietietojen käsittelyyn, sekä taata ja edistää henkilötietojen vapaata liikkuvuutta. Asetusta sovelletaan henkilötietojen käsittelyyn, pois lukien oikeushenkilöiden ja luonnollisten henkilöiden henkilökohtainen tai kotitaloutta koskeva henkilötietojen käsittely. Lisäksi, Asetus sääntelee muun muassa milloin henkilötietojen kerääminen ja käsittely on sallittua, henkilötietojen käsittelyyn liittyvistä rajoituksista[101] ja velvollisuuksista, sekä määrittelee henkilötietojen käsittelyssä vastuulliset tahot.

Asetuksen mukaan vastuulliset tahot henkilötietojen käsittelyssä ovat Rekisterinpitäjät[102] sekä henkilötietojen käsittelijät (jäljempänä ”*Henkilötietojen käsittelijä*”[103]), joiden toimintaa valvotaan viranomaiskeinon.[104] Rekisterinpitäjänä toimiva yritys tai organisaatio määrittelee mihin tarkoitukseen ja millä tavalla henkilötietoja käsitellään. Rekisterinpitäjä voi olla esimerkiksi jäsenistään tietoja keräävä yhdistys, potilastietoja käsittelevä sairaala, verkkokauppa tai sosiaalisen median palvelu.[105] Käsitteen määritelmä on merkittävä Asetusta sovellettaessa, sillä Asetus määrittelee kulloinkin henkilötietojen käsittelystä vastuussa olevan tahon. Yrityksen vastuu ja sitä koskevat velvollisuudet tietosuojasääntelyn noudattamisesta ovat ym-

[100] Euroopan unionin perusoikeuskirja (2010/C83/02), EUVL C 83, 30.3.2010.
[101] Muun muassa erityisten henkilötietoryhmien, kuten terveystietojen käsittely on lähtökohtaisesti kiellettyä. Jotta käsittely olisi sallittua, tulee siitä olla poikkeussäännös Asetuksessa tai kansallisessa lainsäädännössä. Tutkielmassa ei paneuduta erityisiin henkilötietoryhmiin tämän tarkemmin. Ks. aiheesta tarkemmin Asetuksen artiklasta 9.
[102] Rekisterinpitäjän määritteleminen on osoittautunut käytännöntasolla epäselväksi, linjaa on haettu myös oikeuskäytännöstä. Ks. komission ennakkoratkaisupäätös tapauksessa, jossa Facebookin fanisivuja ylläpitävää saksalaista yritystä pidettiin Rekisterinpitäjänä yhdessä Facebookin kanssa. C-40/17 *Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV Oberlandesgericht Düsseldorf* ECLI:EU:C:2019:629, kohdat 64 ja 85.
[103] Henkilötietojen käsittelijällä tarkoitetaan Asetuksen artiklan 4.8 mukaisesti luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, joka käsittelee henkilötietoja Rekisterinpitäjän lukuun.
[104] Huomattavaa, että kyseessä voi olla myös yritysten tai organisaatioiden yhteistyö, jossa tahot yhdessä päättävät henkilötietojen käsittelystä; heidän osalta puhutaan ns. *yhteisrekisterinpitäjistä*.
[105] Ks. tapaus Jehovan todistajat, jossa punninnassa oli mm. voitiinko yhdyskuntaa pitää Rekisterinpitäjänä C-25/17 *Tietosuojavaltuutettu v Jehovan todistajat — uskonnollinen yhdyskunta* ECLI:EU:C:2018:551, kohta 75.

märrettävissä Asetuksen käsitteiden määritelmien kautta.[106] Vastuukysymykset voivat realisoitua myös tutkielman näkökulmasta hyvin merkityksellisessä tilanteessa yrityksen ulkoistaessa osan henkilötietojensa käsittelystä toiselle yritykselle, jolloin kysymyksen asettelu koskee Asetuksen artiklan 28 mukaista Rekisterinpitäjän ja Henkilötietojen käsittelijän välistä suhdetta.

Asetuksen määrittelemät Rekisterinpitäjän velvollisuudet koskettavat kaikkia yrityksen käsittelemiä henkilötietoja riippumatta siitä, koskevatko tiedot yksityishenkilöitä, yhteistyökumppaneita, asiakkaita tai oman henkilöstön tietoja. Uudistunut tietosuojasääntely koskettaa siten erityisesti yrityksiä, joiden liiketoiminta perustuu suurissa määrin yksityishenkilöiden henkilötietojen käsittelyyn, kuten vähittäiskauppa, finanssi-, media-, ja terveydenhuoltoalan yritykset sekä IT- palveluyritykset ja teleoperaattorit.[107] Yritystoiminnan käytännön toteuttaminen vaatii usein myös yhteistyötä eri toimijoiden välillä. Oli sitten kyse finanssi- tai terveydenhuoltoalan edustajasta, toimien ulkoistaminen, palveluiden hankinta ja myyminen toiminnan edistämiseksi ja ylläpitämiseksi ovat osa yritysten arkea. Mainittujen toimien toteuttamiseksi yritysten välinen konsensus kirjataan ylös kaikkia osapuolia sitovana sopimuksena. Sopimuksien sisältämien toimien toteuttaminen voi koostua kokonaan tai osin henkilötietojen käsittelystä. Asetuksen myötä, ulkoistettaessa henkilötietojen käsittely toisen yrityksen tehtäväksi kokonaan tai osin, käsittelystä on solmittava kirjallinen Tietojenkäsittelysopimus Asetuksen artiklan 28 vaatimusten mukaisesti tai sisällytettävä käsittelyn ehdot kirjalliseen palvelusopimukseen. Jotta mainittujen Sopimusvaatimusten yritysvaikutukset tulevat mahdollisimman kattavasti esiteltyä, on ensin selvitettävä yleisemmällä tasolla Asetuksen aiheuttamat velvoitteet ja niistä aiheutuvat kustannukset Rekisterinpitäjille. Tämän myötä on mahdollista selvittää, kuinka suurta hallinnollista kuormaa Asetus Rekisterinpitäjille aiheuttaa ja kuinka suuri osuus tästä kuormasta muodostuu artiklan 28 Sopimusvaatimuksista.

Tässä luvussa käsitellään yritysten eli Rekisterinpitäjien velvollisuuksia ja selvitetään näistä aiheutuvia kustannuksia. Luvun alussa käydään läpi hieman taustatietoa Asetuksesta yleisesti, jonka jälkeen käsitellään tarkemmin Asetuksen yrityksille asettamia velvollisuuksia. Lopuksi aihe nivoutuu yhteen kappaleessa, jossa arvioidaan mainituista velvollisuuksista aiheutuvia kustannuksia. Tutkielman keskittyessä puhtaasti Asetuksen vaikutuksiin yrityksissä, lienee

[106] Ks. myös *Tietosuojatyöryhmä* 2010, s. 4. Huomattavaa etteivät Asetuksen käsitteet ”Rekisterinpitäjä” tai ”Henkilötietojen käsittelijä” määritelmät ole sisällöllisesti muuttuneet Asetusta edeltävästä henkilötietodirektiivin aikaisesta sääntelystä, jota kyseinen lausunto käsittelee.
[107] *Valtioneuvoston selvitys* 2017, s. 2.

tarpeellista painottaa, ettei tutkielmassa käsitellä Asetuksen vaikutuksia julkisen sektorin toimijoille. Seuraavissa luvuissa 4 ja 5 keskitytään tarkemmin artiklan 28 Sopimusvaatimuksiin ja sen aiheuttamiin yritysvaikutuksiin.

3.2 Rekisterinpitäjän velvollisuuksista

3.2.1 Henkilötietojen käsittelyä koskevat periaatteet

Rekisterinpitäjänä toimivan yrityksen on henkilötietojen käsittelyssä noudatettava Asetuksen mukaan yksittäisten säännösten lisäksi henkilötietojen käsittelyä koskevia periaatteita, sekä varmistettava käsittelyn lailliset perusteet. Lisäksi Rekisterinpitäjän on toteutettava kaikki Asetuksen määrittämät Rekisteröidyn oikeudet.

Henkilötietojen käsittelyä koskevat periaatteet on esitelty Asetuksen toisessa luvussa. Periaatteet velvoittavat kaikkia tahoja, jotka käsittelevät henkilötietoja, niin Rekisterinpitäjiä kuin Henkilötietojen käsittelijöitä, riippumatta tietojen käsittelytavasta. Tarkoituksena on, että yritykset käsittelevät tietoja niin, että se kunnioittaa Rekisteröidyn oikeuksia ja vapauksia.[108] Seuraavissa kappaleissa on kerrottuna tarkemmin henkilötietojen käsittelyä koskevista periaatteista.

Asetuksen 5.1 artiklan (a) alakohta määrittelee periaatteet koskien lainmukaisuutta, kohtuullisuutta ja läpinäkyvyyttä. *Lainmukaisuus* tarkoittaa käytännössä sitä, että kaikki henkilötietojen käsittely on pohjauduttava kirjoitettuun lakiin eli käsittelylle on oltava laillinen peruste. Tarkemmin henkilötietojen käsittelyn lainmukaisuuden perusteista on säädetty Asetuksen 2 luvun artikloissa 6 sekä 9-11. Asiaa on tämän lisäksi tarkennettu myös lukuisissa kansallisissa erityislaeissa sekä erityisiä henkilötietoryhmiä koskien myös uudessa tietosuojalain 2 luvussa[109]. Asetuksen 6 artiklan mukaan *lainmukaiset käsittelyperusteet* ovat Rekisteröidyn suostumus; Rekisteröityä koskevan sopimuksen täytäntöönpano; Rekisterinpitäjän lakisääteisen velvoitteen noudattaminen; Rekisteröidyn elintärkeiden etujen suojaaminen; Rekisterinpitäjän julkisen vallan käyttäminen; yleistä etua koskevien toimien toteuttaminen; ja Rekisterinpitäjän tai kolmannen osapuolen oikeutettujen etujen toteuttaminen.[110]

[108] *Talus ym.* 2017, s. 12.
[109] *Korpisaari* 2018, s. 89.
[110] Ks. myös *Korpisaari* 2018, s. 90.

Yritysten on huomioitava henkilötietojen käsittelyssä myös *kohtuullisuus*. Kohtuullisuudella tarkoitetaan tulkintojen mukaan tietyntasoista reiluutta Rekisteröityjä kohtaan. Henkilötietoja on käsiteltävä ennakoitavasti; Rekisteröityjen on voitava luottaa siihen millaista käsittelyä ja tietojen keräämistä Rekisterinpitäjän toiminnasta on kohtuudella odotettavissa. Toisin sanoen yritys ei voi ilman nimenomaista suostumusta kerätä henkilötietoja esimerkiksi varmuuden vuoksi mahdollista tulevaisuuden tarvetta varten, vaan Rekisteröidyn tulee olla tietoinen kaikesta toiminnasta, johon hänen tietojaan käytetään. Kohtuullisuuden periaate onkin sidoksissa käyttötarkoitussidonnaisuuden periaatteeseen.[111]

Henkilötietojen käsittely on käytännössä usein vaikeaselkoista ja näkymätöntä. Tästä tiedollisesta epätasapainosta johtuen, luonnollisten henkilöiden asemaa ja oikeuksia on ollut tarve parantaa suhteessa Rekisterinpitäjiin. Rekisteröidyn oikeuksien turvaamiseksi, säännös velvoittaa henkilötietojen käsittelyn *läpinäkyvyyttä*. Läpinäkyvyys takaa luonnollisille henkilöille mahdollisuuden seurata, tarkistaa, muuttaa tai tilanteesta riippuen myös poistaa itseään koskevia henkilötietoja. Asetuksen johdantolauseen (39) mukaisesti, läpinäkyvyyden periaate on toteutettava siten, että Rekisteröityjä koskevat tiedot on ”*oltava helposti saatavilla ja ymmärrettävissä ja niissä on käytettävä selkeää ja yksinkertaista kieltä”*. Yritysten on myös Asetuksen johdantolauseen (39) mukaisesti ilmoitettava Rekisteröidyille mahdollisista suojatoimista ja riskeistä, soveltuvista säännöistä ja oikeuksista. Mainittu ilmoitusvelvollisuus voidaankin nähdä Asetuksen 5.2 artiklan osoitusvelvollisuutta tukevana toimenpiteenä.[112]

Asetuksen 5.1 artiklan (b) alakohdan mukaisen *käyttötarkoitussidonnaisuuden periaatteen* mukaan yritysten tulee kerätä tiedot vain tiettyä tarkoitusta varten. Niitä ei saa käyttää myöhemmin tavalla, joka ei ole yhteensopiva alkuperäisen käyttötarkoituksen kanssa. Käytännössä yritysten on määriteltävä nimenomainen tarkoitus ja ilmoitettava tästä ennen henkilötietojen keräämistä.[113] Poikkeuksen käyttötarkoitussidonnaisuuden periaatteelle tekee Asetuksen 89.1 artikla; yhtyeensopimattomana tietojen hyödyntämisenä ei pidetä myöhempää toimintaa, jossa tietoja kerätään yleisen edun mukaisiin arkistointitarkoituksiin tai tieteellisiin, historiallisiin ja tilastollisiin tutkimustarkoituksiin.[114]

[111] *Korpisaari* 2018, s. 90.
[112] *Korpisaari* 2018, s. 91.
[113] *Korpisaari* 2018, s. 92.
[114] *Aalto-Setälä - Viitaila* 2018, s. 14.

Henkilötietoja tulee kerätä Asetuksen 5.1 artiklan (c) alakohdan mukaisen *minimointiperiaatteen* mukaan vain niiltä osin, kun se käyttötarkoitus huomioiden on tarpeellista. Jotta henkilötiedot olisivat riittäviä, olennaisia ja rajoittuisivat vain käsittelyn kannalta välttämättömiin, on niiden alkuperäinen käsittelyn tarkoitus määriteltävä huolella. Lisäksi, Asetuksen johdantolause (39) painottaa henkilötietojen käsittelyn toissijaisuutta. Tietojen minimointi tarkoittaa siten myös sitä, ettei henkilötietoja tule ylipäänsä käsitellä, jos käsittelyn tarkoitus on toteutettavissa jotenkin muutoin – kevyempiä keinoja hyödyntäen. Tietojen minimointiperiaatteeseen kuuluu myös henkilötietojen säilytys ajan rajoittaminen tietojen todelliseen tarpeeseen. Periaate voidaankin nähdä osin päällekkäisenä säilytyksen rajoittamisen periaatteen kanssa. Henkilötietojen säilyttämisaika tulee minimoida; kun tietoja ei enää tarvita, ne tulee poistaa rekisteristä. Tämä voi tarkoittaa myös henkilötietojen osittaista poistoa. Minimointiperiaatteen oikeaoppinen totuttaminen takaa yrityksen rekisterin mahdollisimman suppea sisältöisenä.[115]

Asetuksen 5.1 artiklan (d) alakohdan mukaan henkilötietojen tulee olla myös *täsmällisiä* ja *ajantasaisia*. Rekisterinpitäjän on toteutettava kaikki kohtuulliset toimenpiteet, jotta epätarkat ja virheelliset tiedot tulee poistetuksi tai korjatuksi viipymättä. Kohtuullisina toimenpiteinä pidetään muun muassa säännöllisiä henkilötietojen tarkistuksia ja niiden päivittämistä sekä säännöllistä arviointia tallennettujen henkilötietojen tarpeellisuudesta.[116]

Asetuksen 5.1 artiklan (e) alakohdan mukaan Rekisterinpitäjän on asetettava ennen henkilötietojen keräämistä niiden säilyttämiselle selkeät määräajat, jonka myötä tietojen tarpeellisuus tulee aina uudelleen arvioitavaksi. Tarkoittaen samalla sitä, että Rekisteröity on tunnistettavissa vain tämän rajoitetun ajan. Vain tietyissä tapauksissa tietoja voidaan säilyttää pidempään, jos se esimerkiksi tieteellisen tutkimuksen kannalta on tarpeellista. Tällöin tulee kuitenkin huomioida muut Asetuksen vaatimat toimenpiteet[117].[118] Vaihtoehtoisesti yritys voi tietojen poistamisen sijaan *anonymisoida* Rekisteröidyn henkilötiedot. Anonymisoinnista on Asetuksen johdantolauseen (26) mukaan kyse silloin, kun tietojen tunnistettavuus on poistettu siten, ettei Rekisteröidyn tunnistaminen ole enää mahdollista. Henkilötietojen säilytyksen rajoittamisella pyritään varmistamaan, että Rekisteröityjen tietoja säilytetään ainoastaan sen aikaa kuin se on tietojen käsittelyn suhteen tarpeellista.

---

[115] *Korpisaari* 2018, s. 93.
[116] *Korpisaari* 2018, s. 93–94.
[117] Esimerkiksi Asetuksen artiklan 13 mukaan Rekisteröidylle on ilmoitettava henkilötietojen arvioidusta säilytysajasta jo ennen Rekisteröidyn mahdollisen suostumuksen antamista.
[118] *Korpisaari* 2018, s. 94.

Asetuksen 5.1 artiklan (f) alakohdan mukaan henkilötietojen käsittelyssä tulee huomioida asianmukainen turvallisuustaso, jolla tietojen *luottamuksellisuus* ja *eheys* taataan. Eheydellä viitataan henkilötietojen kokonaisuuteen ja muuttumattomuuteen; Rekisterinpitäjällä ei ole lupaa muokata tai poimia valitsemiaan Rekisteröidyltä saamiaan tietoja mielivaltaisesti, vaan se tarvitsee tähän Rekisteröidyn nimenomaisen suostumuksen.[119] Henkilötiedot eivät saa myöskään hävitä tai niihin ei saa kohdistua luvatonta käsittelyä. Tähän tulee varautua niin *teknisin kuin organisatorisin toimin*, joiden avulla ja turvin henkilötietojen käsittely on mahdollista toteuttaa Asetuksen vaatimusten ja periaatteiden mukaisesti. Käytännössä teknisiä toimia ovat esimerkiksi henkilötietojen suojaaminen salasanojen taakse tai automaatiotoimintojen hyödyntäminen, kuten järjestelmän automaattinen sulkeutuminen tietyn ajan jälkeen. Organisatorisilla toimilla pyritään taas luonnollisesti tarkastelemaan organisaation henkilöstön toimenkuvia.[120]

Luottamuksellisuuden periaatteella voi nähdä olevan liittymä Asetuksen *riskiperusteiseen lähestymistapaan*. Tällä tarkoitetaan sitä, että vaadittuihin Rekisteröidyn oikeuksiin ja vapauksiin tulee suhteuttaa asianmukaiset suojatoimet ja velvoitteet. Näin ollen yrityksen on arvioita perusteellisesti millaisia riskejä henkilötietojen käsittelyyn voi liittyä. Riskit voivat aiheuttaa Rekisteröidyille niin fyysisiä, aineellisia kuin aineettomiakin vahinkoja, esimerkiksi käsittelyn johtaessa identiteettivarkauteen, syrjintään tai sosiaaliseen vahinkoon. On huomioitavaa, että riskit voivat olla suurempia silloin kun henkilötietojen käsittely kohdistuu *erityisiin henkilötietoryhmiin*, joihin esimerkiksi lapset kuuluvat tai kun käsitellään suurta Rekisteröityjen joukkoa[121].[122] Henkilötietojen käsittely ja tarkastelu tuleekin olla mahdollista vain henkilöille, jotka tosiasiassa työtehtäviensä vuoksi tarvitsevat kyseisiä tietoja. Vaatimuksena tekniset ja organisatoriset toimet saattavat olla jopa helposti ymmärrettävissä, mutta niiden käytännön toteutus lienee ollut monelle taholle työläs prosessi toteuttaa. Kyseessä on moniulotteinen ja teknologisesti haastava vaatimus, jossa tulee huomioida niin työntekijöiden tietokoneet, matkapuhelimet, jaetut sisäiset sähköpostit kuin yrityksen ulkopuoliset mahdolliset tiedon hallintaa koskevat uhat.[123]

---

[119] *Korpisaari* 2018, s. 94–95.
[120] *Korpisaari* 2018, s. 94–95.
[121] Suuresta Rekisteröityjen joukosta oli kyse esimerkiksi British Airwaysin tapauksessa, jossa 500 000 asiakkaan tiedot joutuivat tietosuojahyökkäyksen kohteeksi. Ison-Britannian tietosuojaviranomainen (ICO) on esittänyt tapauksessa jopa 183,38 miljoonan punnan sakkoja. Ks. *ICO – British Airways* 2019.
[122] *Talus ym.* 2017, s. 16; *Sulin – Tainio* 2017, s. 5.
[123] *Korpisaari* 2018, s. 94–95.

Asetuksen 25 artikla määrittelee *sisäänrakennetun* ja *oletusarvoisen tietosuojan periaatteet*. Kyseisten periaatteiden tarkoituksena on varmistaa, että Rekisterinpitäjät huomioisivat tietosuojan tarpeen jo tietojärjestelmien suunnittelussa. Sisäänrakennettu tietosuoja (*privacy by design*) velvoittaa yrityksiä toteuttamaan kaikki tarvittavat tekniset ja organisatoriset toimet, joilla varmistetaan henkilötietojen Asetuksen mukainen käsittely.[124] Tämä tarkoittaa edellä listattujen tietosuojaperiaatteiden täytäntöönpanoa ja noudattamista kaikissa henkilötietojen käsittelyn vaiheissa ja toiminnoissa, kattaen henkilötietojen käsittelyn koko elinkaaren.[125] Konkreettisella tasolla teknisinä ja organisatorisina toimenpiteinä nähdään muun muassa henkilöstön kouluttaminen, salassapitosopimusten hyödyntäminen, sekä tietojärjestelmien muokkaaminen niin, että tarpeettomat tiedot ovat tosiasiassa poistettavissa.

Vastaavasti oletusarvoinen tietosuoja (*privacy by default*) velvoittaa yrityksiä käsittelemään henkilötietoja vain siltä osin, kuin se on käsittelyn luonne huomioiden tarpeellista ja varmistamaan, että henkilötietoja käsittelee oletusarvoisesti vain rajoitetut henkilöt. Tämä koskee niin henkilötietojen määrää, käsittelyn laajuutta, saatavuutta kuin säilytysaikaa[126]. Myös oletusarvoinen tietosuoja turvataan yrityksen toteuttamilla teknisillä ja organisatorisilla toimenpiteillä. Toimenpiteillä varmistetaan, että henkilötietojen käsittelyn laajuus ja henkilötietojen säilytysaika pysyvät rajattuina. Tietojärjestelmän yksityisyyttä suojaavat oletusasetukset ovat erinomainen esimerkki onnistuneesta oletusarvoisen tietosuojan toteuttamisesta käytännössä. Yksityisyyttä suojaavat oletusasetukset turvaavat myös Asetuksen käsittelyperusteet; jos Rekisteröity on halukas jakamaan itsestään enemmän tietoja, muokkaamalla oletusasetuksia muutos on tehty sekä nimenomaisesti että tietoisesti tiettyä tarkoitusta varten.[127] Digitaalisten alustojen monimutkaisuus vaatii kuitenkin usein teknistä osaamista ja ymmärrystä, jolloin yksityisyysasetusten muokkaaminen itselleen turvallisemmaksi ei ole kaikille itsestään selvä taito[128].

[124] Ks. Asetuksen johdantolause 78.
[125] *Talus ym.* 2017, s. 13–14.
[126] *Talus ym.* 2017, s. 13–14.
[127] *Pitkänen* 2018, s. 277–281.
[128] Komission erityiseurobarometrin mukaan suomalaiset päivittävät yksityisyysasetuksiaan verkkoyhteisöpalveluissa muita eurooppalaisia tiheämmin. Tulosten mukaan Suomessa yksityisyysasetuksia oli yrittänyt päivittää 72 % tutkimukseen osallistuneista, kun keskitaso jäsenmaissa oli 56 %. Lisäksi 62 % suomalaisista vastaajista oli huolestuneita siitä, ettei heillä ole täyttä valtaa verkossa annettuihin tietoihin. *Euroopan komission erityisbarometri* 2019b, s. 3–4.

3.2.2 Henkilötietojen käsittelyperusteet

Yleisten periaatteiden lisäksi, Asetuksen artiklat 6-8 määrittelevät millä perusteilla henkilötietoja saa käsitellä. Yrityksen henkilötietojen käsittely on lainmukaista vain silloin, kun lain sallimat käsittelyperusteet täyttyvät. Käsittely voi perustua yhteen tai useampaan *käsittelyperusteeseen.* Kulloinkin sovellettava käsittelyperuste vaikuttaa merkittävästi edelleen Rekisteröidyllä oleviin oikeuksiin[129].

3.2.2.1 Rekisteröidyn suostumus

Rekisteröity voi antaa 6.1 artiklan (a) alakohdan mukaan *suostumuksensa* henkilötietojensa käsittelyyn yhtä tai useampaa tarkoitusta varten. Rekisteröidyn suostumus henkilötietojen käsittelylle tulee olla 4.11 artiklan mukaan vapaaehtoinen, yksilöity, tietoinen ja yksiselitteinen tahdonilmaisu. Käsitellessä henkilötietoja suostumuksen nojalla, 7.1 artiklan mukaisesti yrityksen on voitava jälkikäteen osoittaa, että Rekisteröidyn antama suostumus on annettu.

Käsittelyperusteen täyttävä suostumus voidaan antaa käytännössä esimerkiksi kirjallisella tai suullisella lausumalla tai muulla riittävän selkeällä toimella. Riittävän selkänä toimena voidaan pitää esimerkiksi internetsivuston ruudun rastittamista, kunhan suostumus kattaa kaikki tavoitellut käsittelytoimet. Huomattavaa on, ettei suostumus ole Rekisterinpitäjän tulkittavissa; muun muassa vaikeneminen, valmiiksi rastitetut internetsivuston ruudut tai jonkin toimen tekemättä jättäminen eivät täytä Asetuksen 4.11 artiklassa asetettuja suostumuksen kriteereitä.[130] Lisäksi, 7.2 artiklan mukaan, kirjallisessa ilmoituksessa esitetty suostumusta koskeva pyyntö on oltava eriteltävissä muista kirjallisen ilmoituksen asioista selkeästi ja yksinkertaisesti ilmaistuna.[131]

EU:n tietosuojaviranomaisista koostuva *WP29-työryhmän* antamien ohjeistusten mukaan, tietoisen suostumuksen antaminen edellyttää Rekisteröidyn riittävää informointia. Rekisteröidyllä tulee olla (i) tieto kuka Rekisterinpitäjänä toimii, (ii) tieto mihin tarkoituksiin henkilötietoja käsitellään, (iii) tieto minkälaisia tietoja Rekisterinpitäjä kerää ja käyttää, (iv) oikeus peruuttaa antamaansa suostumus, (v) tieto jos henkilötietoja hyödynnetään automaattiseen

[129] Ks. tarkemmin käsittelyperusteen vaikutuksista Rekisteröidyn oikeuksiin *Tietosuojavaltuutetun toimisto* 2019a, kohta Mitä oikeuksia rekisteröidyllä on eri tilanteissa.
[130] Ks. myös Asetuksen johdantolauseet 32, sekä 42–43.
[131] Ks. *Article 29 Working Party* 2017, s. 14; Huomattavaa, että Asetuksen artikla 8 huomioi lasten henkilötietojen käsittelyn ja suostumuksen korostuneesti. Asetus suojaa lasten asemaa edellyttäen lapsen vanhemman tai huoltajan suostumusta. Tietosuojalain 5§:n mukaan alle 13 vuotiaan henkilötietojen käsittely on lainmukaista vain siltä osin kuin lapsen huoltaja on antanut tähän suostumuksen.

päätöksentekoon, sekä (vi) tieto käsittelyyn liittyvistä riskeistä ja Rekisterinpitäjän hyödyntämistä Asetuksen artiklan 46 mukaisista suojatoimista.[132] Jos yritys laiminlyö edellä mainitut *informointivelvollisuutensa*, voidaan sen katsoa olevan 6 artiklan vastainen rikkomus käsittelyn lainmukaisuuden noudattamisesta. Rekisterinpitäjä ei voi myöskään niin sanotusti oikaista asetettujen vaatimusten osalta, esimerkiksi pyytämällä suostumusta, jonka nojalla Rekisteröity antaa tietonsa kaikkiin Rekisterinpitäjän tarvitsemiin tarpeisiin. Vastaavassa muodossa annettu suostumus on mitätön; Asetuksen käsittelyperiaatteita ei voi syrjäyttää Rekisteröidyn suostumuksella.[133]

Jotta suostumus on ymmärrettävissä vapaaehtoisesti annetuksi, Rekisteröidyn tulee voida myös peruuttaa antamansa suostumus. Artiklan 7.3 mukaisesti, peruutus on oltava helposti annettavissa, milloin tahansa. Peruuttamista koskevan tiedon saatuaan, yrityksen tulee lopettaa henkilötietojen käsittely – siinä laajuudessa kuin Rekisteröity on peruutuksensa antanut. Yritys voi edelleen hyödyntää saamiaan tietoja myös peruuttamisen jälkeen – kunhan tiedot ovat ajalta ennen suostumuksen peruuttamista ja sille on 6 artiklan mukainen laillinen peruste, tietosuojalain sallima peruste, tai suostumuksella saatu lupa jatkaa jo kerättyjen tietojen käsittelyä. Muussa tilanteessa yrityksen tulee poistaa keräämänsä tiedot, sillä myös pelkkä henkilötietojen säilyttäminen yrityksen tietojärjestelmissä täyttää henkilötietojen käsittelyn määritelmän.[134]

3.2.2.2 Sopimukseen perustuva käsittely

Käsittelyperusteeksi riittää, jos Rekisteröity on sopimuksen osapuolena tai Rekisteröity on pyytänyt Rekisterinpitäjältä sopimusta edeltäviä toimia. Mainituissa tilanteissa Rekisteröidyltä ei tarvita erillistä suostumusta 6.1 artiklan (b) alakohdan mukaisesti. Rekisteröityjen ja Rekisterinpitäjien välisissä sopimuksissa voi olla kyse esimerkiksi kuluttajan verkko-ostoksista. Jotta yritys saa toimitettua kuluttajan ostokset oikeaan osoitteeseen, tarvitsee yrityksen Rekisterinpitäjänä käsitellä kuluttajan osoitetietoja. Myös sopimusta edeltävien toimien käsittelyperusteet, on mahdollista perustaa osapuolten väliseen sopimukseen; yksityishenkilön hakiessa lainaa, esimerkiksi luotonantajana toimiva pankki voi päätöstään harkitessaan käsitellä lainanhakijan luottokelpoisuutta koskevia taloudellisia tietoja.[135]

---

[132] *Article 29 Working Party* 2017, s. 12–13.
[133] *Korpisaari* 2018, s. 136.
[134] *Korpisaari* 2018, s. 137.
[135] Ks. *Tietosuojavaltuutetun toimisto* 2019b, kohta Sopimus.

3.2.2.3 Muut henkilötietojen käsittelyperusteet

Asetuksen 6.1 artiklan (c) alakohdan mukaan käsittelyn lainmukaisuus voi perustua myös Rekisterinpitäjän *lakisääteiseen velvoitteeseen*. Rekisterinpitäjää pakottava lakisääteinen velvoite tulee kyseeseen vain tilanteissa, joissa velvoite perustuu EU tason sääntelyyn tai kansalliseen lakiin. Näissä tilanteissa velvoite voi edellyttää Rekisterinpitäjää käsittelemään henkilötietoja ilman Rekisteröidyn erillistä suostumusta. Lakisääteisten velvoitteiden kirjo on laaja, näitä ovat muun muassa työnantajan palkkailmoitukset veroviranomaisille sekä rahoituslaitosten tekemät ilmoitukset viranomaisille epäilyttävästä liiketoiminnasta.[136]

Henkilötietojen lainmukainen käsittely on mahdollista perustaa myös *elintärkeiden etujen suojaamiseen* Asetuksen 6.1 artiklan (d) alakohdan mukaisesti. Elintärkeiden etujen suojaamisesta on kyse kun henkilötietojen käsittely on tarpeen Rekisteröidyn tai toisen luonnollisen henkilön elintärkeiden etujen suojaamiseksi. Käsiteltäessä henkilötietoja elintärkeiden etujen nimissä Rekisteröidyltä ei tarvita erillistä suostumusta. Käytännössä elintärkeiden etujen suojaaminen tulee sovellettavaksi elämää uhkaavissa tilanteissa, kuten luonnonkatastrofeissa tai epidemioissa.[137]

Asetuksen 6.1 artiklan (e) alakohdan mukaan henkilötietojen käsittely on sallittua ilman Rekisteröidyn erillistä suostumusta myös silloin, kun käsittely tehdään *yleistä etua koskevan tehtävän* toteuttamiseksi tai käytettäessä Rekisterinpitäjälle kuuluvaa *julkista valtaa*. Käsittelyperuste soveltuu vain tilanteissa, joissa asiasta säädetään tarkemmin lailla tai säännöksillä. Muun muassa tieteellisen tutkimuksen nimissä tapahtuva henkilötietojen käsittely katsotaan kuuluvan yleisen edun alaisuuteen.[138]

Viimeisenä, henkilötietojen käsittely on 6.1 artiklan (f) alakohdan mukaan sallittua, kun Rekisterinpitäjällä on *oikeutettu etu* käsitellä muun muassa asiakkaidensa tai alaistensa henkilötietoja. Oikeutettu etu vaatii kuitenkin aina niin sanottua tasapainotestiä jossa punnitaan esimerkiksi Rekisterinpitäjänä toimivan yrityksen intressejä suhteessa sen alaisten intresseihin ja perusoikeuksiin.[139]

---

[136] Ks. *Tietosuojavaltuutetun toimisto* 2019b, kohta Lakisääteinen velvoite.
[137] Ks. *Tietosuojavaltuutetun toimisto* 2019b, kohta Elintärkeiden etujen suojaaminen.
[138] Ks. *Tietosuojavaltuutetun toimisto* 2019b, kohta Yleinen etu ja julkinen valta.
[139] Ks. *Tietosuojavaltuutetun toimisto* 2019b, kohta Rekisterinpitäjän oikeutettu etu.

3.2.3 Rekisterinpitäjän merkittävimmät velvollisuudet

Yleisten periaatteiden ja käsittelyperusteiden lisäksi, Asetus asettaa yrityksille myös joukon tarkempia velvoitteita henkilötietojen käsittelyä varten.

3.2.3.1 Osoitusvelvollisuus

Osoitusvelvollisuus tarkoittaa sitä, että yrityksen on pystyttävä osoittamaan noudattavansa henkilötietojen käsittelyä koskevia periaatteita ja säännöksiä, tarkoittaen, että käytännön toteutus tulee dokumentoida.[140] Ei toisin sanoen riitä, että soveltuvaa lainsäädäntöä vain noudatetaan, vaan sen on oltava näytettävissä toteen. Osoitusvelvollisuudesta säätää Asetuksen 5.2 artikla, jonka mukaan Rekisterinpitäjän edellytetään suunnittelevan ja dokumentoivan henkilötietojen käsittelyn elinkaari niin, että se on jälkeenpäin tarkistettavissa ja todistettavissa. Rekisterinpitäjiä helpottaakseen, tietosuojavaltuutetun toimisto on koonnut verkkosivuilleen osoitusvelvollisuuden toteuttamista varten listan tarvittavista toimenpiteistä ja dokumenteista. Listasta on nähtävissä, että vaadittavia velvoitteita on huomattava määrä[141]. Osoitusvelvollisuus ei kuitenkaan sovellu kaikille yrityksille samanlaisena, vaan sen sisältö on riippuvainen Rekisterinpitäjänä toimivan yrityksen koosta, henkilötietojen määrästä sekä henkilötietojen sisällöstä.[142] Yritysten on muun muassa varmistettava riittävä dokumentaatio koskien henkilötietojen tietoturvaloukkauksia, vaikutusarviointeja, riskiarvioita sekä siirtoja kolmansiin maihin. Käytännössä velvoite tarkoittaa monelle yritykselle enemmän sisäistä koulutusta, dokumentoinnin lisäämistä, kattavampia ohjeistuksia, sekä muutoksia organisaatioon ja tietoteknisiin järjestelmiin.

Samalla kun kyseinen velvoite on kannustanut yrityksiä päivittämään ja tehostamaan järjestelmiään taatakseen vaaditun henkilötietojen suojan, se on luultavasti lisännyt myös yritysten hallinnollista taakkaa. Velvoitteen noudattamisen tärkeyttä korostaa myös laiminlyönnistä mahdollisesti langetettavat huomattavat sanktiot[143]. Osoitusvelvollisuuden myötä, esimerkiksi tietosuojaloukkauksen tapahtuessa, yritys pystyy osoittamaan asianmukaisella dokumentaati-

---

[140] *Talus ym.* 2017, s. 14; Osoitusvelvollisuuden toteutuksessa on huomattava, että henkilötietojen käsittelyä koskevan sääntelyn noudattaminen sisältää Asetuksen lisäksi runsaasti myös muita säännöksiä. Kansallisesti tietosuojasääntelyä on mm. tietosuojalaissa ja lukuisissa erityislaeissa.

[141] *Tietosuojavaltuutetun toimisto* 2019c, kohta Toimenpiteet ja dokumentit osoitusvelvollisuuden toteuttamiseksi.

[142] *Tietosuojavaltuutetun toimisto* 2019c, kohta Osoita noudattavasi tietosuojasäännöksiä; Ks. myös *Talus ym.* 2017, s. 14.

[143] Hallinnollisista seuraamuksista tarkemmin jäljempänä kappaleessa 3.3.2. Seuraamukset Asetuksen rikkomisesta.

olla, että tietosuojariskeihin on varauduttu ja tarvittavia toimenpiteitä niiden estämiseksi on tehty. Mikäli tarvittavaa dokumentaatiota ei esitetä, voi se aiheuttaa sekä hallinnollisia seuraamuksia että mainehaittoja yritykselle. Toisaalta osoitusvelvollisuutta noudattamalla yritys pystyy osoittamaan myös kunnioituksensa käsittelemiään henkilötietoja kohtaan.

3.2.3.2 Henkilötietojen käsittelyyn liittyvien riskien arviointi

Yrityksen ovat vastuussa sekä omista että niiden lukuun suoritetusta henkilötietojen käsittelystä. Asetus velvoittaa Rekisterinpitäjiä säännöllisesti arvioimaan henkilötietojen käsittelyn aiheuttamia riskejä kohdistuen Rekisteröityjen oikeuksiin ja vapauksiin. Artiklan 24 mukaan riskien todennäköisyyden ja vakavuuden arviointi tulee kuitenkin suhteuttaa käsittelyn luonteeseen, laajuuteen, asiayhteyteen ja tarkoitukseen. Henkilötietojen käsittelystä aiheutuvat riskit voivat olla moninaiset, ollen kaikkea aineellisen ja aineettoman vahingon välillä. Korkeariskisestä käsittelystä on kyse esimerkiksi silloin, kun yritys luo yksityisistä henkilöistä henkilöprofiileja tai käsittelee tietoja näiden työsuorituksista ja terveydentilasta. Vahingon seurauksena voi olla Asetuksen johdantolauseiden (75 ja 76) mukaan yritykseen tai yksittäiseen henkilöön kohdistuva syrjintä, identiteettivarkaus, petos, taloudelliset menetykset sekä mainevahingot. Jotta vahingoilta vältyttäisiin, henkilötietoja käsittelevän yrityksen tulee kartoittaa toiminnastaan aiheutuvat todennäköiset riskit ja niiden vakavuudet, ja toteuttaa tämän jälkeen tarvittavat asianmukaiset toimet henkilötietojen turvaamiseksi. Hallinnollisina (organisatorisina) toimenpiteinä yritys voi tehdä muun muassa toimintalinjauksia ja organisaatiojärjestelyjä, sekä antaa ohjeistusta ja koulutusta. Riskien arvioinnilla on kiinteä liittymä yrityksen mahdolliseen velvollisuuteen toteuttaa Asetuksen mukainen *vaikutustenarviointi*.

3.2.3.3 Tietosuojaa koskeva vaikutustenarviointi ja ennakkokuuleminen

Edellä mainitusta riskien arvioinnin tuloksista riippuen, yritys voi olla velvollinen tekemään ennen henkilötietojen käsittelyä niin sanotun vaikutustenarvioinnin (*Data Protection Impact Assessment* – jäljempänä ”*DPIA*”). Jos yrityksen toteuttama henkilötietojen käsittely aiheuttaa Rekisteröityjen oikeuksille todennäköisen ja korkean riskin, yrityksen on selvitettävä miten riski olisi pienennettävissä. Artiklan 35.3 mukaan DPIA vaaditaan erityisesti tilanteissa, joissa tietojen käsittelyssä: (i) käytetään uutta teknologiaa; (ii) on kyse luonnollisten henkilöiden automatisoidusta henkilökohtaisten ominaisuuksien arvioinnista, jolla on merkittäviä vaikutuksia arvioitaville yksilöille; (iii) tiedot koskevat erityisiä henkilötietoryhmiä – kuten terveystietoja tai poliittisia mielipiteitä, laajaa rikostuomioiden tai rikkomusten tietokantaa; tai (iv)

valvotaan järjestelmällisesti ja laajamittaisesti yleisölle avointa aluetta.[144] Artiklan 36 mukaan yrityksen tulee kuulla tietosuojaviranomaista tilanteissa, joissa sen tekemä DPIA osoittaa käsittelyn korkea riskiseksi toiminnaksi, eikä yrityksellä ole käytettävissä toimenpiteitä riskien pienentämiseksi. Ennakkokuulemisen avulla yritys voi saada tietosuojaviranomaiselta ohjeita, miten käsittelyn aiheuttamat riskit olisivat pienennettävissä[145]. Rekisterinpitäjänä toimivan yrityksen tulee arvioida henkilötietojen käsittelyä myös jatkossa. Jos esimerkiksi käsittelyyn liittyvät riskit muuttuvat myöhemmin, yritys voi olla velvollinen tekemään uuden DPIA:n.

3.2.3.4 Seloste käsittelytoimista

Yritysten on ylläpidettävä artiklan 30 mukaista kirjallista *selostetta* heidän vastuullaan olevista *käsittelytoimista.*[146] Seloste on ensisijaisesti tarkoitettu yrityksen sisäiseksi asiakirjaksi, mutta sitä voi hyödyntää myös osana osoitusvelvollisuuden toteuttamista. Seloste onkin pyydettäessä toimitettava tietosuojaviranomaisille. Selosteen on Asetuksen mukaan sisällettävä seuraavat tiedot: Rekisterinpitäjän ja mahdollisen yhteisrekisterinpitäjän ja Rekisterinpitäjän edustajan ja tietosuojavastaavan nimi ja yhteystiedot; käsittelyn tarkoitukset; kuvaus Rekisteröityjen ryhmistä ja henkilötietoryhmistä; henkilötietojen vastaanottajien ryhmät, joille henkilötietoja on luovutettu tai luovutetaan; tiedot henkilötietojen siirtämisestä EU-alueen ulkopuolelle tai kansainvälisille järjestöille; tietojen säilytysajat; kuvaus teknisistä ja organisatorisista turvatoimista.

3.2.3.5 Käsittelyn turvallisuus

Jotta yrityksen henkilötietojen käsittely on Asetuksen mukaan turvallista, tulee turvallisuustason ylläpidossa ja toteutuksessa toteuttaa asianmukaiset tekniset ja organisatoriset toimenpiteet. Toimenpiteet tulee suhteuttaa käsittelyn luonne, laajuus, tarkoitus ja riskit huomioiden. Käytännössä tietoturvan toteuttamiseksi riittää pienen riskin tilanteessa kevyetkin toimet, tarkoituksena on toisin sanoen toteuttaa turvaamistoimet oikeasuhteisina riskeihin nähden[147]. Riittävän turvallisuustason varmistamiseksi teknisinä ja organisatorisina toimenpiteinä maini-

[144] Ks. myös tietosuojavaltuutetun luettelo DPIA:n vaativista käsittelytoimista *Tietosuojavaltuutetun toimisto* 2018b, kohta Tietosuojavaltuutetun toimisto katsoo, että seuraavien käsittelytoimien yhteydessä tulee tehdä vaikutusarviointi; Ks. myös aiheesta tarkemmin *Tietosuojatyöryhmä* 2017.
[145] *Tietosuojavaltuutetun toimisto* 2019d, kohta Ennakkokuuleminen.
[146] Poikkeuksena artiklan 30 vaatimuksista mainittakoon yritykset tai järjestöt, jotka työllistävät alle 250 henkilöä. Artiklan 30.5 mukaan poikkeus ei kuitenkaan sovellu jos mainitun tahon käsittely koskee erityisiä henkilöryhmiä, rikostuomioita tai rikkomuksia, tai käsittely aiheuttaa todennäköisesti riskin Rekisteröityjen oikeuksille ja vapauksille. Lisäksi 30.2 artiklan mukaan selosteen vaadittu sisältö on myös laajuutena suppeampi jos käsittelijänä toimii Henkilötietojen käsittelijä tai sen edustaja.
[147] *Warma-Lehtinen* 2018, s. 308.

taan artiklassa 32 muun muassa: henkilötietojen *pseudonymisointi* ja salaus; toimet joiden turvin taataan käsittelyjärjestelmien ja palveluiden jatkuva luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus; sekä kyky palauttaa nopeasti tietojen saatavuus vian sattuessa. Lisäksi yrityksen on huolehdittava siitä, että jokainen tietojen parissa toimiva taho käsittelee henkilötietoja sen antamien ohjeiden mukaisesti.

3.2.3.6 Henkilötietojen tietoturvaloukkauksista ilmoittaminen

Vaikka yritys toimisi Asetuksen säännösten mukaisesti, on mahdollista, että henkilötiedot päätyvät vääriin käsiin. Asetuksen 4.12 artikla määrittelee *tietoturvaloukkauksen* tapahtumana, jonka seurauksena henkilötietoja vahingossa tai lainvastaisesti tuhoutuu, häviää, muuttuu, tai henkilötietoja luvattomasti luovutetaan tai ne päätyvät ulkopuolisen tahon käsiin. Tieturvaloukkauksissa ei ole aina kyse massiivisesta kyberhyökkäyksestä vaan myös hävinnyt USB-tikku, varastettu tietokone tai tiliotteen postitus väärälle henkilölle riittävät täyttämään tietoturvaloukkauksen määritelmän. Jotta tietovuotojen ja niiden aiheuttamat vahingot saataisiin minimoitua, on yritysten ja sen työntekijöiden ymmärrettävä toiminnastaan aiheutuvat riskit ja niiden mahdolliset seuraukset. Muun muassa identiteettivarkaus, maineen vahingoittuminen tai salassa pidettävien henkilötietojen leviäminen voivat aiheuttaa mittavia vahinkoja kärsineelle osapuolelle.[148] Tällöin asian selvittäminen ja tiedottaminen nopealla aikataululla on kaikkien osapuolten etu.[149]

Jos mainittu tietoturvaloukkaus syystä tai toisesta tapahtuu, siitä tulee ilmoittaa edelleen tietosuojaviranomaiselle ja Rekisteröidyille artiklan 33 ja 34 mukaisesti niissä vaadituin minimisisällöin. Toisin sanoen, yrityksen on ilmoitettava tietoturvaloukkauksesta tietosuojavaltuutetun toimistoon 72 tunnin kuluessa tietoturvaloukkauksen tiedoksisaannista. Ilmoituksen voi jättää tekemättä vain jos tapahtuma ei todennäköisesti aiheuta Rekisteröityjen oikeuksille ja vapauksille riskiä. Vaikka *ilmoitusvelvollisuus* ei täyttyisi, tulee yrityksen 30.5 artiklan mukaisesti dokumentoida kaikki tietoturvaloukkaukset ja tehdä järjestelmiin tarvittavat korjaukset, jotta tulevilta tapahtumilta vältyttäisiin. Dokumentointi mahdollistaa myös valvontaviranomaisille jälkikäteisen tarkistamisen, että Asetusta on noudatettu. Jos tapahtuma aiheuttaa *todennäköisesti korkean riskin* Rekisteröityjen oikeuksille ja vapauksille, yrityksen on artiklan 34.1 mukaisesti ilmoitettava loukkauksesta myös Rekisteröidyille. Rekisteröity saa siten tilai-

[148] *Tietosuojavaltuutetun toimisto* 2019e, kohta Mikä on henkilötietojen tietoturvaloukkaus?
[149] Ks. *Warma-Lehtinen* 2018, s. 315.

suuden suojautua, esimerkiksi sulkemalla pankkikorttinsa. Mainitussa korkean riskin tilanteessa, Rekisteröidyille ei kuitenkaan tarvitse ilmoittaa artiklan 34.3 määrittämissä tilanteissa; esimerkiksi jos yritys on jo kerinnyt tekemään tarvittavat suojatoimet niin, etteivät loukkauksen kohteena olevat henkilötiedot ole enää saatavilla tai hyödynnettävissä. Ilmoitusvelvollisuutta ei myöskään ole, jos ilmoittamisesta aiheutuisi yritykselle kohtuutonta vaivaa.[150] Toisin sanoen tietoturvaloukkauksiin reagointi vaatii yrityksiltä selkeitä prosesseja ja jatkuvaa riskien arviointia. Yhtenä keinona tukemaan Rekisterinpitäjän tietoturvaloukkauksen arviointia mahdollisuus hyödyntää edellä kuvattua yrityksen tekemään artiklan 35 mukaista DPIA:ta.[151]

3.2.3.7 Tietosuojavastaavan nimittäminen

Asetuksen artiklat 37–39 säätävät seikkaperäisesti *tietosuojavastaavan* asemasta ja tehtävistä. Tiivistetysti voidaan sanoa, että tietosuojavastaava seuraa yrityksen tietosuojasääntelyn noudattamista, neuvoo sen toteuttamisessa ja tiedottaa havaitsemistaan puutteista, sekä toimii yhteyshenkilönä ja yhteistyössä tietosuojavaltuutetun toimiston kanssa. Tietosuojavastaavan nimittäminen ei kuitenkaan koske kaikkia yrityksiä. Nimenomainen velvollisuus nimetä tietosuojavastaava koskee vain yrityksiä, joissa Rekisteröityjen henkilötietojen käsittely on säännöllistä ja systemaattista. Lisäksi, velvoite koskee yrityksiä, joissa käsitellään laajamittaisesti tietoja koskien erityisiä henkilötietoja, rikostuomioita tai rikkomuksia, esimerkiksi terveyspalveluidentuottajia tai lakitoimistoja. Luonnollisesti tietosuojavastaavan voi näin halutessaan nimittää myös muut, kyseisestä Asetuksen velvoitteesta vapaat yritykset. Tietosuojavastaava voi olla Asetuksen johdantolauseen (97) mukaisesti myös yrityksen henkilöstön jäsen tai kyseinen toimi on hankittavissa myös ulkoistamalla tehtävä sopimusperusteisesti.

3.2.3.8 Tietojenkäsittelysopimuksen laatiminen

Yritys voi halutessaan ulkoistaa myös henkilötietojen käsittelynsä. Asetus määrittelee tälle kuitenkin tietyt reunaehdot. Ulkoistaessaan henkilötietojen käsittelyn, Rekisterinpitäjän tulee artiklan 28 mukaisesti valita Henkilötietojen käsittelijöiksi vain sellaisia tahoja, jotka pystyvät täyttämään Asetuksen edellyttämät vaatimukset ja suojaamaan Rekisteröityjen oikeudet. Sen lisäksi, että ulkoistavan yrityksen tulee varmistua ja kyetä seuraamaan Henkilötietojen käsittelijän toimintavalmiuksia noudattaa ja toteuttaa Asetuksen vaatimuksia, sen tulee myös laatia kirjallinen Tietojenkäsittelysopimus ulkoistettavasta henkilötietojen käsittelystä. Käytännössä

[150] Ks. esimerkkejä henkilötietojen tietoturvaloukkauksista ja siitä, kenelle niistä ilmoitetaan *Tietosuojatyöryhmä* 2019, s. 1–4.
[151] *Warma-Lehtinen* 2018, s. 318.

kaiken kokoiset yritykset riippumatta toimintasektoristaan, joutuvat päivittämään ja jatkossa huomioimaan kyseisen vaatimuksen kaikissa sopimuksissaan, jotka koskevat henkilötietojen käsittelyä. Tämä tarkoittaa huomattavaa sopimusten joukkoa moninaisten palveluiden osalta. Kyseisen Tietojenkäsittelysopimuksen sisältövaatimuksista ja sen vaikutuksista Rekisterinpitäjään ja Henkilötietojen käsittelijään esitellään tarkemmin tutkielman seuraavassa luvussa 4.

3.2.4 Rekisteröidyn oikeuksien toteuttaminen

Rekisteröityjen oikeuksia ei ole tämän tutkielman kannalta tarkoituksenmukaista lähteä avaamaan seikkaperäisesti, mutta niiden olemassa olon tiedostaminen ja tunnistaminen Rekisterinpitäjän velvollisuutena on tärkeää. Rekisteröityjen oikeuksien toteuttamisessa on kuitenkin huomattava, että Rekisteröityjen oikeudet ovat sidoksissa yrityksellä oleviin henkilötietojen käsittelyperusteisiin[152]. Toisinsanoen se, mistä tiedot on kerätty ja millä perusteella henkilötietoja käsitellään, vaikuttaa Rekisteröidyllä oleviin oikeuksiin. Esimerkiksi Rekisteröidyn oikeus saada poistettua Rekisterinpitäjän tiedostoista itseään koskevia tietoja, mikä tunnetaan myös nimellä *oikeus tulla unohdetuksi*, ei sovellu tilanteisiin, joissa on kyse lakisääteisen velvoitteen noudattamisesta. Rekisteröity ei voi muun muassa vaatia tulla poistetuksi väestötietojärjestelmästä.[153] Lisäksi, vaikka Rekisteröidyt ovat hyvin tietoisia heillä olevista oikeuksistaan[154], olisi yritysten hyvä pystyä tarvittaessa ohjeistamaan Rekisteröityjä heitä koskevien henkilötietojen käsittelyssä.

Rekisteröityjen oikeuksista säädetään Asetuksen 3. luvussa, kyseiset oikeudet voidaan tiivistää seuraavasti: (i) Rekisterinpitäjän on huolehdittava, että Rekisteröidyille annetut tiedot heidän henkilötietojensa käsittelystä ovat helposti ymmärrettävissä ja saatavilla – viestinnän ja informoinnin tulee olla läpinäkyvää (artiklat 12–14), (ii) Rekisterinpitäjän on vahvistettava Rekisteröidylle käsitteleekö se häntä koskevia henkilötietoja ja mahdollistaa Rekisteröidyn pääsy häntä koskeviin henkilötietoihin (artikla 15), (iii) Rekisterinpitäjän on mahdollistettava Rekisteröidyn oikeus oikaista häntä koskevat virheelliset tiedot, sekä tietyin rajoituksin pois-

[152] Ks. edellä kappale 3.2.2. Rekisterinpitäjän käsittelyperusteet.
[153] Vrt. *KHO 2018:112* päätökseen, jossa tietosuojavaltuutettu oli määrännyt Rekisterinpitäjänä toiminutta Google Inc:iä poistamaan Google Search – hakutuloksia. Päätöksessä hakutuloksilla löytyneet henkilötiedot (hakijan nimi, oireyhtymä ja murhatuomio) määrättiin poistettaviksi niiden arkaluonteisuuden vuoksi. Kyseessä intressipunninta hakijan oikeudesta tulla unohdetuksi ja suuren yleisön oikeuksien välillä.
[154] Ks. *Euroopan komission erityisbarometri* 2019c, kohta Erityseurobarometrin tulokset.

taa Rekisteröidyn pyynnöstä häntä koskevat tiedot (artiklat 16–17)[155], (iv) Rekisterinpitäjän on pyydettäessä rajoitettava Rekisteröidyn tietojen aktiivista käsittelyä (artikla 18), (v) Rekisterinpitäjän on mahdollistettava Rekisteröidyn tietojen siirtäminen järjestelmästä toiseen luovuttamalla tiedot jäsennellyssä, yleisesti käytetyssä ja koneellisesti luettavassa muodossa (artikla 20), (vi) Rekisterinpitäjän on huomioitava Rekisteröidyn henkilötietojen käsittelyn vastustamisoikeus toiminnassaan, esimerkiksi suoramarkkinointia toteuttaessaan (artikla 21), lisäksi (vii) Rekisterinpitäjän on ilmoitettava henkilötietojen oikaisua, poistoa tai käsittelyn rajoittamista koskevat tiedot myös edelleen niille joille se on luovuttanut kyseessä olevia tietoja (artikla 19).

Rekisteröityjen oikeuksia toteutettaessa yritysten on kaikessa toiminnassaan muistettava myös muut niitä koskevat velvoitteet ja niistä tässä yhteydessä erityisesti mainittakoon osoitusvelvollisuus[156]. Käytännössä yritysten on dokumentoitava edellä esitettyihin velvoitteisiin liittyvät tapahtumat, koskien myös tilanteita, jolloin henkilötietojen käsittelyä jatketaan Rekisteröidyn vastustamisesta huolimatta. Käsittelyn jatkamista koskevien perusteluiden ja arvioinnin läpinäkyvä kirjaaminen ovat osa Asetuksen velvoitteiden noudattamista ja oikein toteutettuna ne tukevat yrityksen tietosuojasääntelyn noudattamisen todentamista myös valvontaviranomaisia kohtaan.[157]

3.3 Rekisterinpitäjän toiminnan valvonta ja seuraamukset

3.3.1 Asetuksen valvonta

Yritysten henkilötietojen käsittelyn lainmukaisuuden valvonta rakentuu kansallisesta riippumattomasta tietosuojaviranomaisesta - Suomessa *tietosuojavaltuutetun toimistosta*[158], unionin sisäisestä rajatylittävästä kansallisten tietosuojaviranomaisten yhteistyöstä sekä Euroopan

[155] Ks. C-507/17 *Google v CNIL - Commission Nationale de l'Informatique et des Libertés* ECLI:EU:C:2019:772, kohta 60. Tuomion myötä Rekisteröityjen oikeus tulla unohdetuksi voidaan katsoa olevan maantieteellisesti rajattu.
[156] Ks. edellä kappale 3.2.3.1 Osoitusvelvollisuus.
[157] *Korpisaari* 2018, s. 96.
[158] Tietosuojavaltuutetun rooli tietosuojasääntelyn kokonaisvaltaisessa voimaan saattamisessa on ollut merkittävä. Tietosuojavaltuutetun toimintakertomuksen (2018) mukaan tietosuojavaltuutettu oli eduskunnan kuultavana yhteensä 93 kertaa ja antoi lausuntonsa 332 eri lainvalmisteluhankkeeseen *Tietosuojavaltuutetun toimisto* 2018a, s. 22.

tietosuojaneuvostosta (EDPB)[159]. Valvontaviranomaisten toimivallasta, tehtävistä ja valtuuksista säädetään Asetuksen artikloissa 55 – 59.

Asetuksen yhdenmukaistaessa jäsenmaiden tietosuojasääntelyä ja siihen kohdistettua valvontaa, yritysten on helpompi toimia useammassa EU jäsenmaassa samanaikaisesti, sillä kansainväliset yritykset voivat asioida vain yhden jäsenmaan valvontaviranomaisen kanssa. Puhutaan niin sanotusta *yhden luukun periaatteesta*, jossa yritys voi keskittää henkilötietojen käsittelyä koskevat asioinnit päätoimipaikkansa sijaintimaan valvontaviranomaiselle usean maan valvontaviranomaisen sijaan. Yhdenmukaistettu valvonta toteutetaan parhaimmillaan jäsenmaiden tietosuojaviranomaisten välisenä yhteistyönä.

3.3.2 Seuraamukset Asetuksen rikkomisesta

Asetuksen rikkomisen seuraamuksista säädetään artikloissa 58, 82 ja 83, sekä kansallisella tasolla tietosuojalain luvussa 4. Jos yritys laiminlyö Asetuksen velvoitteita ja aiheuttaa kyseisellä toiminnallaan Rekisteröidyille aineellista tai aineetonta vahinkoa tulee sen korvata aiheuttamansa vahinko.

Tietosuojalain 24 §:n mukaan Asetuksen 83 artiklan mukaisen hallinnollisen seuraamusmaksun määrää *tietosuojavaltuutetun* ja *apulaistietosuojavaltuutettujen* yhdessä muodostama *seuraamuskollegio*. Seuraamuskollegio perustettiin 1.5.2019 kun tietosuojavaltuutetun toimistoon nimettiin kaksi apulaistietosuojavaltuutettua[160]. Päätös seuraamusmaksun asettamisesta tehdään tietosuojalain 24.2 §:n mukaisesti seuraamuskollegiolle esittelystä. Seuraamuskollegion päätökseksi valitaan äänestyksen perusteella saanut enemmistön kanta. Tilanteessa, jossa äänet menevät tasan, valitaan päätökseksi vastaajalle lievempi seuraamus. Yrityksen hakiessa muutosta hallinto-oikeudelta, tietosuojavaltuutettu tai apulaistietosuojavaltuutettu voi tietosuojalain 25.3 §:n mukaan määrätä, että annettu päätös pidetään voimassa muutoksenhausta huolimatta, jollei valitusviranomainen toisin määrää.

[159] Euroopan tietosuojaneuvosto (European Data Protection Board - EDPB) on EU:n riippumaton elin, koostuen EU jäsenmaiden kansallisista tietosuojaviranomaisista sekä Euroopan tietosuojavaltuutetun edustajista. Tietosuojaneuvostoon kuuluvat myös ETA-maat Islanti, Norja ja Liechtenstein. EDPB vastaa mm. Asetuksen yhdenmukaisesta soveltamisesta. Tarkemmin EDPB:sta Ks. *Euroopan tietosuojaneuvosto* 2019, kohta Tietoa Euroopan tietosuojaneuvostosta.

[160] Suomen tietosuojavaltuutettuna toimii *Reijo Aarnio*, apulaistietosuojavaltuutettuna *Anu Taulus* ja *Jari Rämä Tietosuojavaltuutetun toimiston tiedote* 2019.

Määrättävät *hallinnolliset sakot* voivat olla yrityksille hyvinkin tuntuvia. Hallinnollisen sakon perusteista, edellytyksistä ja määrästä säädetään Asetuksen artikloissa 82 ja 83. Laiminlyönnistä määrättävä sakko on sidoksissa rikottuun velvoitteeseen. Asteikkoja on kaksi; esimerkiksi edellä esitettyjen velvollisuuksien, kappaleet 3.2.3.3 – 3.2.3.8, rikkomuksista voidaan määrätä sakko, joka on enintään 10 000 000 euroa tai 2 % edeltävän tilikauden vuotuisesta maailmanlaajuisesta kokonaisliikevaihdosta, kun taas esimerkiksi edellä kappaleiden 3.2.2 (henkilötietojen käsittelyperusteet) ja 3.2.4 (Rekisteröidyn oikeuksien toteuttaminen) rikkomuksesta voidaan määrätä sakko, joka on huomattavasti suurempi mutta enintään 20 000 000 euroa tai 4 % edeltävän tilikauden vuotuisesta maailmanlaajuisesta kokonaisliikevaihdosta. Sakkojen kohteena voi olla sekä yritys, joka on laiminlyönyt Asetuksen velvoitteitaan, että laiminlyöneen yrityksen sopimuskumppani. Yritykset ovat toisin sanoen yhteisvastuullisia ja voivat tarvittaessa hakea toisiltaan korvauksia regressioikeuteensa vedoten.[161] Rikkomuksesta voi siis joutua vastuuseen myös useampi taho, jos henkilötietoja on käsitellyt useampi Rekisterinpitäjä – kuten yhteistyötä tehneet yritykset. Käytännössä vastuun osoittaminen yritysten kesken voi olla haastavaa, kuten *Wennäkoski* kirjoittaa:

> ”*vastuunjako -- ei aina ole niin suoraviivaista, sillä esimerkiksi monet alustat ja sovellukset ovat yhteenkietoutuneita, ja toisistaan riippuvaisia, ja rajanveto sen suhteen, milloin yhden palveluntarjoajan vastuu loppuu ja toisen alkaa, voi osoittautua haastavaksi*”[162].

Tietosuojavaltuutetun tiedonsaanti- ja tarkastusoikeuden tehosteeksi on asetettavissa myös tietosuojalain 22 §:ään perustuva *uhkasakko*. Uhkasakon asettamisesta ja tuomitsemisesta maksettavaksi säädetään uhkasakkolaissa (1113/1990). Uhkasakko on annettavissa tehosteeksi myös Asetuksen 58.2 artiklan (c-g, j) alakohtien mukaisissa tilanteissa. Näitä ovat: (c) määrätä Rekisterinpitäjä noudattamaan Rekisteröidyn oikeuksiin perustuvia pyyntöjä; (d) määrätä Rekisterinpitäjä korjaamaan käsittelytoimiaan (tietyllä tavalla ja tietyn määräajan kuluessa); (e) määrätä Rekisterinpitäjä ilmoittamaan henkilötietojen tietoturvaloukkauksesta Rekisteröidylle; (f) asettaa väliaikainen tai pysyvä rajoitus käsittelylle, mukaan lukien käsittelykielto; (g) määrätä henkilötietojen oikaisemisesta tai poistamisesta tai käsittelyn rajoittamisesta 16, 17 ja 18 artiklan perusteella sekä näistä toimenpiteistä ilmoittamisesta niille vastaanottajille, joille henkilötietoja on luovutettu 17.2 artiklan ja 19 artiklan mukaisesti; sekä (j) määrätä tie-

[161] *Korpisaari* 2018, s. 269.
[162] *Wennäkoski* 2017, s. 85.

donsiirtojen keskeyttämisestä kolmannessa maassa olevalle vastaanottajalle tai kansainväliselle järjestölle.

Asetuksen myötä, yritysten on pystyttävä näyttämään Asetuksen lainmukainen noudattaminen toteen, on *Nyyssölää* lainattuna ”*melkoinen kummajainen oikeusjärjestelmässämme*”.[163] Oikeusjärjestelmämme todistusvastuuta koskeva pääsääntö *syyttömyysolettamasta*[164] on Asetuksen osoitusvelvollisuuden myötä käännetty päälaelleen. Tämän käännetyn todistustaakan johdosta todistusvastuu tietosuojasääntelyn noudattamisesta on nyt yrityksillä. Asetuksen 82.3 artiklan mukaan Rekisterinpitäjä on vastuusta vapaa vain jos se pystyy osoittamaan, ettei sen toiminta ole aiheuttanut Rekisteröidylle vahinkoa.

Luonnollisesti yritykset pyrkivät huomioimaan niiden toimintaa rasittavia riskejä ja pyrkivät mahdollisuuksien mukaan myös minimoimaan toteutuvien vahinkojen aiheuttamia kuluja. Ennakollisesti yritykset voivat pyrkiä parhaansa mukaan noudattaa pakottavia säännöksiä, pyrkiä valitsemaan luotettavia yhteistyökumppaneita ja vakuuttamaan toimintansa mahdollisimman kustannustehokkaasti. Finanssivalvonta on kuitenkin antanut tulkintansa hallinnollisten ja rikosoikeudellisten sakkojen sekä seuraamusmaksujen varalta vakuuttamisesta ja linjannut sen olevan ”*hyvän vakuutustavan vastaista ja ristiriidassa yhteiskunnassa yleisesti hyväksyttyjen arvojen kanssa*”[165]. Yritykset eivät toisinsanoen voi saada vakuutuksia Asetuksen seuraamusmaksujen aiheuttaman riskin varalle.

3.3.3 Hallinnollisten sakkojen oikeuskäytäntöä

Käytännössä Suomessa ei ole vielä langetettu yhtään hallinnollista seuraamusmaksua[166], johtuen mahdollisesti seuraamuskollegion myöhäisestä perustamisesta, mutta mahdollisesti myös tietosuojavaltuutetun *Reijo Aarnion* valitsemasta linjasta, kuten *Lång* kirjoittaa[167]. Aarnio on tuonut useammassa blogi kirjoituksessaan esille sanktiojärjestelmän riskistä ohjata yrityksiä ”*forum shoppingiin*”, jos kyseisen ilmentymän olemassa oloa ei huomioida päätöstenteossa.[168] Hallinnolliset sakot ovat silti olleet korostuneesti esillä Asetusta koskevassa julkisessa kes-

[163] Ks. *Nyyssölä* 2017, kohta Tietosuoja-asetus tuo työnantajille käännetyn todistustaakan.
[164] Ks. tarkemmin syyttömyysolettamasta prosessioikeudellisena perusperiaatteena *Korkein oikeus* 2019, kohta Syyttömyysolettama; Ks. myös Esitutkintalaki (805/2011) 4 luku 2 §.
[165] *Finanssivalvonta* 2018.
[166] Vrt. ETA-alueella annettujen sakkojen yhteismäärä oli noin 9 kuukautta Asetuksen täytäntöönpanosta yhteensä lähemmäs 56 miljoonaa euroa. *Euroopan tietosuojaneuvoston katsaus* 2019, s. 8.
[167] Ks. *Lång – Taka* 2019.
[168] Ks. *Aarnio* 2018, 2017 ja 2016.

kustelussa ja tiedottamisessa. Sakkojen langettamisesta on annettu maalikoille herkästi kuva viranomaisten ensisijaisena rangaistuskeinona tietosuojasääntelyn laiminlyönnissä. Todellisuudessa hallinnolliset sakot ovat puuttumiskeinoista sekä järein että viimeisin vaihtoehto. Tietosuojavaltuutetulla on käytettävissään monia muita kevyempiä ratkaisuja laiminlyöntitilanteita varten.[169] Asetuksen artikla 58 listaa laiminlyönnin korjaavia toimivaltuuksia, joita ovat muun muassa: varoitus, huomautus, henkilötietojen käsittelyn väliaikainen tai pysyvä rajoittaminen, määräys henkilötietojen oikaisemisesta tai poistamisesta, sekä artikla 42 ja 43 mukainen sertifioinnin peruuttaminen[170]. Tietosuojavaltuutettu voi näiden lisäksi tai sijaan langettaa laiminlyöneelle taholle artiklan 83 mukaisen hallinnollisen sakon. Seuraamuskollegion päätyessä hallinnollisiin sakkoihin, tarvitsee heidän punnita tapausta kokonaisuutena 83.2 artiklan mukaisesti. Sakkojen tulee toisin sanoen olla suuruusluokaltaan varottavuuden ja tehokkuuden lisäksi aina myös oikeassa suhteessa tapahtuneeseen laiminlyöntiin nähden. Kussakin yksittäistapauksessa on myös huomioitava muun muassa laiminlyönnin luonne, vakavuus ja kesto, sekä teon tuottamuksellisuus[171].

Vaikka Suomessa ei ole vielä langetettu hallinnollisia seuraamusmaksuja, tietosuojavaltuutetulle vireille tulleiden asiamäärien runsas kasvu kertoo tietosuoja-asioiden kiinnostuksesta ja korostumisesta yhteiskunnassa. Vuonna 2017 Suomen tietosuojavaltuutetun toimisto vastaanotti 3957 tapausta, kun 2018 asiamäärät yli kaksinkertaistuivat, jolloin vireille tuli jopa 9617 tapausta – joista 23,1 % eli 2220 tapausta koski tietoturvaloukkauksia[172].

Sanktiomekanisminsa ja ankaruutensa vuoksi Asetuksen sanktiouhkaa ja määrättäviä sakkoja on verrattu EU:ssa jo vakiintuneisiin kilpailuoikeudellisiin sanktioihin.[173] Kilpailuoikeudellisissa rikkomuksissa Euroopan komissio voi sulautuma-asetuksen[174] artiklan 14.2 mukaan määrätä yritykselle sakon, joka on enintään 10 % keskittymään osallistuvan yrityksen koko-

[169] Ks. *Pitkänen* 2018, s. 534–353 ja 537.
[170] Ks. sertifioinneista tarkemmin seuraavassa luvussa 4.
[171] Ks. hallinnollisten sakkojen määräämisessä huomiotavat asiat Asetuksen artiklan 83.2 alakohdat (a-k).
[172] *Tietosuojavaltuutetun toimisto* 2018a, s. 26.
[173] Ks. *Heikinsalmi* 2009, s. 76; *Mäenpää* 2018, s. 4; *Lång* 2016, s. 7; *Wennäkoski* 2017, s. 77, 88–91; Ks. myös kilpailulainsäädännön ja tietosuojalainsäädännön tavoitteiden osittaisesta ristiriitaisuudesta *Warma – Nieminen* 2016, s. 566–569.
[174] Neuvoston asetus (EY) N:o 139/2004, annettu 20 päivänä tammikuuta 2004, yrityskeskittymien valvonnasta ("EY:n sulautuma-asetus").

naisliikevaihdosta, jos nämä tahallaan tai tuottamuksesta rikkovat asetuksessa määritettyjä velvoitteita[175].

3.4 Asetuksen Rekisterinpitäjälle aiheuttavista kustannuksista

3.4.1 Yleistä Asetuksen yritysvaikutuksista

Asetuksen velvoitteiden noudattaminen ja toteuttaminen aiheuttavat yrityksille kustannuksia. Vaikka kaikki Asetuksen velvoitteet eivät ole yritykselle uusia suhteessa henkilötietodirektiivin ja henkilötietolain (HeTL, 523/1999)[176] aikaisiin velvoitteisiin, Asetuksen on katsottu aiheuttavan moninaisia kustannuksia Rekisterinpitäjille niin yksityisellä kuin julkisellakin sektorilla[177]. Asetuksen aiheuttamat kustannukset kohdistuvat kaikkiin yrityksiin, jotka käsittelevät henkilötietoja, tarkoittaen käytännössä koko yrityskenttää[178]. Asetuksen hallinnollista taakkaa ja taloudellisia vaikutuksia on arvioitu useammassa selvityksessä ja muistiossa ennen Asetuksen voimaan tuloa ja sittemmin myös jälkiseurannan muodossa. Tutkielman kannalta tärkeimpiä ovat ne selvitykset, jotka ottavat kantaa Suomessa toimiville yrityksille kohdistuneisiin kustannuksiin.

Suomen keskeisimpiin neuvottelutavoitteisiin Asetuksen valmistelussa oli taata yrityksille järkevät ratkaisut, pysyttäen Asetuksen yrityksille aiheuttamat kustannukset ja hallinnollisen taakan kohtuullisena.[179] Tavoitteiden toteutumista on kuitenkin kritisoitu, muun muassa Elinkeinoelämän keskusliiton mukaan Asetus voi aiheuttaa merkittäviä kustannuksia yrityksille.[180] Merkittävimpiä kustannusten aiheuttajia ovat Asetuksen uudet velvoitteet. Uusien velvoitteiden myötä yritysten investoinnit ja kulut henkilötietojen käsittelyn toteuttamiseksi ovat odotettavasti kasvaneet. Valtioneuvoston selvitys- ja tutkimustoiminnan rahoittaman Tampereen yliopiston tekemän selvityksen mukaan, Asetuksen uusien velvoitteiden aiheuttaman kertainvestoinnin arvioitiin olevan *suuryritysten*[181] osalta suuruusluokkaa 2,5 miljoonaa eu-

[175] Viimeaikaisista sanktioista esimerkkinä sulautuma-asetuksen sakkojen langettamisesta komission Canonille langettamat sakot 28 miljoonaa euroa, Canonin edetessä yrityskaupoissa Toshiba Medical Systems Corporation kanssa ennen komission lopullista hyväksyntää (M.8179).
[176] HeTL on kumottu 1.1.2019 voimaan tulleella tietosuojalailla (1050/2018).
[177] *HE 9/2018 vp*, s. 64.
[178] *Lång* 2016, s. 1.
[179] *HaVL 25/2015 vp*, s. 2, 4–5.
[180] *Elinkeinoelämän keskusliitto* 2015, s. 2–3.
[181] Yritys, jonka henkilöstön määrä on vähintään 250 henkilöä ja liikevaihto yli 50 miljoonaa euroa tai taseen loppusumma yli 43 miljoonaa euroa määritellään suuryritykseksi perustuen Euroopan komission suositukseen mikroyritysten sekä pienten ja keskisuurten yritysten määritelmästä (2003/361/EY). Suosituksen artikla 2 mukaan mikroyritysten sekä pienten ja keskisuurten yritysten (pk-yritysten) luokka koostuu yrityksistä, joiden pal-

roa, jonka jälkeen jatkuvaiskulujen arvioitiin olevan noin 900 000 euroa.[182] Vertailukohtana mainittakoon Kuntaliiton arvio, jonka mukaan maltillinen arvio Asetuksen velvoitteista aiheuttaa kunnille jopa 100–200 miljoonan euron vuotuiset kulut.[183] Puhutaan siis kiistatta merkittävistä kulueristä, ottaen huomioon suomalaisyritysten vähäiset taloudelliset panostukset tietosuojasääntelyä kohtaan ennen Asetuksen voimaan tuloa[184].

Komissio on arvioinut Asetuksen tuovan vuosittain jopa 2,3 miljardin euron säästöt yritysmaailmalle.[185] Säästöt kohdistunevat kuitenkin pääsääntöisesti kansainvälisiin yrityksiin, joiden liiketoimintaa harjoitetaan useammassa EU jäsenmaassa. On siis oletettavaa, että komission yrityksille arvioimat säästöt koostuvat suurilta osin tietosuojasääntelyn yhdenmukaistumisesta. Kansainvälisten yritysten ei enää tarvitse Asetuksen myötä sitoa resursseja jokaiseen jäsenmaahan erikseen, selvittääkseen näissä voimassa olevat tietosuojasäännökset.

Asetuksen velvoitteita on kevennetty myös pk-yritysten osalta. Esimerkiksi artiklan 30 vaatimus käsittelytoimia koskevan selosteen ylläpidosta ei lähtökohtaisesti koske yrityksiä, joissa on alle 250 työntekijää. Tarkoittaen, ettei kyseinen velvoite lähtökohtaisesti myöskään aiheuta kustannuksia tämän kokoluokan yrityksissä. Toisena esimerkkinä mainittakoon artiklan 35 DPIA:n tekeminen, joka on rajattu koskemaan vain yrityksiä, joiden henkilötietojen käsittely voidaan luokitella todennäköisesti korkeariskiseksi. DPIA:n toteuttaminen Asetuksen mukaisesti vaatinee moniportaisena prosessina sen alaisuudessa olevilta yrityksiltä paljon taloudellista panostusta ja investointeja[186]. DPIA:n aiheuttama taloudellinen kuorma onkin täysin riippuvainen yrityksestä ja sen toimenkuvasta Henkilötietojen käsittelijänä. Kolmantena esimerkkinä Asetuksen mahdollistama yhden luukun järjestelmä, eli yritysten mahdollisuus asioida vain yhden tietosuojaviranomaisen kanssa, keventänee useassa EU jäsenmaassa toimivien yritysten compliance – velvoitteita ja tuo siten mahdollisesti myös säästöjä kyseisten yritysten hallinnollisiin kuluihin.[187] Myös ilmoitus- ja rekisteröitymisvelvollisuuksia on Asetuk-

---

veluksessa on vähemmän kuin 250 työntekijää ja joiden vuosiliikevaihto on enintään 50 miljoonaa euroa; pieni yritys määritellään yritykseksi, jonka palveluksessa on vähemmän kuin 50 työntekijää ja jonka vuosiliikevaihto tai taseen loppusumma on enintään 10 miljoonaa euroa; mikroyritys määritellään yritykseksi, jonka palveluksessa on vähemmän kuin 10 työntekijää ja jonka vuosiliikevaihto tai taseen loppusumma on enintään 2 miljoonaa euroa.

[182] Huomattavaa, etteivät pienet ja keskisuuret yritykset osanneet selvityksessä vielä arvioida tietosuojasääntelyn uudistumisen kustannuksia. Ks. *Valtioneuvoston selvitys* 2017, s. 9.

[183] *Elinkeinoelämän keskusliitto* 2015, s. 5.

[184] Ks. *Lång* 2016, s. 5.

[185] *SEC (2012) 72, lopull.*, s. 71.

[186] Ks. DPIA:n sisällöstä ja käytännön ohjeet *Tietosuojavaltuutetun toimisto* 2019f, kohta Vaikutustenarviointi.

[187] Vrt. *Moerel* 2019, s. 2.

sen avulla kevennetty, mutta tämä ei juurikaan hyödytä Suomalaisia yrityksiä kansallisen lainsäädännön ollessa jo ennen Asetusta tämän osalta huomattavasti kevyempi kuin monessa muussa EU jäsenmaassa.[188]

3.4.2 Kustannuksista tarkemmin

Asetuksen aiheuttamat kustannukset voidaan jakaa välittömiin ja välillisiin kustannuksiin. *Välittömillä kustannuksilla* tarkoitetaan hallinnollisista velvoitteista aiheutuvia suoria kuluja, joita sääntely aiheuttaa yrityksille – voidaan puhua myös yritysten jatkuvaluonteisista kustannuksista. Välittömiä hallinnollisia kuluja aiheutuu muun muassa tietosuojavastaavan nimittämisestä sekä tietojärjestelmien uusimisesta. *Välilliset kulut* taas muodostuvat muun muassa yrityskohtaisten riskikartoitusten ja sen perusteella päätetyn riskienhallintakäytäntöjen kautta.[189] Välilliset kulut voivatkin olla hyvin eri kokoluokkaa eri yritysten välillä. Kustannuksien vaihteluun vaikuttanee myös yritysten kulttuurilliset erot. Joidenkin yritysten kohdalla pelkästään hypoteettinen mahdollisuus joutua hallinnollisten seuraamusmaksujen kohteeksi tai pyrkimys saada kilpailuetua ja hyvää mainetta markkinoilla riittää investoimaan ja panostamaan tietosuojasääntelyn velvoitteisiin, kun toinen yritys taas pyrkii laskelmoimaan riskit ja toteuttaa vain pakollisen minimin Asetuksen vaatimusten toteuttamiseksi[190].[191] Toisin sanoen, taloudelliset vaikutukset ovat riippuvaisia yrityksen toimialasta, yhtiömuodosta, omistusrakenteesta ja kansainvälisyydestä. Lisäksi eroihin vaikuttaa yritysten koko; isojen yritysten mahdollisuudet ja intressit panostaa Asetuksen noudattamiseen ovat lähtökohtaisesti suuremmat kuin pk-yrityksillä.[192]

Asetuksen uusien velvoitteiden uskottiin aiheuttavan yrityksille kustannuksia. Oikeusministeriön tilaaman selvityksen mukaan, merkittävimmät uudet velvoitteet ovat tietosuojavastaavan nimittäminen ja velvoite ilmoittaa tietomurrosta sekä viranomaisille että Rekisteröidyille. Selvityksen mukaan erityisesti Asetuksen *compliance-velvoitteet* tulevat kuormittamaan yrityksiä taloudellisesti, näihin lukeutuu muun muassa osoitusvelvollisuus ja sisäänrakennetun tietosuojan vaatimus, ennakkokuuleminen sekä ennakollinen riskien hallinta ja DPIA. Käytännössä osoitusvelvollisuuden kustannukset muodostuvat yritysten sisäisen hallinnon uudelleen

[188] Ks. *HE 9/2018 vp*, s. 66-67; *Lång* 2016, s. 8–9.
[189] *Lång* 2016, s. 6–7.
[190] Ks. *Acubiz* 2019, kohta Compliance as a competitive advantage or a risk factor?
[191] *HE 9/2018 vp*, s. 66–67.
[192] Ks. *Lång* 2016, s. 2–4.

järjestelemisestä sekä tarvittavien toimenpiteiden tekemisestä riskienhallinnan toteuttamiseksi kuten teknisten ja organisatoristen toimenpiteiden huomioimisesta.[193] Asetusta koskevissa vaikutusarvioinneissa hallinnollisia kuluja uskottiin aiheuttavan myös Asetuksen useat velvollisuudet laatia, ylläpitää, uudistaa ja luovuttaa yrityksen henkilötietoja käsitteleviä asiakirja-aineistoja muun muassa huolehtiessaan Rekisteröidyn oikeuksista ja henkilörekisteritietojen oikeellisuudesta. Mainittujen velvoitteiden toteuttaminen tarkoittaa käytännössä monelle yritykselle IT-järjestelmien päivittämistä ja uusien hankkimista.[194] Kuluja aiheutunee myös tietojenkäsittelyä koskevien sopimusten laatimisesta ja hallinnoinnista.[195] Lisäksi moni yritys lienee turvautunut Asetuksen vaatimusten toteuttamisessa ulkopuolisten asiantuntijoiden ja konsulttien apuun.[196] Tietosuojasääntelyn noudattamisen ulkoistaminen voi kuitenkin olla monella tapaa yritykselle resursseja ja varoja säästävä valinta, varsinkin jos vaihtoehtona on kokonaan uuden asian huomioiminen organisaatiossa ja useiden uusien henkilöiden palkkaaminen tehtävien hoitamista varten.

Oikeusministeriön tilaaman selvityksen lisäksi, myös valtioneuvoston suomalaisille yrityksille teettämä selvitys arvioi Asetuksen yrityksille aiheutuvia kustannuksia. Selvityksen mukaan hallinnollista taakkaa uskottiin aiheuttavan muun muassa henkilötietojen käsittelyä koskevien periaatteiden noudattaminen, Rekisteröidyn suostumus-vaatimuksista huolehtiminen, sekä käsittelytoimien selosteen ylläpito.[197] Oikeusministeriön selvitystä mukaillen, myös valtioneuvoston selvityksessä korostuu yritysten *compliance – kustannukset* sekä tietosuojavastaavan nimittämisestä aiheutuvat lisäkulut[198]. Myös Asetuksen tuoman taloudellisen sanktion uhka välillisenä kustannuksena uskottiin osoittautuvan merkittäväksi monen yrityksen kohdalla.[199] Muutos on huomattava Asetuksen edeltävään aikaan verrattuna, jolloin tietosuojalainsäädännön rikkomisesta ei voinut seurata muuta kuin matalahkot uhkasakot[200]. Taloudellisen sanktion uhan ja tietosuojaskandaalin aiheuttaman mahdollisen mainehaitan epätodennäköisyys lienee ainakin osasyy, miksi tietosuojasääntelyn asemaa ei ole kaikissa suomalaisissa

[193] *Lång* 2016, s. 7, 11–14 ja 18–19.
[194] *Lång 2016*, s. 15–17; Ks. myös *Valtioneuvoston selvitys* 2017, s. 9.
[195] *Lång 2016*, s. 7–8, 18–19 ja 20. Asiasta tarkemmin seuraavassa luvussa 4.
[196] Ks. *Lång 2016*, s. 20; *HE 9/2018 vp*, s. 68–69.
[197] *Valtioneuvoston selvitys* 2017, s. 2 ja 6.
[198] Suuret yritykset arvioivat tietosuojavastaavan vuosikuluksi n. 70 000 euroa. *Valtioneuvoston selvitys* 2017, s. 6.
[199] *Valtioneuvoston selvitys* 2017, s. 7 ja 20.
[200] Tietosuojalailla kumotun henkilötietolain 46 §:n mukaan: *"Tietosuojavaltuutettu voi asettaa 39 §:n 1 ja 3 momentin mukaisen tietojenantovelvollisuuden ja 40 §:n 2 momentin nojalla tekemänsä päätöksen ja tietosuojalautakunta 39 §:n 1 momentin mukaisen tietojenantovelvollisuuden ja 44 §:n nojalla tekemänsä päätöksen tehosteeksi uhkasakon siten kuin uhkasakkolaissa (1113/1990) säädetään."*

yrityksissä aikaisemmin nähty merkittävänä.[201] Nähtäväksi jää missä määrin yritykset huomioivat hallinnollisen seuraamuksen riskien budjetoinnissaan ja miten Henkilötietojen käsittelijät tulevat hinnoittelemaan heille sopimuksin siirrettyjä riskejä.[202]

Aloitetun jälkiseurannan perusteella vaikutusarvioinneissa esille nousseet kuormaa odotettavasti aiheuttavat velvoitteet ovat monilta osin pysyneet samoina. Oikeusministeriön lausuntopyyntöön vastanneiden mukaan[203] ja komission asiantuntijaryhmälle teettämän kyselyn perusteella[204], artiklan 35 mukainen yritysten tietosuojaa koskevan DPIA:n toteuttaminen on osoittautunut myös käytännössä haasteelliseksi. Vastausten mukaan DPIA tarvitsisi tarkennusta muun muassa sen yleistä sisältöä ja arviointivaatimuksia koskien. DPIA:n sisältämän henkilötietojen käsittelyn aiheuttaman korkean riskin määrittäminen nähtiin ongelmalliseksi.[205] DPIA:n kuormittavuus näkyy erityisesti pk-yrityksissä, joissa Asetuksen noudattamista vaikeuttavat rajatut resurssit ja osaamisvaje.[206] Myös artiklan 30 seloste käsittelytoimista on osoittautunut vastanneiden mukaan työlääksi ja vaatimuksiltaan osin päällekkäiseksi Rekisteröidyille annettavan tiedonantovelvoitteen kanssa.[207]

Myös Asetuksen osoitusvelvollisuuden ja compliance- velvoitteiden toteuttaminen ovat odotetusti lisänneet yritysten hallinnollista taakkaa ja aiheuttaneet merkittäviä kustannuksia.[208] Komission asiantuntijaryhmän vastausten perusteella, suurin osa yritysten Asetuksen täytäntöönpanon vaatimista resursseista on kohdistunut osoitusvelvollisuuden toteuttamiseen, Rekisteröityjen suostumusten pyytämiseen, tietosuojailmoitusten ja Tietojenkäsittelysopimusten päivittämiseen, tietojärjestelmien uusimiseen, tietosuojarikkomusten käsittelyyn sekä henki-

---

[201] Ks. *Lång* 2016, s. 5.
[202] *Lång* 2016, s. 22–23; Ks. myös *Valtioneuvoston selvitys* 2017, s. 6.
[203] Ks. *Oikeusministeriön selvitys* 2019, kohta Jakelu.
[204] Ks. *Komission asiantuntijaryhmä* 2019, kohta Jäsenet; *Komission asiantuntijaryhmälle tehty selvitys* 2019, kohta Asiakirjat.
[205] Näkemyksen jakoi mm. Elinkeinoelämän keskusliitto, Finanssiala ry, Kilpailu- ja kuluttajavirasto, Helsingin yliopisto. Riskien arviointi ja määrittäminen koettiin myös yleisellä tasolla haasteelliseksi niin Oikeusministeriön kuin komission saamissa vastauksissa. Ks. *Oikeusministeriön selvitys* 2019, kohta Lausunnonantajien lausunnot; *Komission asiantuntijaryhmän raportti* 2019, s. 4.
[206] Ks. myös *Komission asiantuntijaryhmän raportti* 2019, s. 15.
[207] Näkemyksen jakoi mm. Oikeusrekisterikeskus, Itä-Savon koulutuskuntayhtymän, Senaatti-kiinteistöt. Lisäksi Suomen Yrittäjät ry kyseenalaistaa lausunnossaan artiklan 30 sisältämän pk-yrityksiä koskevan kevennyksen, tarkoittaen, ettei hallinnollinen taakka käytännössä ole pienempi kyseisen säännöksen osalta pk-yrityksille artiklan 30.5 sisältämien poikkeusten vuoksi: ”*Asetuksen sanamuodon mukaan selosteen ylläpitämisvelvollisuus koskee siten käytännössä kaikkia yrityksiä, myös pk- ja mikroyrityksiä, koska käytännössä kaikilla yrityksillä on työntekijöitä tai asiakasrekisteri. Artiklaan kirjattu oikeus poiketa velvollisuudesta jää siten epäselväksi ja sen merkitys kyseenalaiseksi.*” Ks. *Oikeusministeriön selvitys* 2019, kohta Lausunnonantajien lausunnot.
[208] *Komission asiantuntijaryhmän raportti* 2019, s. 4 ja 14.

löstön tiedottamiseen ja koulutukseen.[209] Pk-yritysten osalta Asetuksen täytäntöönpano ja noudattaminen ovat vaatineet huomattavia resursseja suhteessa isompiin toimijoihin. Suurempi hallinnollinen taakka selittyy vastausten mukaan osaamis- ja resursointivajeena niin henkilöstön, tietojärjestelmien kuin taloudenkin osalta. Yrityksen toiminnan lainmukaisuuden varmistamiseksi, pk-yritykset ovat joutuneet konsultoimaan ulkopuolisia asiantuntijoita sekä kouluttamaan työntekijöitään.[210]

Oikeusministeriön saamissa lausunnoissa mainittiin myös muita hallinnosta taakkaa nostavia Asetuksen velvoitteita kuten tietoturvaloukkauksista ilmoittaminen sekä tietosuojavastaavan nimittäminen.[211] Finanssiala ry:n mukaan tietoturvaloukkauksista ilmoittaminen on kasvattanut yritysten kustannuksia, sekä vaatinut resursseja erityisesti pienissä yrityksissä. Kuluja on aiheutunut muun muassa ylitöistä ja päivystyksistä.[212] Myös Asetuksen käsitteiden ja terminologian vaikeus ja niistä johtuvat tulkintaongelmat korostuivat Oikeusministeriölle annetuissa lausunnoissa. Epäselvyyttä ylitse muiden, on ilmennyt Henkilötietojen käsittelijän, Rekisterinpitäjän ja erityisesti yhteisrekisterinpitäjien määritelmien tulkinnassa ja vastuunjakokysymysten selvittämisessä.[213]

3.5 Yhteenveto

Asetuksen kansallisen täytäntöönpanon valmisteluvaiheessa, lainsäädännön arviointineuvosto otti kantaa hallituksen esityksen luonnoksen sisältöön. Arviointineuvosto kritisoi lausunnossaan tehtyjen vaikutusarviointien riittämättömyyttä ja puutteellisuutta.[214] Arviointineuvoston

[209] *Komission asiantuntijaryhmän raportti* 2019, s. 4, 7 ja 16.
[210] *Komission asiantuntijaryhmän raportti* 2019, s. 4, 14–16.
[211] Tietosuojavastaavan nimittämisen mainitsi mm. SOSTE Suomen sosiaali- ja terveys ry, Oikeusrekisterikeskus, Itä-Savon koulutuskuntayhtymän, Suomen Yrittäjät ry. Tietoturvaloukkausten ilmoitusvelvollisuus sitoi resursseja ja on lisännyt hallinnollista taakkaa mm. Elinkeinoelämän keskusliiton (EK), Finanssiala ry:n, Secrays Oy:n, Helsingin kaupungin ja Senaatti-kiinteistöjen mukaan. Ks. *Oikeusministeriön selvitys* 2019, kohta Lausunnonantajien lausunnot.
[212] Ks. *Oikeusministeriön selvitys* 2019, kohta Lausunnonantajien lausunnot.
[213] Sama huomio tehtiin komission asiantuntijaryhmässä *Komission asiantuntijaryhmän raportti* 2019, s. 18; Oikeusministeriön saamissa lausunnoissa Henkilötietojen käsittelijän ja Rekisterinpitäjän välisiä vastuita ja epäselviä rooleja käsiteltiin myös runsaasti. Asian toi esille mm. CSC-Tieteen tietotekniikan keskus Oy , Etelä-Suomen aluehallintovirasto, STM, Liikenne- ja viestintävirasto, Secrays Oy, Kansallisarkisto, Suomalaisen Kirjallisuuden Seura, Itä-Savon koulutuskuntayhtymän, Senaatti-kiinteistöt, Opetus- ja kulttuuriministeriö, Terveyden ja hyvinvoinnin laitos THL, Jyväskylän yliopisto, Ammattikorkeakoulujen rehtorineuvosto Arene ry. Haasteet koskien yhteisrekisterinpitäjän määritelmää ja velvoitteita mainitsi: Opetushallitus, F-Secure Oyj, Elinkeinoelämän keskusliitto EK, Maa- ja metsätalousministeriö, STM, Liikenne- ja viestintävirasto, Suomen sosiaali- ja terveys ry, Kansallisarkisto. Jyväskylän yliopisto, Helsingin yliopisto, Suomen Lääkäriliitto, Keskuskauppakamari, Toimihenkilökeskusjärjestö STTK ry, Kansaneläkelaitos, HKI kaupunki, Senaatti-kiinteistöt. Ks. *Oikeusministeriön selvitys* 2019, kohta Lausunnonantajien lausunnot.
[214] *Lainsäädännön arviointineuvoston lausunto (VNK/133/32/2018)* 2018, s. 1–2.

lausunto huomioitiin hallituksen lopullisessa esityksessä, mutta Asetuksen lopulliset vaikutukset yrityksille selvinnee vasta myöhemmin, kun Asetuksen täytäntöönpanosta on kulunut riittävästi aikaa. Asetuksen yrityksille aiheuttamat pitkäaikaiset jatkuvaiskulut vaativatkin ilmetäkseen usean vuoden käytännön soveltamista. Asetuksen velvoitteiden täytäntöönpano mahdollistaa kuitenkin yritysvaikutusten yksityiskohtaisemman ja kattavamman selvittämisen jälkiseurannan muodossa, jo lyhyelläkin aikavälillä.

Tietosuojasääntelyn täytäntöönpanon valvonta ja ohjeistus on keskittynyt pääosin komissiolle ja EDPB:lle.[215] Komission heinäkuussa 2019 julkaisemassa tiedonannossa tarkastellaan unionin tietosuojasääntöjen vaikutuksia ja pohditaan miten sääntelyn täytäntöönpanoa voitaisiin parantaa.[216] Lisäksi komissio on teettänyt kyselyn asiantuntijaryhmälle Asetuksen täytäntöönpanosta. Kyselyllä selvitettiin asiantuntijaryhmän kokemuksia Asetuksen toimivuudesta ja selvitettiin heidän näkemyksiään parannusehdotuksista.[217] Myös kansallinen tietosuojasääntelyn yritysvaikutusten jälkiseuranta on käynnistynyt, kun Oikeusministeriö julkaisi elokuussa 2019 lausuntopyynnön Asetuksen toimivuudesta ja sen soveltamiseen liittyvistä kokemuksista.[218] Selvityksistä saadut tulokset eivät ole kuitenkaan vielä tarkkuudeltaan riittäviä, jotta voitaisiin arvioida onko Asetuksen yrityksille aiheuttamat kustannukset ja hallinnollinen taakka onnistuttu pitämään kohtuullisena.[219]

[215] Ks. tietosuojavaltuutetun toimiston laatima kattava listaus EDPB:n antamista ohjeistuksista *Euroopan tietosuojaneuvoston ohjeet* 2019.
[216] Ks. *COM (2019) 374, lopull.*, s. 17–21.
[217] *Komission asiantuntijaryhmän raportti* 2019, s. 3–4.
[218] Ks. *Oikeusministeriön selvitys* 2019.
[219] Vrt. *HaVL 25/2015 vp*, s. 2–5.

4 ARTIKLAN 28 AIHEUTTAMISTA VAIKUTUKSISTA SUOMESSA TOIMIVILLE YRITYKSILLE

4.1 Tietojenkäsittelysopimuksista lyhyesti

Asetuksen vaatimus Tietojenkäsittelysopimusten laatimisesta on yksi merkittävimmistä Asetuksen tuomista muutoksista yritysten arkeen. Asetuksen artiklan 28 mukaan Rekisterinpitäjän ulkoistaessa kaikki tai edes osan henkilötietojensa käsittelystä Henkilötietojen käsittelijälle, käsittelystä on laadittava kirjallinen sopimus.[220] Artiklan 28 kohtien 3 ja 4 sisältämät Sopimusvaatimukset, henkilötietojen käsittelyä koskevista Tietojenkäsittelysopimusten minimivaatimuksista, on Asetuksen voimaan tulon myötä huomioitava myös yrityksen jo voimassa olevissa sopimuksissa. Käytännössä tämä tarkoittaa yritysten lukuisten palvelusopimusten päivittämistä Asetuksen mukaiseksi, jos sopimusten sisältämä henkilötietojen käsittely on jatkunut Asetuksen voimaan tulon jälkeen.

Tietojenkäsittelysopimusten tarkoituksena on sisällyttää artiklan 28 Sopimusvaatimukset osaksi yritysten henkilötietojen käsittelyä koskevia sopimuksia. Tietojenkäsittelysopimuksessa määritellään Rekisterinpitäjän ja Henkilötietojen käsittelijän oikeudet ja vastuut henkilötietojen käsittelyssä. Huomattavaa on, että ulkoistamalla henkilötietojen käsittelyn yrityksen ei ole mahdollista vapautua sille asetetuista Rekisterinpitäjän vastuista tai velvollisuuksista. Tämän vuoksi onkin tärkeää, että ulkoistava yritys panostaa palveluntarjoajien valintaan sekä Tietojenkäsittelysopimusten sisältöön.

Artikla 28 sisältää yritysten Tietojenkäsittelysopimusten laadintaa keventäviä toimenpidemahdollisuuksia, kuten mahdollisuuden hyödyntää EU:n tai Suomen tietosuojavaltuutetun toimiston laatimia v*akiosopimuslausekkeita*. Mutta viranomaiset eivät ole näitä vielä tutkielman kirjoitusvaiheessa julkaisseet. Käytännössä tämä on johtanut siihen, että yritykset ovat joutuneet neuvottelemaan ja laatimaan Tietojenkäsittelysopimukset alusta alkaen itse.[221] Lisäksi yrityksissä käsiteltävien henkilötietojen ja ulkoistettavien palveluiden kirjo on laaja, jonka vuoksi kulloinkin soveltuvat Tietojenkäsittelysopimukset voivat erota paljonkin toisistaan.[222] Tietojenkäsittelysopimusten vaatimuksiin perehtyminen, niiden laatiminen ja neuvottelu sekä olemassa olevien sopimusten päivittäminen ovatkin oletettavasti työllistäneet yrityk-

[220] Artikla 28 sisällytetty kokonaisuudessaan tutkielman liitteeksi 1.
[221] Ks. esimerkki Tietojenkäsittelysopimuksesta *Huikko ym.* 2017, s. 18–22.
[222] Ks. *Partanen* 2018, kohta Tietosuojasopimuksia on monenlaisia.

siä merkittävästi. Kirjoitettavan tutkielman tarkoituksena on selvittää artiklan 28 velvoitteet ja vaikutukset yritysten toiminnassa, eli miten Sopimusvaatimukset vaikuttavat Suomessa toimivien yritysten toimintaan. Aihe on merkittävä pohdittaessa sääntelyn yrityksille aiheuttamaa taakkaa.

Vaikka tietosuojavaltuutettu on ollut aktiivinen ja julkaissut useita ohjeistuksia koskien tietosuojasääntelyn tulkintaa sekä raportoinut tietosuojavaltuutetun toimiston arvioitavaksi tulleista kysymyksistä, Oikeusministeriölle annetuissa lausunnoissa painottuivat epätietoisuus Sopimusvaatimusten soveltamisesta sekä Sopimusvaatimusten aiheuttama huomattava kuorma. Jotta Tietojenkäsittelysopimusten toteutuneet yritysvaikutukset Suomessa toimiville yrityksille olisi mahdollista saada selvitettyä riittävällä tarkkuudella, tutkielman ohessa toteutettiin erillinen kyselytutkimus. Kyselyä ja sen tuloksia on esitelty tarkemmin luvussa 5.

Tässä luvussa käydään läpi artikla 28 sisältämät velvoitteet ja näiden velvoitteiden aiheuttamia yritysvaikutuksia Suomessa toimiville yrityksille. Tutkielman rajauksesta johtuen, tässä luvussa ei tulla käsittelemään Sopimusvaatimusten vaikutuksia yritysten eri markkina-alojen välillä, vaan kaikkia yrityksiä käsitellään yhtenä joukkona. Lukijan on myös hyvä huomioida, että yritysten joukko on rajattu Suomessa toimiviin yksityisiin yrityksiin, jättäen ulkopuolelle julkisessa omistuksessa olevat yritykset sekä kansainvälisen vertailun – vaikkakin aihetta sivutaan lyhyesti.

4.2 Artiklan 28 velvoitteet

4.2.1 Henkilötietojen käsittelyn ulkoistaminen

Rekisterinpitäjänä toimiva yritys voi halutessaan ulkoistaa henkilötietojen käsittelyn tai osia siitä valitsemalleen palveluntarjoajalle – Henkilötietojen käsittelijälle. Henkilötietojen käsittelijä käsittelee henkilötietoja Rekisterinpitäjän lukuun, eikä sillä tästä syystä ole päätösvaltaa esimerkiksi mitä ja miten se niitä käsittelee. Tarve ulkoistamiselle voi olla esimerkiksi tilanteissa, joissa yrityksen omat resurssit kuten toiminnot, henkilöstö tai tietojärjestelmät eivät riitä hallinnoimaan yrityksen käsittelemiä henkilötietoja. Yrityksellä voi muun muassa olla tarve ostaa henkilötietojen säilytys-, analysointi- tai palkkahallinnonpalveluita[223]. Esimerkiksi, jos vakuutusyhtiö jakaa henkilötietoja salatulla sähköpostilla, kyseisen sähköpostipalvelun tarjoaja on vakuutusyhtiön Henkilötietojen käsittelijä. Asetuksen sisältämien velvollisuuksien

[223] *Elinkeinoelämän keskusliitto* 2019, kohta 5.2.8. henkilötietojen käsittelyn ulkoistaminen.

kannalta merkittävää on henkilötietojen käsittelyn päätäntävallan kohdistumisella. Sopimuskumppanit eivät voi keskenään sopia kumpi toimii tietojenkäsittelyn osalta Rekisterinpitäjänä ja kumpi Henkilötietojen käsittelijänä, sillä tosiasiallinen tilanne ratkaisee. Osapuoli, joka määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot katsotaan Rekisterinpitäjäksi[224]. Käsittelyä koskeva tekninen toteutus on kuitenkin osa ulkoistettavaa palvelua, eikä sen toteuttamisesta päättäminen ole kirjallisuuden mukaan Rekisterinpitäjää määrittelevä ominaisuus.[225] Jos Henkilötietojen käsittelijäksi katsottu sopimuskumppani alkaa käsitellä yritykseltä saamiaan tietoja esimerkiksi omiin tarkoituksiinsa tai vastoin Rekisterinpitäjän antamia ohjeistuksia, Henkilötietojen käsittelijästä tulee Rekisterinpitäjä – Rekisterinpitäjän vastuineen ja velvollisuuksineen.[226]

Artiklan 28.3 mukaan Rekisterinpitäjän lukuun tehtävästä henkilötietojen käsittelystä on laadittava Tietojenkäsittelysopimus. Yrityksen henkilötietojen käsittelyä koskevat Tietojenkäsittelysopimukset voivat olla esimerkiksi henkilöihin liittyvien palvelujen ulkoistamissopimuksia, henkilöihin liittyvien palvelujen ostosopimuksia, tietojärjestelmiin liittyviä sopimuksia, tai suoria henkilötietojen käsittelysopimuksia toisen yrityksen kanssa.[227] Toisin sanoen, Tietojenkäsittelysopimukset voidaan toteuttaa erillisinä sopimuksina palvelun tarjoajan ja ulkoistavan yrityksen välillä tai erillisinä liitteinä laajemman sopimuskokonaisuuden yhteydessä, esimerkiksi palvelua koskevassa projektisopimuksessa[228].

4.2.2 Henkilötietojen käsittelijän valinta, valtuudet ja vastuu

Ulkoistaessa yrityksen henkilötietojen käsittelyn, 28.1 artiklan mukaan yrityksen tulee valita yhteistyökumppaneikseen ainoastaan sellaisia tahoja, jotka pystyvät huolehtimaan Rekisteröityjen oikeuksista ja joiden toiminta täyttää Asetuksen vaatimukset asianmukaisista teknisistä

[224] Kuten Tietosuojavaltuutettu 2.9.2019 antamassaan päätöksessään toteaa: *”Rekisterinpitäjän määrittelemiseksi on siten viranomaisten kohdalla arvioitava, millä taholla on kyseessä olevien palvelujen järjestämisvastuu. Se viranomainen, jolla on jonkin palvelun järjestämisvastuu, on myös tämän palvelun antamisen yhteydessä kerättyjen asiakastietojen Rekisterinpitäjä. Palvelunjärjestäjä Rekisterinpitäjänä voi joko itse tuottaa kyseessä olevan palvelun tai ostaa sen joltain ulkopuoliselta, kuten esim. kuntayhtymältä*.” Päätöstä tulkittaessa on huomattava, että Rekisterinpitäjän määritteleminen soveltuu samojen kriteerien perustella niin yksityiselle kuin julkisellekin sektorille. *Tietosuojavaltuutetun päätös* (*5036/183/2019*) 2019, kohta Tietosuojavaltuutetun vastaus.
[225] *Pitkänen* 2018, s. 293.
[226] *Pitkänen* 2018, s. 292–293.
[227] *Sulin – Tainio* 2017, s. 9–10.
[228] *Partanen* 2018, kohta Tietosuojasopimuksia on monenlaisia.

ja organisatorisista toimenpiteistä[229]. Jotta valinnasta voidaan varmistua, yrityksen on saatava Henkilötietojen käsittelijältä riittävät takeet sen Asetuksen vaatimukset täyttävistä toiminnoistaan. Henkilötietojen käsittelijän arviointi ja valinta on tärkeää myös yrityksen osoitusvelvollisuuden noudattamisen todistamiseksi. Yrityksen suorittaman arvioinnin ja valinnan tärkeys korostuu erityisesti ulkoistettaessa korkean riskin sisältävien henkilötietojen käsittely, kuten terveystietoja koskeva käsittely.[230] Asetuksen johdantolauseen (81) mukaan, kelpoisuuden osoittamiseksi, yrityksen tulisi saada näyttöä erityisesti Henkilötietojen käsittelijän asiantuntemuksesta, luotettavuudesta ja resursseista. Käytännössä Rekisterinpitäjä voi yrittää selvittää Henkilötietojen käsittelijän toimien lainmukaisuutta muun muassa ennakkokyselyn tai tarkastuksena avulla[231]. Asetuksen johdantolauseen (81) mukaan, myös noudattamalla *hyväksyttyjä käytännesääntöjä* tai *sertifiointimekanismeja*, Henkilötietojen käsittelijä voisi osoittaa kelpoisuutensa asiantuntevana ja luotettavana yhteistyökumppanina.[232]

Henkilötietojen käsittelijän oikeutta käyttää *alihankkijoita* sille annettujen velvollisuuksien toteuttamisessa on rajattu 28.2 artiklassa; toisen Henkilötietojen käsittelijän palveluksia ei voi hyödyntää ilman Rekisterinpitäjän antamaa erityistä tai yleistä kirjallista ennakkolupaa. Alihankkijoiden hyödyntämisestä on toisin sanoen sovittava päävastuullisena toimivan yrityksen eli Rekisterinpitäjän kanssa ja sisällytettävä sovittu linjaus Tietojenkäsittelysopimuksen ehtoihin. Jos henkilötietojen käsittely edellyttää uusien Henkilötietojen käsittelijöiden lisäämistä tai aikaisempien alihankkijoiden vaihtamista, tulee Henkilötietojen käsittelijän tiedottaa ja hyväksyttää tämä Rekisterinpitäjällä. Jotta Asetuksen lainmukaisuuden toteuttaminen on mahdollista, tulee Rekisterinpitäjällä olla tosiasialliset mahdollisuudet valvoa ja valita jokainen taho, joka sen alaisuudessa käsittelee sille kuuluvia henkilötietoja. Näin ollen lähtökohtainen *aliurakointikielto* mahdollistaa Rekisterinpitäjänä toimivan yrityksen omien vastuiden ja velvollisuuksien toteuttamisen pidättämällä kontrollin itsellään.

Henkilötietojen käsittelijän alihankita ei lähtökohtaisesti muuta tilannetta alkuperäisestä asetelmasta. Artiklan 28. 4 mukaisesti, alihankkijaan sovelletaan samoja velvoitteita kuin Henkilötietojen käsittelijän ja Rekisterinpitäjän välisessä Tietojenkäsittelysopimuksessa. Tämä ei

[229] Ks. Marriot International tapaus. Tapauksessa globaali hotelliketju laiminlöi riittävät toimet henkilötietojen turvaamiseksi, jonka seurauksena jopa 339 miljoonan asiakkaan henkilö- ja maksutiedot joutuivat tietomurron kohteeksi. ICO on esittänyt tapauksessa lähes 100 miljoonan punnan sakkoa. *ICO – Marriot* 2019.
[230] *Partanen* 2018, kohta Tietosuojasopimuksia on monenlaisia.
[231] *Lilja* 2019, s. 224.
[232] Hyväksytyistä käytännesäännöistä ja sertifiointimekanismeista jäljempänä tarkemmin vakiosopimuslausekkeiden yhteydessä kappaleessa 4.2.4. Sopimusneuvotteluissa hyödynnettävät mekanismit.

kuitenkaan siirrä Henkilötietojen käsittelijän vastuita alihankkijalle, vaan alihankkijan laiminlyödessä velvoitteensa ”alkuperäinen” Henkilötietojen käsittelijä vastaa täysimääräisesti alihankittavien velvoitteiden toteuttamisesta suhteessa Rekisterinpitäjään. Rekisterinpitäjän kontrollia ja alkuperäisen Tietojenkäsittelysopimuksen sisältämien velvoitteiden tärkeyttä korostaa edelleen Asetuksen artikla 29, jonka mukaan kaikkien henkilötietojen käsittelyyn osallistuvien tahojen on noudatettava Rekisterinpitäjänä toimivan yrityksen antamia ohjeistuksia. Ulkoistaminen tai alihankinta eivät toisin sanoen ole keinoja laistaa Asetuksen asettamista vastuista.

4.2.3 Tietojenkäsittelysopimuksen Asetuksen mukainen sisältö

Sen lisäksi, että Asetuksessa määrätään sopimaan kirjallisesti henkilötietojen käsittelystä, Asetus määrittelee minimisisällön kyseiselle sopimukselle. Asetuksen 28.3 artikla luettelee seikkaperäisesti asiat, jotka Tietojenkäsittelysopimuksen tulisi vähintäänkin sisältää. Käyttötarkoitussidonnaisuuden periaatetta mukaillen, osapuolten on solmittava sopimus, jossa vahvistetaan henkilötietojen käsittelyn kohde ja kesto, käsittelyn luonne ja tarkoitus, henkilötietojen tyyppi ja Rekisteröityjen ryhmät, sekä Rekisterinpitäjän velvollisuudet ja oikeudet. Tietojenkäsittelyn yksilöinnillä selkeytetään sopimuksen alaiset eli ulkoistettavat toimet (esimerkiksi palkanmaksu) ja rajataan ulkoistettavan käsittelyn kohteena olevat henkilöt (esimerkiksi työntekijät) ja tietoluokat (esimerkiksi työntekijöiden yhteystiedot)[233]. Myös Rekisterinpitäjän oikeuksien ja velvollisuuksien sisällyttäminen ja määrittäminen sopimukseen luo läpinäkyvyyttä ja selkiyttää osapuolten välisiä vastuita. IT2018 henkilötietojen käsittelyä koskevien erityisehtojen (jäljempänä ”*EHK-ehdot*”) mukaan, Rekisterinpitäjän oikeuksiin voi kuulua muun muassa kirjallisten ohjeiden antaminen (esimerkiksi Tietojenkäsittelysopimus liitteineen) ja velvollisuuksiin muun muassa Rekisterinpitäjän velvollisuus varmistaa oman käsittelynsä lainmukaisuus ennen tietojen luovuttamista Henkilötietojen käsittelijälle.[234]

Tietojenkäsittelysopimuksen tulee lisäksi sisältää seuraavat asiakokonaisuudet:

(i) Henkilötietojen käsittelijän tulee sitoutua noudattamaan henkilötietojen käsittelyssä ainoastaan Rekisterinpitäjän antamia ohjeita ja laadittuja sopimusehtoja (artikla 28.3(a)). Rekis-

[233] Ks. *Partanen* 2018, kohta Henkilötietojen käsittelystä on tehtävä sopimus.
[234] *Lilja* 2019, s. 219–220.

terinpitäjällä on näin ollen myös määräysvalta valita antaako se luvan henkilötietojen siirroille EU:n tai Euroopan talousalueen (ETA) ulkopuolelle[235];

(ii) Henkilötietojen käsittelijän on varmistettava ja huolehdittava, että kaikki henkilötietojen käsittelyyn osallistuvat ovat sitoutuneet salassapitovelvollisuuteen, kuten omat työntekijät (artikla 28.3(b));

(iii) Henkilötietojen käsittelyssä on toteutettava riittävät tekniset ja organisatoriset toimenpiteet, jotta saavutetaan tarvittava turvallisuustaso. Asetuksen 32 artiklan mukaan toteutettaessa asianmukaisia teknisiä ja organisatorisia toimenpiteitä, tulee käsittelijän huomioida uusin tekniikka ja siitä aiheutuvat toteuttamiskustannukset, käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat riskit. Tarkoittaen, että toteutettavat toimet tulee suhteuttaa olemassa oleviin riskeihin[236]. Joten riskien korostuessa, käsiteltäessä esimerkiksi erityisiä tietoryhmiä, kuten terveystietoja, tietoturvan tasoa on nostettava (artiklat 28.3(c) ja 32). Artiklan 32.1 mukaisina toimenpiteinä esitetään muun muassa henkilötietojen pseudonymisointi ja salaus, tietojärjestelmien vikasietoisuuden huomioiminen, kyky tietojen palauttamiseen teknisten ongelmien sattuessa, sekä tietojenkäsittelyn turvallisuuden säännöllinen testaaminen. Käytännössä toimet voivat olla muun muassa tietokoneiden virustorjuntaa, palomuureja, kulunvalvontaa, käyttöoikeuksien rajaamista tai resurssien lisäämistä[237];

(iv) Henkilötietojen käsittelijän on sitouduttava noudattamaan, mitä alihankkijoiden käyttämisestä on sovittu. Tietojenkäsittelysopimuksessa tulee sopia toisen Henkilötietojen käsittelijän käytön edellytyksistä. Käytännössä osapuolet sopivat tarvitseeko Rekisterinpitäjältä pyytää erillinen suostumus alihankintaa varten vai riittääkö, että Henkilötietojen käsittelijä ilmoittaa asiasta jälkikäteen, jolloin Rekisterinpitäjän mahdollisuus vastustaa alihankintaa on myös jälkikäteinen (artikla 28.3(d));

(v) Henkilötietojen käsittelijän avustamis- ja tiedonantovelvollisuuden sisältö on kirjattava sopimukseen (artikla 28.3(e-f)). Avustaminen ja tietojen saattaminen Rekisterinpitäjälle mah-

[235] Vrt. EHK-ehdot, joissa Henkilötietojen käsittelijälle on haluttu antaa lähtökohtainen oikeus siirtää henkilötietoja EU:n tai ETA alueen ulkopuolelle, ellei toisin sovita. *Lilja* 2019, s. 22.
[236] Artiklan 32.2 mukaan turvallisuustason arvioinnissa käsittelyn sisältämiä riskejä tulee arvioida erityisesti siirrettyjen, tallennettujen tai muutoin käsiteltyjen henkilötietojen vahingossa tapahtuvan tai laittoman tuhoamisen, häviämisen, muuttamisen, luvattoman luovuttamisen tai henkilötietoihin pääsyn vuoksi.
[237] Ks. *Partanen* 2018, kohta Henkilötietojen käsittelystä on tehtävä sopimus.

dollistaa Rekisterinpitäjän omien velvollisuuksien toteuttamisen, kuten velvollisuuden vastata Rekisteröityjen tietopyyntöihin;

(vi) Tietojenkäsittelysopimuksen päätyttyä Henkilötietietojen käsittelijän on, Rekisterinpitäjän valinnasta riippuen, joko poistettava tai palautettava kaikki sillä olevat henkilötiedot Rekisterinpitäjälle, myös säilössä olevat varmuuskopiot. Poikkeuksena mainittakoon tilanteet, joissa Henkilötietojen käsittelijää vaaditaan 28.3 artiklan (g) alakohdan mukaisesti säilyttämään henkilötiedot unionin oikeuden tai kansallisen lainsäädännön nojalla. Rekisterinpitäjän päätäntävaltaa korostaen ja sillä olevien velvollisuuksien toteuttamisen suojaamiseksi, EHK-ehtoihin on lisätty vaatimus, ettei Henkilötietojen käsittelijä saa myöskään poistaa käsittelemiään henkilötietoja sopimuksen voimassaoloaikana[238];

(vii) Rekisterinpitäjän *auditointioikeus* on sisällytettävä sopimukseen. Rekisterinpitäjän tulee saada tehdä auditointeja tai valtuuttaa ulkopuolisen auditoijan tekemään ja osallistumaan auditointeihin (artikla 28.3(h)). Auditoinneilla edesautetaan ja varmistetaan Rekisterinpitäjän tosiasiallinen mahdollisuus puuttua ja valvoa oman ja yhteistyökumppaneidensa Asetuksen lainmukaista noudattamista osana osoitusvelvollisuutensa toteuttamista.

4.2.4 Muut Tietojenkäsittelysopimukseen suositeltavat asiat

Artiklan 28 sisältämät velvoitteet Tietojenkäsittelysopimuksen sisällöstä eivät tarjoa tyhjentävää listausta sen sisällöstä, vaan määräävät sopimuksen vähimmäissisällön siinä huomioitavista seikoista ja toimista. Sopimuksen laadun parantamiseksi voi olla perusteltua sopia laajemmin myös muista asioista.[239] Sopimukseen voi olla tarvetta lisätä muun muassa tarkennuksia kuinka nopeasti tietovuodoista on ilmoitettava Rekisterinpitäjälle, miten osapuolten vahingonkorvausvelvollisuus jakaantuu, korvataanko Henkilötietojen käsittelijälle Rekisterinpitäjän avustamisesta aiheutuvat kulut, sekä selkeät linjaukset sovituista vastuunrajoituksista[240]. Rekisterinpitäjällä voi olla myös laillinen oikeus vaatia turvallisuusselvityksiä[241]. Tietoturvan

[238] *Lilja* 2019, s. 230.
[239] Esim. tilanteet joissa henkilötietojen käsittely on osa laajempaa sopimuskokonaisuutta, jolloin Tietojenkäsittelysopimuksen ehdot on tärkeää sisällyttää palvelu- tai pääsopimukseen tai lisätä ainakin viittaus mainittuihin sopimuksiin. Sopimuskokonaisuus voikin sisältää Tietojenkäsittelysopimuksen lisäksi huomattavan määrän tarpeellisia liitteitä kuten tuote – ja palvelukuvauksen, tuki- ja ylläpitosopimuksen, ja takuuehdot (tässä mainittuna vain muutama). Ks. kattavampi listaus mahdollisista liitetiedostoista ja Tietojenkäsittelysopimuksista *Turunen – Lilja* 2019, s. 45–48 ja 213–232.
[240] Ks. *Partanen* 2018, kohta Tietosuojasopimuksia on monenlaisia.
[241] Ks. S*uojelupoliisi* 2019, kohta Turvallisuusselvitys on ennaltaehkäisevää turvallisuustyötä; Ks. myös Turvallisuusselvityslaki (726/2014).

toteutumisen varmistamiseksi, osapuolet voivatkin sopia turvallisuusselvitysten hyödyntämistä, jolloin henkilötietoja saisi käsitellä vain henkilöt, jotka ovat suorittaneet hyväksytysti turvallisuusselvityksen. Valtiovarainministeriön vahtiohjeiden mukaan Tietojenkäsittelysopimuksessa olisi myös suositeltavaa sopia Henkilötietojen käsittelijän palvelun laadun seurannasta. Laadun seuranta voisi olla mahdollista esimerkiksi Henkilötietojen käsittelijän tietosuojan ja tietoturvan tason säännöllisellä raportoinnilla ja säännöllisillä tapaamisilla.[242]

Artiklan 28.3 alakohta (a) mainitsee myös henkilötietojen siirrot kolmansiin maihin antamatta asiasta sen tarkempia määräyksiä.[243] Säännöksen mukaan Henkilötietojen käsittelijän on noudatettava sille annettuja dokumentoituja ohjeistuksia. Jos siirtoja kolmansiin maihin ei käsitellä sopimuksessa, henkilötietojen siirto ja käsittely kolmansissa maissa on lähtökohtaisesti kiellettyä artiklan 44 mukaisesti. Siirrot kolmansiin maihin ovat kuitenkin yleisiä, sillä IT-palvelut sisältävät usein pilvipalveluita tai etätukea, joiden tuotanto toteutetaan käytännössä globaaleissa verkostoissa[244]. Tästä johtuen, sekä EHK-ehtoja mukaillen, yritysten olisikin hyvä huomioida Tietojenkäsittelysopimuksissaan henkilötietojen siirtomahdollisuus myös kolmansiin maihin. Jos henkilötietojen käsittely sallitaan kolmansissa maissa, tulee sopimuskumppaneiden varmistaa, että tietojen siirto ja käsittely täyttävät Asetuksen nimenomaiset velvoitteet koskien artikloja 44–49. Tästä syystä Tietojenkäsittelysopimukseen olisi tärkeää sisällyttää muun muassa ehto, joka mahdollistaa Rekisterinpitäjän seurannan henkilötietojen käsittelyn sijainnista[245]. Rekisterinpitäjän seurannan mahdollistaminen on tärkeä osa sille kuuluvaa tiedonanto- ja osoitusvelvollisuutta. Yritys voi myös tietoisesti pyrkiä valitsemaan sopimuskumppaneita, joiden henkilötietojen käsittely ja siirrot tapahtuvat valtioissa, joiden osalta komissio on antanut artiklan 45 mukaisen päätöksen tietosuojan riittävyydestä.[246] Jos mainittua päätöstä ei ole kyseessä olevan valtion osalta tehty, sopimuskumppanit voivat toteuttaa siirrot hyödyntäen artiklan 46 sisältämiä asianmukaisia *suojatoimia* osana heidän välistä Tietojenkäsittelysopimusta. Asianmukaisia suojatoimia ovat: (i) komission tai tietosuojaviran-

[242] Ks. *Pietikäinen* 2016, kohta 5.8 Rekisterinpitäjän ja käsittelijän väliset sopimukset.
[243] Kolmansilla mailla tarkoitetaan EU tai ETA maihin kuulumattomia valtioita. Ks. EU ja ETA maat listattuna *Suomen tulli* 2019, kohta EU-, Eta-, Efta- ja Schengen-maat.
[244] *Lilja* 2019, s. 227.
[245] esim. EHK-ehdot kohta 6.1:ssä: ”*…Asiakkaalla on oikeus milloin tahansa saada toimittajalta tiedot henkilötietojen käsittelyn sijainnista.*” *Lilja* 2019, s. 227.
[246] Komissio on tunnustanut päätöksellään tietosuojan tason riittävyyden seuraavien maiden kohdalla: Andorra, Argentiina, Kanada (kaupalliset organisaatiot), Färsaaret, Guernsey, Israel, Mansaari, Japani, Jersey, Uusi-Seelanti, Sveitsi, Uruguay ja Amerikan yhdysvallat (*Privacy Shield – järjestelyn* tuomin rajoituksin). *Euroopan komission päätös tietosuojan tason riittävyydestä* 2019; Ks. myös tietosuojan tason riittävyyttä koskevien päätösten eduista kansainvälisessä kaupassa *Oikeusministeriön perusmuistio (OM2018-00505)* 2018, s. 3 ja 5.

omaisen hyväksymät vakiosopimuslausekkeet, (ii) yrityksiä koskevat hyväksytyt sitovat säännöt[247], (iii) hyväksytyt käytännesäännöt, tai (iv) hyväksytyt sertifiointimekanismit.[248]

Sopimuksen laadinnassa on lisäksi huomioitava tilanteet, joissa osapuolten roolit poikkeavat edellä kuvatusta olettamasta, jolloin toinen toimii Rekisterinpitäjänä ja toinen Henkilötietojen käsittelijänä. Kuten aikaisemmassa luvussa 3 mainittiin, on myös mahdollista, että molemmat toimivat Rekisterinpitäjinä ja/tai Henkilötietojen käsittelijöinä, joko osittain tai yhteisrekisterinpitäjinä. Tietojenkäsittelysopimus on siten laadittava aina tapauskohtaisesti, tosiasiallisen tilanteen mukaisesti, sekä kokonaiskuva huomioiden.[249]

4.2.5 Sopimusneuvotteluissa hyödynnettävät mekanismit

Asetus tarjoaa erilaisia työkaluja, joiden avulla yritykset pystyvät osoittamaan noudattavansa Asetuksen vaatimuksia ja joiden avulla ne voivat muun muassa pyrkiä antamaan itsestään luotettavan kuvan markkinoilla. Yritys voi esimerkiksi hyödyntää laadittuja käytännesääntöjä tai käyttää sertifiointijärjestelmiä osoittaakseen muille yrityksille ja yksityishenkilöille noudattavansa tietosuojaperiaatteita. Näiden lisäksi Asetus mahdollistaa vakiosopimuslausekkeiden hyödyntämisen Rekisterinpitäjän ja Henkilötietojen käsittelijän sopimusneuvotteluiden tukena. Seuraavaksi hieman tarkemmin, mistä Asetuksen mahdollistavissa mekanismeissa on kyse.

4.2.4.1 Vakiosopimuslausekkeet

Tietojenkäsittelysopimus voi 28.6 artiklan mukaisesti koostua kokonaan tai osaksi vakiosopimuslausekkeista[250]. Tarkoittaen lisäksi sitä, että Henkilötietojen käsittelijän hyödyntäessä alihankkijoita, myös heidän välinen sopimus olisi mahdollista toteuttaa samoja vakiosopimuslausekkeita hyödyntäen, kunhan niissä toteutuu Rekisterinpitäjän antamat alkuperäiset velvoitteet Henkilötietojen käsittelijälle. Vakiosopimuslausekkeiden hyödyntäminen on myös

[247] kyseisiä artiklan 47 mukaisia niin sanottuja ”*binding corporation rules*”, ei tulla käsittelemään työssä tämän enempää.
[248] EU:n ja ETA-alueen ulkopuolella tapahtuvan henkilötietojen käsittelyn sopimukseen sisällyttämisen tärkeyttä korostaa IT2018-Käytännön käsikirjassa mainittu tarkennus `henkilötietojen siirron´ Asetuksen mukaisesta määrittelystä: *”Henkilötietojen siirtona pidetään Asetuksen nojalla tietojen fyysisen siirtämisen ja lähettämisen lisäksi myös esimerkiksi sitä, että EU:n/ETA-alueen ulkopuoliselle vastaanottajalle annetaan pääsy EU:ssa sijaitsevan Rekisteripitäjäntietokantaan ja sitä, että henkilötietoja julkaistaan internetissä. Siirtäminen EU:n / ETA-alueen ulkopuolelle ei edellytä siirtoa kolmannelle taholle, vaan henkilötietojen siirtoa koskeva sääntely soveltuu silloinkin, kun tiedot siirretään käsittelijän omalle palvelimelle EU:n / ETA-alueen ulkopuolelle.” Lilja* 2019, s. 226.
[249] *Lilja* 2019, s. 214.
[250] Vrt. henkilötietodirektiivin aikaiset mallisopimuslausekkeet. Ks. *Euroopan komissio (SCC)* 2019.

keino suojata henkilötietojen turvallinen käsittely kolmansiin maihin sijoittautuneiden sopimuskumppaneiden kanssa. Vakiosopimuslausekkeiden avulla yritys voi pyrkiä varmistamaan henkilötietojen turvallisen siirron mainittuihin kolmansiin maihin.[251] Vakiosopimuslausekkeet voi laatia ja hyväksyä komissio noudattaen mitä tarkastelumenettelystä säädetään, tai kansallinen valvontaviranomainen hyödyntäen *yhdenmukaisuusmekanismia*.

Komissio voi laatia artiklan 28.7 mukaan vakiosopimuslausekkeita noudattaen artiklan 93.2 mukaista *komitea- eli tarkastelumenettelyä*. Tarkastelumenettelystä säädetään yleisistä säännöistä ja periaatteista annetun asetuksen (EU 182/2011) 5 artiklassa. Asetuksella komissiolle siirretty täytäntöönpanovalta mahdollistaa unionin Asetuksen yhdenmukaisen täytäntöönpanon valvonnan.[252] Komission apuna Asetuksen täytäntöönpanossa toimii erillinen komitea. Vakiosopimuslausekkeiden lisäksi, tarkastelumenettelyä sovelletaan myös artiklan 40 säätämien käytännesääntöjen hyväksymisessä sekä artiklan 43 mukaisten sertifiointimekanismien, tietosuojasinettien ja – merkkien tunnustamisessa.[253] *Pitkänen* tiivistää menettelyprosessin vaiheet selkeästi ymmärrettävään muotoon:

> *”Tarkastelumenettelyssä komitea antaa lausuntonsa Euroopan unionista tehdyn sopimuksen (SEU)[254] 16 artiklan 4 ja 5 kohdassa ja soveltuvissa tapauksissa Euroopan unionin toiminnasta tehdyn sopimuksen (SEUT) 238.3 artiklassa määrätyllä enemmistöllä, kun on kyse säädöksistä, jotka hyväksytään komission ehdotuksesta. Jos komitea antaa puoltavan lausunnon, komissio hyväksyy ehdotuksen täytäntöönpanosäädökseksi. Jos taas komitea antaa kielteisen lausunnon, komissio ei lähtökohtaisesti hyväksy ehdotusta. Sen sijaan, jos täytäntöönpanosäädös katsotaan tarpeelliseksi, puheenjohtaja voi joko toimittaa muutetun ehdotuksen uudelleen komitealle kahden kuukauden kuluessa tai toimittaa ehdotuksen täytäntöönpanosäädökseksi muutoksenhakukomitean käsiteltäväksi kuukauden kuluessa lausunnon antamisesta. Jos lausuntoa ei anneta, komissio voi yleensä yksinkertaisella ääntenenemmistöllä hyväksyä ehdotuksen. Jos komissio ei hyväksy ehdotusta, puheenjohtaja voi esittää komitealle sitä koskevan muutetun ehdotuksen. Komissio neuvottelee jäsenvaltioiden kanssa. Aikaisintaan 14 päivän ja viimeistään kuukauden*

[251] Ks. esimerkinomainen listaus asianmukaisista suojatoimista kolmansiin maihin, joiden osalta komissio ei ole tehnyt päätöstä tietosuojan riittävyydestä *Euroopan komission suojatoimet* 2019, kohta Vastaus.
[252] Ks. Euroopan komission täytäntöönpanovallasta Asetuksen johdantolause 167.
[253] Tarkastelumenettelyn keskeinen asema Asetuksen säännösten täytäntöönpanossa ilmenee tiivistettynä johdantolauseessa 168, jossa listataan määräykset ja toimet, joihin kyseistä menettelyä sovelletaan.
[254] Sopimus Euroopan unionista, tehty 13 päivänä joulukuuta 2007 (Konsolidoitu toisinto 2016; *EUVL C 202, 7.6.2016, s. 13–388*).

kuluttua komitean kokouksesta komissio ilmoittaa komitean jäsenille neuvottelujen tuloksista ja toimittaa ehdotuksen täytäntöönpanosäädökseksi muutoksenhakukomitean käsiteltäväksi."[255]

Myös kansallinen valvontaviranomainen voi hyväksyä vakiosopimuslausekkeita artiklan 28.8 mukaan. Komission tarkastelumenettelystä poiketen, Kansallisen valvontaviranomaisen hyväksyntä noudattaa artiklan 63 mukaista yhdenmukaisuusmekanismia. Yhdenmukaisuusmekanismin tarkoituksena on varmistaa Asetuksen johdonmukainen ja yhdenmukainen soveltaminen kaikissa jäsenmaissa. Yhdenmukaisuusmekanismin määräyksen myötä vahvistetaan jäsenmaiden valvontaviranomaisten välistä yhteistyötä. Yhteistyön avulla turvataan Asetuksen yhtenäinen tulkinta. Yhdenmukaisuusmekanismi tulee sovellettavaksi, kun valvontaviranomaisen tarkoituksena on hyväksyä käsittelytoimia sisältäviä toimenpiteitä, joilla on olennaisia oikeusvaikutuksia merkittävälle Rekisteröityjen joukolle useassa eri jäsenmaassa. Asetuksen johdantolauseen (135) mukaan, yhdenmukaisuusmekanismia sovelletaan myös jos valvontaviranomainen tai komissio pyytää asian käsittelyä mekanismin mukaisesti. *Warma-Lehtinen* havainnollistaa yhdenmukaisuusmekanismin soveltamista käytäntöön:

"Käytännössä yhdenmukaisuusmekanismilla tarkoitetaan tilannetta, jossa asian käsittelyä johtaa johtava valvontaviranomainen, jonka tehtävänä on pyrkiä löytämään käsillä olevaan asiaan konsensus. Jos valvontaviranomaiset eivät löydä yhteistä näkemystä asiaan johtavan valvontaviranomaisen johdolla, siirtyy asia yhdenmukaisuusmekanismin puitteissa Euroopan tietosuojaneuvoston käsiteltäväksi. Euroopan tietosuojaneuvosto voi antaa kannanoton käsiteltävään asiaan tai valvontaviranomaisten ollessa erimielisiä se voi antaa sitovan päätöksen. Johtavan valvontaviranomaisen tehtävänä on toimia käsiteltävän asian yhteys-tahona kaikille osapuolille, sekä asianosaisille rekisterinpitäjille ja käsittelijöille, mutta myös muille valvontaviranomaisille. Johtavan valvontaviranomaisen tehtävänä on myös laatia päätös-ehdotus asiaan. Päätösehdotus on lähetettävä kaikille asiassa mukana oleville valvontaviranomaisille, jotka voivat kommentoida tai vastustaa päätösehdotuksen sisältöä. Mikäli johtava valvontaviranomainen päättää muuttaa päätösehdotuksen sisältöä kommenttien perusteella, se tulee laittaa tiedoksi muille käsittelyyn osallistuville valvontaviranomaisille. Tämän jälkeen johtava valvontaviranomainen voi päättää ehdotusten hyväksymisestä tai hylkäämisestä. Jos johtava valvontaviranomainen ei muuta ratkaisuehdotustaan vastustavien kommenttien sisältöiseksi, siirtyy asia Euroopan tietosuojaneuvoston kiistanratkaisumenettelyyn Asetuksen 65 artiklan mukaisesti, jonka lopputu-

[255] *Pitkänen* 2018, s. 631.

loksena asiaan annetaan sitova päätös, jonka mukaisesti johtava valvontaviranomainen tekee asiassa päätöksen.”[256]

4.2.4.2 Käytännesäännöt

Artiklassa 28.5 viitatuilla hyväksytyillä käytännesäännöillä tarkoitetaan toimialakohtaisesti annettuja ohjeita tietosuojasääntelyn soveltamisesta. Tarkoittaen, että yritys voi halutessaan ottaa käyttöönsä valitsemansa elinkeinoyhdistyksen julkaisemat käytännesäännöt. Käytännesääntöjen laatiminen ja noudattaminen on vapaaehtoista[257], kuten hallituksen esityksessä asia ilmaistaan: ”*käytännesäännöt ovat Rekisterinpitäjälle mahdollisuus, ei velvollisuus*”[258]. Käytännesäännöt ovat siis suositus, jolla helpotetaan Rekisterinpitäjän ja Henkilötietojen käsittelijän työtä, heidän arvioidessaan niin oman yrityksen kuin myös toisten organisaatioiden henkilötietojen käsittelyn lainmukaisuutta. Käytännesäännöistä säädetään tarkemmin Asetuksen artiklassa 40. EDPB on antanut käytännesääntöjä koskevat uudet ohjeistukset, joiden tarkoituksena on selkeyttää niiden vaatimuksia, sisältöä, hyväksymistä, julkaisemista ja valvontaa[259].[260] Vapaaehtoisten käytännesääntöjen suurimpana hyötynä yritysten näkökulmasta on niiden toimiala- ja intressikohtainen fokus[261]. Toimialakohtaisilla käytännesäännöillä pystytään huomioimaan kulloinkin kyseeseen tulevat tarpeet, erityspiirteet ja täsmentämään Asetuksen säännöksiä, mitkä saattavat olla monelle yritykselle vielä osin epäselviä.[262]

Käytännesääntöjen olemassaolo sinänsä ei ole suora osoitus Asetuksen mukaisesta toiminnasta tai takaa yksinään Asetuksen noudattamista[263], mutta yritykset voisivat parhaimmillaan saavuttaa sen avulla kilpailuetua muihin saman sektorin toimijoihin nähden, jotka eivät hyödynnä käytännesääntöjä. Yritykset voivat halutessaan myös edellyttää palveluntuottajiltaan tiettyjen käytännesääntöjen noudattamista. Hyväksytyistä käytännesäännöistä hyötynevät eri-

[256] *Warma-Lehtinen* 2018, s. 476–477.
[257] *Warma-Lehtinen* 2018, s. 373.
[258] *HE 9/2018 vp*, s. 109.
[259] Ks. *EDPB Guidelines (1/2019)* 2019.
[260] Vrt. ”*Käytännesääntöjä kritisoivat tahot ovat nostaneet esiin kysymyksen toimialaa ohjaavista toimintatavoista, minkä seurauksena on pahimmillaan yhdenmukaisten käytäntöjen muotoutuminen, mikä samalla voisi estää tai hidastaa omien, organisaatiokohtaisten parhaiden käytäntöjen suunnittelua. Tämänkaltainen toimintamalli ei ole yhdenmukainen asetuksen tavoitteiden, kuten Privacy by Design -periaatten kanssa. Tämä on käytännesääntöjen laatimisen ytimeen pureutuva ongelma – jos käytännesäännöt ovat hyvin yleiset ja sisällöltään suppeat, ne eivät tarjoa riittävää toimialakohtaista tukea ja tulkintaa tärkeisiin henkilötietojen käsittelyä koskeviin kysymyksiin. Jos taas käytännesäännöt ovat kovinkin yksityiskohtaiset, ei rekisterinpitäjän tai käsittelijän käsittelytoimien omalle suunnittelulle välttämättä jää kaikissa tilanteissa riittävästi tilaa.” Warma-Lehtinen* 2018, s. 376–377.
[261] esimerkkinä finanssialan laatimat käytännesäännöt. Ks. *Finanssiala* 2017.
[262] *Warma-Lehtinen* 2018, s. 373–376.
[263] Ks. *EDPB Guidelines (1/2019)* 2019, s. 8.

tyisesti Henkilötietojen käsittelijät, jotka tavoittelevat asiakkaikseen korkeariskisen alan yrityksiä – joiden liiketoiminnan elinehtona on Rekisteröityjen oikeuksien turvaaminen.[264] Rekisterinpitäjät voivat toisin sanoen nähdä käytännesääntöjen noudattamisen pienentävän heihin kohdistuvia riskejä valitessaan palveluntuottajia henkilötietojensa käsittelyä varten.[265] Luonnollisesti, myös Henkilötietojen käsittelijä voi katsoa käytännesääntöjen noudattamisen eduksi valitessaan alihankkijoitaan. Yritykset voivat hyötyä käytännesääntöjen hyödyntämisestä myös toimiessaan kansainvälisillä markkinoilla, kolmansiin maihin sijoittautuneiden yritysten kanssa. Hyväksyttyihin käytännesääntöihin sitoutunut unionin ulkopuolelle sijoittautunut yritys, vakuuttaa paremmin käyttävänsä asianmukaisia suojatoimia siirrettyjen tietojen suojaamiseksi.[266]

Vapaaehtoisuudestaan huolimatta, käytännesääntöjen noudattamista valvotaan. Valvojana toimii erillinen toimielin, joka valvoo, että yritykset noudattavat valitsemiaan käytännesääntöjä. Toimielimen tehtävänä on toimia kansallisen valvontaviranomaisen rinnalla, kuitenkaan rajoittamatta valvontaviranomaisen toimenkuvaa tai sille kuuluvia valtuuksia. Toimielimeltä vaadittavista edellytyksistä säädetään tarkemmin Asetuksen artiklassa 41.2.[267] Sen lisäksi, että käytännesäännöt voivat helpottaa Asetuksen velvoitteiden ymmärtämistä ja käytännönsoveltamista, niiden noudattaminen voi osoittautua yritykselle eduksi mahdollisen tietoturvaloukkauksen selvittämisessä. Jos yritys pystyy osoittamaan noudattaneensa hyväksyttyjä käytännesääntöjä, vaikuttanee se tapauksen kokonaisharkinnan arviointiin seuraamuksia pienentävänä tai poistavana tekijänä.[268]

Valitettavasti viranomaiset eivät kuitenkaan ole vielä hyväksyneet tai julkaisseet, yritysten arviointia ja valintaa helpottavia, hyväksyttyjä käytännesääntöjä. Asetus pyrkii johdantolauseiden (98 ja 99) mukaisesti, kannustamaan yrityksiä, niiden edustajia ja sidosryhmiä aloittamaan käytännesääntöjen valmistelun. Nyt kun EDPB on julkaissut ohjeistukset koskien käytännesääntöjä, jää nähtäväksi aktivoituvatko eri toimialojen edustajat. Kynnys saattaa yrityksen käytännesäännöt viranomaiselle artiklan 40.5 mukaisesti vahvistettavaksi voisi tosin olla matalampi, jos sääntöjen valmistelu- ja hyväksyntäprosessi olisi kevyempi. *Warma-Lehtinen* toteaakin kirjoituksessaan, että käytännesääntöjen valmistelu nähdään usein kovin työlääksi,

[264] Ks. *i-SCOOP* 2019, kohta What must be in an (approved) code of conduct under the GDPR?
[265] *Warma-Lehtinen* 2018, s. 372.
[266] Ks. *Euroopan komission suojatoimet* 2019, kohta Vastaus.
[267] *Warma-Lehtinen* 2018, s. 372–373.
[268] *Warma-Lehtinen* 2018, s. 373–376.

eikä vielä ole julkaistu viranomaiskäytäntöä tai ohjeita, jotka voisivat helpottaa valmistelun toteuttamista[269]. Kannanotto on ymmärrettävä perehdyttäessä prosessin eri vaiheisiin; ensi on selvitettävä ja linjattava kyseessä olevan toimialan erityispiirteet jäsenkunnan kesken, varmistettava, että tehdyt linjaukset ja sisältö kokonaisuudessaan täyttävät Asetuksen vaatimukset, tämän jälkeen käytännesäännöt luovutetaan lausuntoa ja hyväksyntää varten toimivaltaiselle valvontaviranomaiselle, jonka jälkeen ne rekisteröidään ja julkaistaan. Jos käytännesääntöjen käsittelytoimet sisältävät liittymiä useampaan EU jäsenmaahan, tulee valvontaviranomaisen luovuttaa ne edelleen EDPB:lle lausuntoa varten artiklan 63 yhdenmukaisuusmekanismia noudattaen, EDPB luovuttaa puoltavan lausuntonsa komissiolle, joka voi vielä täydentää käytännesääntöjä antamalla erityisiä täytäntöönpanosäädöksiä edelleen hyväksyttäväksi artiklan 93 mukaiselle komitea- eli tarkastelumenettelylle, lopuksi komissio julkaisee hyväksytyt käytännesäännöt, ja luovuttaa ne EDPB:lle julkaistavaksi julkiseen tietokantaan.[270]

4.2.4.3 Sertifiointimekanismit

Käytännesääntöjen sijaan tai rinnalla, yritys voi myös päättää hyödyntää artiklan 42 mukaista sertifiointijärjestelmää. EDPB on laatinut sertifiointeja koskevan ohjeistuksen, jossa selvennetään Asetuksen mukaisen sertifioinnin hyödyntämismahdollisuuksia ja kriteereitä.[271] Sertifioinnin avulla yritykset voivat osoittaa noudattavansa Asetuksen määräyksiä henkilötietojen käsittelyssä, helpottaen näin sopimuskumppaneiden valintaa ja osoittaen noudattavansa 28 artiklan kohtia 1 ja 4. Sertifiointimekanismin käyttöönottoa sekä tietosuojasinettien ja –merkkien hyödyntämistä kehotetaan hyödynnettävän myös Asetuksen johdantolauseissa. Asetuksen johdantolauseen (100) mukaan, mekanismit toisivat markkinoille läpinäkyvyyttä ja helpottaisivat henkilötietojen käsittelyä koskevien tuotteiden, palveluiden ja järjestelmien arviointia.[272] Sertifioinnin edellyttämät toimintatavat ovat kaikille yrityksille vapaaehtoisia ja kukin yritys voi ottaa niissä mainitut toimintamallit halutessaan käyttöönsä. Edellä mainitut sinetit ja merkit toimisivat hyväksytyn sertifioinnin osoittamisessa[273]. Yrityksen on mahdollista hyödyntää sertifiointia myös toimiessaan kansainvälisillä markkinoilla, kolmansiin maihin sijoittautuneiden yritysten kanssa. Sertifioinnin avulla yritys voi helpommin luottaa siihen,

[269] *Warma-Lehtinen* 2018, s. 375.
[270] *Warma-Lehtinen* 2018, s. 375–376.
[271] Ks. *EDPB Guidelines (1/2018)* 2019, s. 6.
[272] Vrt. sertifikaattien kohtaama kritiikki, jonka mukaan sertifikaattien hyöty on rajallinen sen vahvistaessa vain tietyt Asetuksenmukaiset toimet – ei koko tietosuojasääntelyn noudattamista. Ks. *Warma-Lehtinen* 2018, s. 383.
[273] *Warma-Lehtinen* 2018, s. 382–386.

että unionin ulkopuolelle sijoittautunut Henkilötietojen käsittelijä käyttää asianmukaisia suojatoimia siirrettyjen tietojen suojaamiseksi.[274]

Asetuksen 43 artiklan mukaan, sertifikaatin voi laatia ja hyväksyä riippumaton sertifiointielin, toimivaltainen valvontaviranomainen tai vaihtoehtoisesti sertifikaatti voidaan saattaa voimaan EDPB:n omien sekä jäsenmaakohtaisesti hyväksyttyjen kriteereiden perusteella.[275] EDPB:n kriteereiden hyödyntäminen 42.5 artiklan mukaisesti mahdollistaa koko unionin kattavan eurooppalaisen tietosuojasinetin myöntämisen.[276] Kansallisen sertifiointielimen akkreditoi Suomessa riittävän asiantuntemuksen omaava tietosuojavaltuutettu.[277] Sertifiointi myönnetään 43.7 artiklan mukaan kerralla enintään kolmeksi vuodeksi, ja se on mahdollista uusia tai peruuttaa riippuen täyttääkö kyseessä oleva yritys sertifikaatin myöntämisen edellytykset. Kansallisen sertifiointielimen akkreditointiin liittyvät vaatimukset, kansalliseen sertifikaattiin ja eurooppalaiseen tietosuojasinettiin vaadittavat kriteerit kootaan sekä julkaistaan kaikille nähtäväksi niiden ollessa valmiit hyödynnettäväksi.[278] Jotta sertifikaattien edellytykset, toimintatavat ja taso olisivat unionissa yhtenäiset, valvontaviranomaisen on hyväksytettävä sertifikaattien sisältö ja kohde EDPB:lla.[279] Lisäksi, artiklan 43.9 mukaan komissio voi tarkastelumenettelyä noudattaen hyväksyä täytäntöönpanosäädöksiä, joilla vahvistetaan tekniset standardit sertifiointimekanismeja, tietosuojasinettejä ja -merkkejä varten sekä menettelyt mainittujen sertifiointimekanismien edistämiseksi ja tunnustamiseksi.

4.2.6 Henkilötietojen käsittelijän rikkomukset ja laiminlyönnit

Asetuksen artiklan 82.1 perustuen *”jos henkilölle aiheutuu -- asetuksen rikkomisesta aineellista tai aineetonta vahinkoa, hänellä on oikeus saada Rekisterinpitäjältä tai Henkilötietojen käsittelijältä korvaus aiheutuneesta vahingosta”*. Yksityisillä henkilöillä on siis oikeus saada kärsimästään vahingosta täysimääräinen korvaus henkilötietojen käsittelyyn osallistuneilta tahoilta. Henkilötietojen käsittelijä on kuitenkin vastuussa käsittelystä aiheutuneesta vahingosta vain, jos se ei ole noudattanut nimenomaisesti sille osoitettuja Asetuksen velvoitteita tai se on toiminut vastoin Rekisterinpitäjänä toimivan yrityksen ohjeistuksia artiklan 82.2 mukai-

[274] Ks. *Euroopan komission suojatoimet* 2019, kohta Vastaus.
[275] Ks. tarkemmin EDPB:n näkemykset sertifioinnin läpinäkyvyydestä *EDPB Guidelines (1/2018*) 2019, s. 7–8.
[276] Ks. tarkemmin *EDPB Guidelines (1/2018)* 2019, luku 4 ja s. 12–14.
[277] Tietosuojavaltuutetun valinta asiantuntevana akkreditoijana vahvistetaan hallituksen esityksessä *HE 9/2018 vp*, s. 98; Ks. myös akkreditoinnin edellytyksistä tarkemmin Artiklassa 43 kohdat 1–3.
[278] *Warma-Lehtinen* 2018, s. 389–390; Ks. myös tiivistettynä Asetuksen tarjoamat vaihtoehdot sertifikaattien myöntämiselle *Warma-Lehtinen* 2018, s. 384–385.
[279] *Warma-Lehtinen* 2018, s. 384–385.

sesti. Toisin sanoen, henkilötietojen käsittelyn ulkoistaminen ei poista Rekisterinpitäjän vastuita. Rekisterinpitäjillä on siten Asetuksen mukaan lähtökohtaisesti *ankara vastuu* eli tuottamuksesta riippumaton vastuu henkilötietojen lainmukaisesta käsittelystä, kun taas Henkilötietojen käsittelijän vastuu voidaan nähdä toissijaisena[280]. Jos Henkilötietojen käsittelijä on kuitenkin 28.10 artiklan mukaisesti määritellyt itsenäisesti käsittelyn tarkoitukset ja keinot, katsotaan hänet Rekisterinpitäjäksi, sille kuuluvineen sanktioineen. Esimerkiksi hyödyntämällä käsittelemiään henkilötietoja omassa markkinointiviestinnässään tai käsittelemällä Rekisteröityjen tietoja vastoin Rekisterinpitäjän antamia ohjeita, Henkilötietojen käsittelijästä tulee Rekisterinpitäjä[281].

Henkilötietojen käsittelijän rikkoessa Tietojenkäsittelysopimus-velvoitteitaan, voidaan sille määrätä artiklan 83 mukainen hallinnollinen sakko Seuraamuskollegion toimesta. Artiklan 28 vastaisesta toiminnasta sakko on enintään 10 000 000 euroa tai 2 % Henkilötietojen käsittelijän edeltävän tilikauden vuotuisesta maailmanlaajuisesta kokonaisliikevaihdosta.[282] Hallinnollisten sakkojen lisäksi tai sijasta tietosuojaviranomaiset voivat edellisessä luvussa kuvatuin tavoin, artiklojen 58 ja 83.2 mukaisesti, hyödyntää myös muita keinoja lainvastaiseen toimintaan, kuten antamalla huomautuksen tai määrätä korjaamaan lainvastainen tilanne. Henkilötietojen käsittelijän ja Rekisterinpitäjän mahdollisuus vapautua vastuustaan on mahdollista vain käänteisen näyttötaakan avulla; henkilötietojen käsittelyyn osallistuneen tahon on osoitettava artiklan 82.3 mukaan, ettei se ole aiheuttanut tapahtunutta vahinkoja ja ettei se ole voinut tosiasiallisesti vaikuttaa tapahtuneeseen.

Osapuolet voidaan katsoa olevan myös yhteisvastuullisia tapahtuneesta vahingosta, jolloin he voivat tarvittaessa hakea toisiltaan korvauksia regressioikeuteensa vedoten.[283] Asiasta säätävän 82 artiklan 4 ja 5 kohtien tarkoituksena on varmistaa Rekisteröidylle kuuluvat korvaukset.

Huomattavaa on, että Asetuksen vaatimuksien koskiessa niin uusia, kuin jo olemassa olevia henkilötietojen käsittelyä koskevia sopimuksia, sanktioriski voi realisoitua myös vanhan pal-

[280] Ks. *Sulin – Tainio* 2017, s. 10.
[281] *Pitkänen* 2018, s. 293.
[282] Artikla 28:n nimissä on käynnistetty tähän mennessä tiedettävästi yksi oikeustapaus Saksassa. Tapauksessa Rekisterinpitäjä Kolibri Image ei ollut saanut solmittua Tietojenkäsittelysopimusta palveluntarjoajansa kanssa yrityksistään huolimatta. Tietosuojaviranomainen antoi palveluntarjoajalle 5000 euron sakot Tietojenkäsittelysopimuksen laiminlyönnistä artiklaan 28.3 vedoten. Palveluntarjoaja on kuitenkin valittanut sakoista ja sakot on tämän johdosta vedetty takaisin, tämän vuoksi asiasta ei ole vielä lopullista päätöstä. *Kolibri Image Regina und Dirk Maass GbR vs Data Protection Authority of Hamburg* 2019.
[283] *Korpisaari* 2018, s. 269.

velusopimuksen alaisen henkilötietojen käsittelyn johdosta. Sanktioriskin koskiessa kaikkia henkilötietoja koskevia palvelusopimuksia, tulee sopimuskumppaneiden selvittää myös jo olemassa olevat sopimukset ja toteuttaa niihin tarvittavat sopimuspäivitykset uusien sopimusneuvotteluiden lisäksi.[284] Mikäli Henkilötietojen käsittelijä laiminlyö sille asetettuja velvoitteitaan, se voi olla vahingonkorvausvelvollinen myös Rekisterinpitäjälle Tietojenkäsittelysopimuksen nojalla.

4.3 Artiklan 28 yritysvaikutukset

Velvollisuus laatia Tietojenkäsittelysopimus tietyn sisältöisenä Rekisterinpitäjän kanssa on muuttanut Henkilötietojen käsittelijöiden riskiprofiilia. Henkilötietojen käsittelijöihin kohdistetut uudet vastuut korostuvat myös Asetuksen sisältämän taloudellisen sanktioriskin myötä. Oikeusministeriön teettämässä selvityksessä arvioitiin Sopimusvaatimusten nostavan Henkilötietojen käsittelijöinä toimivien yritysten palvelusopimusten hintoja.[285] Myös valtioneuvoston teettämässä selvityksessä arvioitiin Asetuksen uusien velvoitteiden ja sanktioriskin nostavan yritysten tietosuojakustannuksia. Valtioneuvoston selvityksen mukaan tietosuojakustannuksia aiheuttanee erityisesti yritysten väliset sopimusneuvottelut sekä niin sanotut compliance – kustannukset, johon voidaan katsoa kuuluvaksi myös yrityksen omien sopimuspohjien päivittäminen.[286]

Arviot Sopimusvaatimusten vaikutuksista näyttävät toteutuneen. Komission asiantuntijaryhmälle[287] teetetyn kyselyn mukaan Tietojenkäsittelysopimusten laadintaa hankaloittaa muun muassa Rekisterinpitäjä-käsittelijäsuhteiden määrittely. Asiantuntijaryhmältä saadussa raportissa ilmenee, että yritykset ovat epävarmoja rooleistaan, jonka vuoksi säännöstä on lähdetty tulkitsemaan soveltaen[288]. Käytännössä tämä on johtanut siihen, että yritykset ovat sopineet Rekisterinpitäjä-käsittelijäsuhteidensa jaosta, antamatta merkitystä sille, kumpi tosiasiassa määrää käsiteltävien henkilötietojen käyttötarkoituksesta ja keinoista.[289] Ongelmallisesti näissä tilanteissa hyödynnetään myös neuvottelevan yrityksen vahvaa *markkina-asemaa*, mikä

[284] Ks. *Partanen* 2018, kohta Miten eteenpäin?
[285] *Lång* 2016, s. 18–19.
[286] *Lång* 2016, s. 22–23; *Valtioneuvoston selvitys* 2017, s. 6.
[287] Ks. *Komission asiantuntijaryhmä* 2019, kohta Jäsenet; *Komission asiantuntijaryhmän raportti* 2019, s. 3.
[288] Epäselvyys näkyy myös viimeaikaisissa oikeustapauksissa. Ks. C-210/16 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein vastaan Wirtschaftsakademie Schleswig-Holstein GmbH* ECLI:EU:C:2018:388, kohdat 36 ja 44. Tapauksessa Facebookin fanisivujen hallitsijan rooli Henkilötietojen käsittelijänä täytyi selvittää. Ratkaisussa fanisivujen hallitsijalla katsottiin olevan mahdollisuus määrätä henkilötietojen käsittelystä ja keinoista, ja se katsottiin tästä syystä Rekisterinpitäjäksi sille kuuluvine vastuineen.
[289] *Komission asiantuntijaryhmän raportti* 2019, s. 17–18.

näkyy erityisesti pienien yritysten osalta heikompana neuvotteluvoimana.[290] Epäselvyys Rekisterinpitäjän ja Henkilötietojen käsittelijän määrittelemisessä on johtanut myös siihen, että osa toimijoista on saattanut kieltäytyä Tietojenkäsittelysopimuksesta, uskoen ettei Sopimusvaatimuksia sovelleta heihin.[291] Asiantuntijaryhmän raportissa vahvistetaan vaikutusarviointien tulokset koskien Tietojenkäsittelysopimusten aiheuttamaa hallinnollista taakkaa; sopimusneuvottelut on koettu aikaa vievinä ja pitkinä prosesseina. Sopimusneuvotteluiden sujuvuuteen on vaikuttanut heikentävästi erityisesti sopimusosapuolien vähäinen asiantuntijuus ja ymmärrys Asetuksen vaatimuksista.[292]

Asetuksen mahdollistamat Tietojenkäsittelysopimusten laatimista tukevat mekanismit voisivat parhaimmillaan keventää yritysten Sopimusvaatimuksista johtuvaa hallinnollista taakkaa. Komission asiantuntijaryhmältä kysyttiin heidän kantaansa vakiosopimuslausekkeista. Raportin mukaan näkemykset vakiosopimuslausekkeiden hyödyistä jakaantuivat puolesta ja vastaan. Osa vastanneista uskoi niiden voivan helpottaa sopimusneuvotteluita tuomalla selkeyttä vastuunjakoon, ja parantaen siten myös sääntelyn yhdenmukaista noudattamista. Vastausten mukaan vakiosopimuslausekkeista hyötyisivät erityisesti pk-yritykset, joilla ei välttämättä ole resursseja neuvotella erikseen jokaista Tietojenkäsittelysopimusta. Osa vastanneista ei kuitenkaan uskonut vakiosopimuslausekkeiden tuovan tarvittavaa hyötyä. Kritiikin mukaan yritykset ovat jo päivittäneet sopimuksensa Sopimusvaatimusten mukaisiksi, jolloin vakiosopimuslausekkeille ei ole enää tarvetta. Toiseksi, Sopimusvaatimusten siirtäminen vakiosopimuslausekkeiden muotoon ei uskottu palvelevan yrityksiä käytännössä sopimusneuvotteluiden sisältöerojen vuoksi. Esimerkkinä mainitaan Henkilötietojen käsittelijältä vaadittavat asianmukaiset tekniset ja organisatoriset toimenpiteet, joita varten Tietojenkäsittelysopimus tarvitsee aina muotoilla erikseen tapauskohtaiset erikoisuudet huomioiden.[293] Osa asiantuntijaryhmän jäsenistä (DIGITALEUROPE ja ETNO-GSMA) kokivat, että henkilötietodirektiivin aikaiset mal-

[290] *Komission asiantuntijaryhmän raportti* 2019, s. 19.
[291] *Komission asiantuntijaryhmän raportti* 2019, s. 18.
[292] Asiantuntijaryhmän mainitsemia haasteita Tietojenkäsittelysopimusten laadinnassa olivat mm.: artiklan 28 ulkopuolisten sopimuslausekkeiden lisääminen (kuten vastuunjako- ja rajoituslausekkeet ns. indemnity-lauseke), Rekisterinpitäjien yritykset siirtää velvoitteitaan Henkilötietojenkäsittelijälle, Henkilötietojen käsittelijän oikeus laskuttaa Rekisterinpitäjän tukemista vaativista toimenpiteistä sekä Henkilötietojen käsittelijöiden aikomukset kieltäytyä yhteistyöstä auditoinneissa tai selvityksissä. Myös Tietojenkäsittelysopimusten suhde osapuolten väliseen pääsopimukseen on herättänyt epäselvyyttä, minkä vuoksi kokonaisia sopimuksia on päädytty jopa purkamaan. *Komission asiantuntijaryhmän raportti* 2019, s. 18.
[293] *Komission asiantuntijaryhmän raportti* 2019, s. 19; Ks. myös asiantuntijaryhmän ehdotuksia vakiosopimuslausekkeiden sisältöehdotuksista, mm. Insurance Europe ehdotti eri riskiperusteisia vakiosopimuslausekkeita, useiden vaihtoehtoisten lausekkeiden tarjoaminen mahdollistaisi niiden hyödyntämisen erilaisissa sopimussuhteissa. *Komission asiantuntijaryhmän raportti* 2019, s. 19–22.

lisopimuslausekkeet ovat jo kansainvälisesti tunnetut ja hyväksytyt ja siten sellaisenaan hyödynnettävissä myös Sopimusvaatimusten osalta. Valtaosan mielestä mainitut mallisopimuslausekkeet tarvitsisi kuitenkin päivittää vastaamaan Asetuksen Sopimusvaatimuksia. Oikeusvarmuuden toteutuminen ja sopimusten turvaama ennakoitavuus koettiin korostuneen tärkeäksi erityisesti kansainvälisessä tietojen vaihdossa, minkä vuoksi Sopimusvaatimusten taannehtiva vaikutus koettiin ongelmalliseksi.[294]

Asetuksen jälkiseuranta on aloitettu myös kansallisesti. Oikeusministeriö toteutti syksyllä 2019 lausuntokierroksen, jossa pyydettiin kannanottoja Asetuksen ja tietosuojalain toimivuudesta.[295] Vastauksissa on yhteneväisyyttä komission asiantuntijaryhmän vastausten kanssa. Sopimusvaatimuksia käsittelevissä lausunnoissa korostuu erityisesti havaitut haasteet koskien sopimusten laatimisen työläyttä[296]; Rekisterinpitäjä-käsittelijäsuhteiden määrittelyä[297], erityisesti vastuiden ja vastuunrajoituksia koskien[298]; sekä Tietojenkäsittelysopimusten muodostumista laajoiksi ja vaikealukuisiksi kokonaisuuksiksi[299]. Tietojenkäsittelysopimusten laatimisesta aiheutunut kuorma johtuu lausuntojen mukaan muun muassa vanhojen sopimusten päivittämisestä ja ylimääräisen asiantuntija-avun tai erityisosaamisen hankkimisesta. Keskuskauppakamari toi esille myös näkemyksensä, jonka mukaan Sopimusvaatimusten täytäntöönpano kuormittaa erityisesti pk-yrityksiä niiden resurssi- ja osaamisvajeen vuoksi. Poiketen komission asiantuntijaryhmän antamista vastauksista, Oikeusministeriön saamissa lausunnoissa tuotiin esille myös yritysten itse laatimat mallipohjat Tietojenkäsittelysopimuksista. Valmiit Tietojenkäsittelysopimukset ovat lausuntojen mukaan aiheuttaneet tilanteita, joissa erityisesti pienet ja neuvotteluvoimaltaan heikommat Rekisterinpitäjänä toimivat yritykset ovat kohdanneet isompien palveluntuottajien kanssa niin sanottuja ”ota tai jätä” – tilanteita.

---

[294] *Komission asiantuntijaryhmän raportti* 2019, s. 20–21; Ks. myös *Euroopan komissio (SCC)* 2019.

[295] Vastauksia oli mahdollista antaa 7.8.–17.9.2019 välisenä aikana. Lausuntoja annettiin yhteensä 74 eri taholta, lausunnoista 22 kannanottoa käsitteli Sopimusvaatimusten vaikutuksia. Lausuntojen antajat koostuivat kansallisista etujärjestöistä ja viranomaisista. Ks. *Oikeusministeriön selvitys* 2019, kohta Lausuntopyynnön taustatiedot.

[296] Asiasta lausui mm. Finanssiala ry, Suomen Kuntaliitto ry, Keskuskauppakamari, Senaatti-kiinteistöt, Suomen Perimistoimistojen Liitto ry, Oikeusrekisterikeskus, Helsingin yliopisto, Suomen Hammaslääkäriliitto ry, Helsingin kaupunki, Suomen Asiakastieto Oy, Suomen Metsäkeskus, SOSTE Suomen sosiaali- ja terveys ry. *Oikeusministeriön selvitys* 2019, kohta Lausunnonantajien lausunnot.

[297] Asiasta lausui mm. Finanssiala ry ja Senaatti-kiinteistöt. *Oikeusministeriön selvitys* 2019, kohta Lausunnonantajien lausunnot.

[298] Asiasta lausui mm. Suomen itsenäisyyden juhlarahasto Sitra, Suomen Perimistoimistojen Liitto ry, Väestörekisterikeskus, Suomen Hammaslääkäriliitto ry, Asiakkuusmarkkinointiliitto ry, SOSTE Suomen sosiaali- ja terveys ry. *Oikeusministeriön selvitys* 2019, kohta Lausunnonantajien lausunnot.

[299] Asiasta lausui mm. Suomen itsenäisyyden juhlarahasto Sitra, Suomen Perimistoimistojen Liitto ry, Väestörekisterikeskus, Suomen Hammaslääkäriliitto ry, Asiakkuusmarkkinointiliitto ry, SOSTE Suomen sosiaali- ja terveys ry. *Oikeusministeriön selvitys* 2019, kohta Lausunnonantajien lausunnot.

Tietojenkäsittelysopimusten sisällön lisäksi, myös artiklan 28 vaatimus alihankintaketjun selvittämisen toteuttamisesta koettiin haastavaksi tai jopa mahdottomaksi.[300] Oikeusministeriölle annetut lausunnot antavatkin ymmärtää, että käytännössä yrityksiltä puuttuu tosiasiallinen mahdollisuus vaikuttaa Tietojenkäsittelysopimusten sisältöön sekä alihankkijoiden valintaan. Lausunnoissa tuodaan esille myös Sopimusvaatimusten liiallinen yksityiskohtaisuus sekä kokemukset sanktio-riskin siirtämisestä edelleen Tietojenkäsittelysopimusten vastuulausekkeisiin tai palvelusopimusten hintoihin.[301] Lausunnoista on luettavissa, että haasteet Sopimusvaatimusten täytäntöönpanossa kasvattavat sekä Rekisterinpitäjien että Henkilötietojen käsittelijöiden työtaakkaa ja aiheuttavat yrityksille huomattavia kustannuksia.

4.4 Yhteenveto

Sopimusvaatimusten aiheuttama hallinnollisen taakan kasvaminen yrityksissä vaikuttaa kiistattomalta tehtyjen selvitysten valossa. Kuitenkin tarkat lukemat vielä uupuvat, minkä vuoksi Asetuksen ja artiklan 28 aiheuttama todellinen taakka yrityksille on vielä suuntaa-antavalla tasolla. Tarkempia tuloksia voitanee saada toukokuussa 2020, kun komissio julkaisee Asetuksen artiklan 97 mukaisen kertomuksensa Asetuksen arvioinnista ja uudelleentarkastelusta.[302]

Arvioitaessa Asetuksen yritysvaikutuksia ennen sen voimaantuloa, yrityksiä kuormittavina tekijöinä arvioitiin olevan erityisesti sopimusneuvottelut sekä Tietojenkäsittelysopimuspohjien laatiminen. Aloitetun jälkiseurannan mukaan Sopimusvaatimukset ovat kasvattaneet yrityksille kohdistuvaa hallinnollista taakkaa ja aiheuttaneet siten huomattavia kustannuksia. Arvioiden mukaisesti tähänastisissa selvityksissä on korostunut Tietojenkäsittelysopimusten laatimisen raskaus sekä sopiminen vastuista ja vastuunrajoituksista. Myös epäselvyys Asetuksen, ja siten myös artiklan 28 määritelmistä ja tulkinnasta ovat vaikeuttaneet yritysten Tietojenkäsittelysopimusten laadintaa. Mahdollisesti näistä johtuen, neuvotteluita tukevien mekanismien tarve on noussut esille monessa lähteessä.

---

[300] Asiasta lausui mm. Finanssiala ry, Suomen asianajajaliitto, Senaatti-kiinteistöt, Suomen Perimistoimistojen Liitto ry, ja Asiakkuusmarkkinointiliitto ry. *Oikeusministeriön selvitys* 2019, kohta Lausunnonantajien lausunnot.

[301] Sopimusten liiallisesta yksityiskohtaisuudesta lausui mm. Elinkeinoelämän keskusliitto EK, Palvelualojen työnantajat PALTA ry, FiCom ry, Suomen Hammaslääkäriliitto ry. Sanktio-riskin siirtämisestä: Senaatti-kiinteistöt, Suomen Perimistoimistojen Liitto ry. Vrt. osa lausuntojen antajista näki artiklan 28 hyvänä uudistuksena, mm. Kirkkohallitus näki sen selkeyttävän Henkilötietojen käsittelijän roolia ja tehtäviä, ja Helsingin kaupunki hyvänä, sopimista helpottavana listauksena. *Oikeusministeriön selvitys* 2019, kohta Lausunnonantajien lausunnot.

[302] Asetuksen 97 artiklan mukaisesti komission tulee toimittaa Euroopan parlamentille ja neuvostolle säännöllisesti kertomukset asetuksen arvioinnista ja uudelleentarkastelusta viimeistään 25 päivänä toukokuuta 2020 ja joka neljäs vuosi sen jälkeen.

Komission asiantuntijaryhmän mukaan vakiosopimuslausekkeet saattaisivat keventää sopimusneuvotteluita ja siten vähentää Sopimusvaatimusten yrityksille aiheuttamaa hallinnollista taakkaa. Tässä olisi kuitenkin huomioitava jokaisen neuvottelun oma erityisluonne ja tarpeet. Tarkoittaen, että hyvin yleisellä tasolla muotoillut lausekkeet vaatinevat muokkausta, joka taas laskee niiltä odotettua hyötysuhdetta. Vaihtoehtona voisi olla useamman vakiosopimuslauseke- pohjan laadinta tai useiden vaihtoehtoisten lausekkeiden tarjoaminen, mutta kuten komission asiantuntijaryhmä toteaa, tämä voisi aiheuttaa sekaannusta.[303] Jääkin nähtäväksi milloin ja millä tarkkuudella komissio julkaisee yritysten sopimusneuvotteluiden tueksi Asetuksen sisältämiä mekanismeja.[304] Ohjeistukset aiheesta olisivat erittäin tarpeellisilta, sillä mekanismien tarvetta sekoittaa tällä hetkellä myös henkilötietodirektiivin aikaiset mallisopimuslausekkeet. Kyseisten mallisopimuslausekkeiden hyödyntäminen ja sovellettavuus ovat toistaiseksi yrityksille epäselviä[305], yritykset kaipaavatkin linjanvetoja täyttävätkö vanhat mallisopimuslausekkeet Sopimusvaatimusten velvoitteita.[306] Kuitenkin komission julkaisemassa tiedonannossa Asetuksen alustavasta arvioinnista todetaan, että Asetus mahdollistaa komission laatimien vakiosopimuslausekkeiden hyödyntämisen niin EU:n sisällä kuin kolmansien maidenkin välillä, toisin kuin kansallisen tietosuojaviranomaisen laatimana – jolloin vakiosopimuslausekkeet ovat hyödynnettävissä vain kyseisessä jäsenmaassa.[307] Tiedonannossa ei oteta kantaa viitataanko näillä henkilötietodirektiivin aikaisiin lausekkeisiin, niiden voimassaoloon tai sovellettavuuteen Asetuksen nojalla.

Vaikka viranomaisten tekemät selvitykset Asetuksen täytäntöönpanosta sisältävät osin myös kannanottoja artiklasta 28, tarvitsee Sopimusvaatimuksista aiheutuneet yritysvaikutukset selvittää suoraan Asetusta soveltavilta yrityksiltä. Tästä johtuen, kirjoitettavan tutkielman ohessa toteutettiin myös kysely kohdistettuna suoraan yrityksille. Kyselyn avulla on mahdollista selvittää tarkemmin rajattua Asetuksen osa-aluetta, Sopimusvaatimuksia ja sen aiheuttamia vaikutuksia Suomessa toimiville yrityksille.

[303] *Komission asiantuntijaryhmän raportti* 2019, s. 20.
[304] Ks. *COM (2019) 374, lopull.*, s. 10 ja 12.
[305] Ks. *Euroopan komissio (SCC)* 2019.
[306] Oikeusministeriön saamissa lausunnoissa mm. Elinkeinoelämän keskusliitto EK, Palvelualojen työnantajat PALTA ry, sekä FiCom ry mainitsivat kannanotoissaan epätietoisuutensa mallisopimuslausekkeiden soveltumisesta artiklan 28 velvoitteisiin. *Oikeusministeriön selvitys* 2019, kohta Lausunnonantajien lausunnot.
[307] Ks. *COM (2019) 374, lopull.*, s. 9–10.

5 KYSELYTUTKIMUS JA TULOKSET

5.1 Kyselytutkimuksen tausta ja toteutus

Koska Asetuksesta tehdyt vaikutusarvioinnit eivät ole tarkkuudeltaan riittäviä selvittämään Asetuksen Tietojenkäsittelysopimusten yritysvaikutuksia, toteutettiin tutkielman osana kyselytutkimus. Kyselytutkimuksella on pyritty selvittämään millaisia vaikutuksia Asetuksella ja erityisesti artiklan 28 määrittävillä Tietojenkäsittelysopimuksilla on ollut Suomessa toimiville yrityksille. Tässä luvussa esitellään toteutettu kyselytutkimus ja siitä saadut tulokset.

Kyselyn tarkoitus oli kartoittaa Sopimusvaatimusten yritysvaikutuksia Suomessa toimiville yrityksille. Kyselytutkimukseen osallistumisen ainoana inkluusiokriteerinä oli vastaajan yrityksen toiminta Suomessa. Tavoiteltu vastaajien joukko oli täten laaja - kattaen myös Suomessa toimivat monikansallisten yhtiöiden tytäryhtiöt. Tavoitteena olikin saada mahdollisimman laaja ymmärrys yritysten käytännön kokemuksista Tietojenkäsittelysopimuksia koskien. Tästä syystä myös ainoa ekskluusiokriteeri kohdistui yrityksiin, joilla ei ollut toimintaa Suomessa.

Tutkielma kirjoitettiin osana asianajotoimisto Roschierin Thesis – ohjelmaa, jonka kautta tutkielman kirjoittajan sai tukea ja apua sähköisen verkkokyselyn teknisessä ja sisällöllisessä toteutuksessa. Sähköinen kysely luotiin Questback-ohjelmalla, joka siirtää vastaukset automaattisesti Excel-ohjelmaan ja luo kysymyksistä graafiset taulukot. Kyselyn ymmärrettävyyden ja vastattavuuden varmistamiseksi, kysymykset annettiin ennen julkistamista arvioitavaksi yhdelle suomalaiselle pörssiyhtiölle, niin sanottua testivastaamista varten. Yhtiöltä saatujen palautteiden huomioimisen jälkeen, kysely lähetettiin sähköisenä verkkokyselynä yhteensä noin 40 yritykselle. Tämän lisäksi kysely julkaistiin sosiaalisen median palvelussa, jossa sen näki useat sadat henkilöt. Sähköpostitse lähetetty kysely pyrittiin kohdistamaan henkilöille, jotka oletettavasti olivat läheisesti tekemisissä Asetuksen Sopimusvaatimusten kanssa, lisäksi vastauskynnystä pyrittiin madaltamaan pyytämällä vastaajilta heillä oleva paras arvio Sopimusvaatimusten kuormittavuudesta tarkkojen lukujen sijaan. Kaikki vastaukset annettiin anonyymisti. Lähetetty ja julkaistu kyselylinkki oli mahdollista jakaa myös eteenpäin, minkä vuoksi ei ollut mahdollista selvittää kuinka suuren joukon kysely lopulta tavoitti. Kyselyyn oli mahdollista vastata 18.4.–7.5.2019 välisenä aikana, jonka jälkeen vastausaikaa jatkettiin 24.5.2019 asti vastaajamäärän kasvattamiseksi. Vastauksia saatiin lopulta 11 kappaletta.

Kysely on jaettu viiteen eri osioon, joita ovat: (1) Yhtiön taustatiedot, (2) Henkilötietojen käsittely yhtiössä, (3) Asetuksen aiheuttama hallinnollinen taakka, (4) Asetuksen Sopimusvaatimukset, ja (5) kysymykset Henkilötietojen käsittelijöille. Viides osio on suunnattu vain niille yrityksille, jotka käsittelevät henkilötietoja myös Henkilötietojen käsittelijänä. Vastaajille tarjottiin mahdollisuutta osallistua tutkimukseen myös haastattelun muodossa, mutta yksikään 11:sta yrityksestä ei valinnut tätä vaihtoehtoa, joten tutkimuksessa ei päästy hyödyntämään haastatteluita. Kysely sisältää erilaisia kysymystyyppejä, joita ovat muun muassa monivalintakysymykset, arviointiasteikkokysymykset sekä kommenttikenttäkysymykset. Kyselyyn oli mahdollista vastata sekä suomeksi että englanniksi. Lisäksi tiettyjä käsitteitä on avattu vastaajille kysymysten tarkentamiseksi ja ymmärrettävyyden helpottamiseksi. Kyselyyn vastatessa, vastaajilla ei ollut mahdollista edetä kysymysten yli, eli jokaiseen kysymykseen tuli vastata, jotta pääsi kyselyssä eteenpäin. Kysely on sisällytetty kokonaisuudessaan tutkielman liitteisiin, mistä on nähtävissä sekä kysymysten tarkka sisältö, että mukana ollut saateteksti[308].

Vastausten jäätyä määrällisesti melko vähäiseksi, ei tutkimuksen tulokset ole yleistettävissä koko yrityskenttään. Syyt miksi moni yritys jätti vastaamatta jää epäselväksi. Syitä voitanee vain arvailla, kuten epävarmuus kysyttävästä asiasta, ajanpuute ja haluttomuus käyttää omaa aikaa kyselyyn tai inhimillinen unohdus. Tulosten kannalta on kuitenkin tärkeää, että vastaajien joukossa oli yritysten edustajia eri sektoreilta, mikä osaltaan rikastuttaa saatuja tuloksia. Lisäksi tulosten laatua parantavana seikkana voidaan mainita, että kaikki vastaajat olivat tehtävänimikkeiltään ja tai työkokemukseltaan sellaisia henkilöitä, jotka olivat oletettavasti työskennelleet Asetuksen tuomien muutosten parissa. Kyselyllä onnistuttiin selvittämään tiettyjä kuormittavia tekijöitä, joita sekä Asetus että artikla 28 ovat aikaansaaneet yrityksissä. Tuloksia katsottaessa, on kuitenkin pidettävä mielessä, että Asetuksen velvoitteet ovat yrityksille vielä tuoreita, eivätkä kaikki sen aiheuttamat vaikutukset ole välttämättä selvillä. Lisäksi osa sääntelyn kuormittavista tekijöistä todennäköisesti vähenee Asetuksen voimassaolon myötä.

5.2 Kyselyn osa-alueet ja niistä saadut tulokset

5.2.1 Yhtiön taustatiedot

Kyselyn ensimmäisessä osiossa haluttiin selvittää, millainen on kyselyyn vastanneiden yritysten joukko. Koska vastaajien osalta ei haluttu tehdä liian tiukkoja inkluusiokriteereitä, oli tär-

[308] Ks. tutkielman liitteet 2–3.

keää selvittää, minkälaiset yritykset kyselyyn vastasivat. Jos vastaajissa olisi useampi saman toimialan yritys, heidän vastauksensa saattaisivat olla vertailukelpoisia keskenään. Yritysten vastausten ristiin vertailu antaisikin arvokasta tietoa tutkielmalle. Lisäksi vastaajien tehtävänimikkeiden ja työkokemuksen kartoittamisen avulla pyrittiin selvittämään vastausten luotettavuutta.

Taustatietoja kartoitettiin yhteensä viidellä kysymyksellä. Ensimmäisessä taustatietoihin liittyvässä kysymyksessä selvitettiin yritysten toimialaa, toisessa kysymyksessä liikevaihtoa, kolmannessa yritysten kotipaikan maantieteellistä sijaintia, neljännessä edelleen yritysten kokoluokkaa kysyen henkilöstön määrää ja viimeisellä kysymyksellä selvitettiin vastaajan taustaa kysyen työkokemusta - ja asemaa yhtiössä. Kaikki kysymykset olivat avoimia, eikä valmiita vastausvaihtoehtoja annettu.

Kyselyyn vastasi taustoiltaan hyvin heterogeenin 11 yrityksen joukko. Kahta yritystä lukuun ottamatta, jokainen yritys edusti eri toimialaa. Suurinta joukkoa edustivat suuryritykset (81,8 %), näistä lähes kaikki (88,9 %) ilmoittivat liikevaihdoksi yli 50 miljoonaa euroa ja suurimmassa osassa (77,8 %) työskenteli yli 250 työntekijää. Loput kaksi vastanneista yrityksistä kuului pk-yritysten luokkaan: toinen yrityksistä edusti mikro yrityksiä alle 2 miljoonan euron liikevaihdolla ja alle 10 henkilön henkilöstö määrällä, ja toinen yritys edusti puolestaan pieniä yrityksiä reilu 2 miljoonan liikevaihdolla ja alle 50 henkilön henkilöstön määrällä.

Maantieteellisesti 90,9 % vastaajista ilmoitti yrityksen kotipaikan sijainniksi Suomen. Edelleen näistä yrityksistä 90,9 % kotipaikan maantieteellinen sijainti oli Etelä-Suomessa. Kaikista vastaajista yksi ilmoitti kotipaikan olevan muualla kuin Suomessa[309].

Vastaajien työkokemus yhtiössä oli kaikilla vastaajilla kaksi vuotta tai enemmän, jakaantuen niin, että alle viiden vuoden työkokemuksella oli 18,2 % vastaajista ja loput 72,7 % yli viiden vuoden työkokemuksella. Yksi vastaajista ei kertonut työkokemustaan lainakaan. Alla on nähtävissä vastaajien tehtävänimikkeet yrityksissä kuten vastaajat ovat ne ilmoittaneet:

> *Lakimies; DP; Chief Business Officer; Director; Customer Support; TJ; IT järjestelmäasiantuntija; Hallintojohtaja; Myyntijohtaja; Osakas, asianajaja; Senior Legal Counsel; DPO; Senior Legal Counsel.*

[309] Ainoa kyselyyn vastannut ulkomaalainen yritys ilmoitti kotipaikakseen Ruotsin.

Ensimmäisen osion vastausten perustella on nähtävissä, että kyselyyn vastanneet yritykset ovat pääosin suomalaisia suuriyrityksiä niin liikevaihdollisesti kuin henkilöstönkin suhteen ja vastaajat yritysten kokeneita työntekijöitä. Tehtävänimikkeiden perusteella on oletettavaa, että vastaajat ovat olleet läheisesti tekemisissä Asetuksen tuomien muutosten parissa. Valtaosa vastaajista ilmoitti kotipaikakseen pääkaupunkiseudun, mikä lienee luonnollista huomioitaessa Suomen yritysten maantieteellinen jakautuminen yleisellä tasolla[310]. Mielenkiintoista vastaajien joukossa on suuryritysten merkittävä osuus, verrattaessa osallistumisotantaa Tilastokeskuksen yritysrekisteriin, jonka mukaan kaikista Suomessa toimivista yrityksistä vain 0,2 % (615 yritystä) ovat suuryrityksiä[311].

5.2.2 Henkilötietojen käsittely yhtiössä

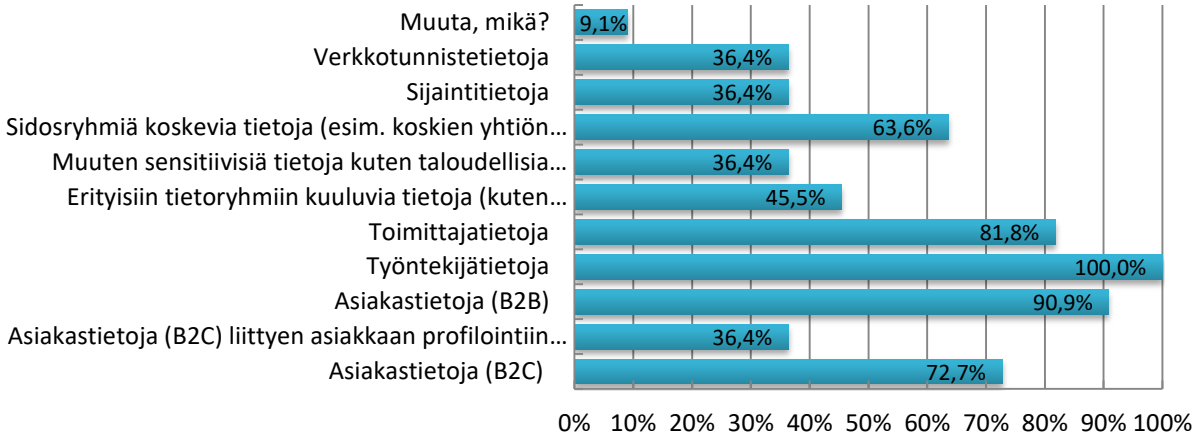
Osiossa kaksi haluttiin varmistaa Asetuksen soveltuvuus yrityksen toimintaan, vaikka käytännössä jokainen yritys käsitteleekin henkilötietoja ainakin jossakin määrin muun muassa henkilöstönsä osalta. Kysymyksillä tavoiteltiin erityisesti yritysten tietojenkäsittelyn luonnetta. Kysymällä toimiiko yritys Rekisterinpitäjänä, henkilötietojen käsittelijänä vai molemmissa rooleissa, pyritään jäljempänä selvittämään näiden vaikutusta Asetuksen aiheuttamaan taakkaan. Lisäksi osiosta kaksi saadut vastaukset tarkensivat henkilötietojen käsittelyn osalta sitä joukkoa, joka kyselyyn vastasi.

Henkilötietojen käsittelyyn liittyvä kysymys oli kolmiosainen: (i) sen ensimmäisessä kysymyksessä selvitettiin, millaisia henkilötietoja yrityksessä käsitellään, (ii) toisessa kysymyksessä sitä, toimiiko yritys Rekisterinpitäjänä vai Henkilötietojen käsittelijänä, (iii) ja viimeisessä sitä, käsittelevätkö yritykset henkilötietoja rajatylittävinä siirtoina. Kaikissa kysymyksissä vastausvaihtoehdot oli annettu valmiiksi ja lisäksi ensimmäisessä kysymyksessä vastaajilla oli myös mahdollisuus valita kohta *”muuta, mikä”*, jolloin vastaajan tuli sanallisesti kertoa, millaisia muita henkilötietoja yritys käsittelee. Vastaajilla oli jokaisen kysymyksen kohdalla mahdollisuus valita useampi kuin yksi annetuista vaihtoehdoista.

Vastauksista nousee esiin, että valtaosa yrityksistä käsittelee työntekijätietoja (100 %), asiakastietoja (*business to busine*ss) (90,9 %), toimittajatietoja (81,8 %), asiakastietoja (*business*

[310] Pääkaupunkiseudun osuus Suomen yrityksistä oli 20 %, yritysten henkilöstömäärästä 30 % ja liikevaihdosta 39 %. Ks. *Henriksson* 2018, s. 4; Ks. myös *Tohmo – Littunen* 2003, s. 427.
[311] *Suomen Yrittäjät* 2019, kohta Yrittäjyys Suomessa.

to consumer) (72,7 %) ja sidosryhmiä koskevia tietoja[312] (63,6 %). Vastauksista käy myös ilmi, että monessa yrityksessä käsitellään lisäksi asiakastietoja (*business to consumer*) liittyen asiakkaan profilointiin ja/tai kanta-asiakastietoihin, erityisiin tietoryhmiin kuuluvia tietoja kuten terveystietoja, muuten sensitiivisiä tietoja kuten taloudellisia tietoja[313], sijaintitietoja sekä verkkotunnistetietoja. Näiden vastausten prosentuaalinen hajonta oli välillä 36,4–45,5 %. (Taulukko 1) Lisäksi yksi vastaaja kertoi yhtiön käsittelevän jotain muuta henkilötietoa, kuin valmiiksi annetuissa vaihtoehdoissa oli valittavana. Vastaaja antoi tällöin avoimeen vastauskenttään vastaukseksi: ”*luottamuksellisen viestin salaisuuden alaisia tietoja”*.



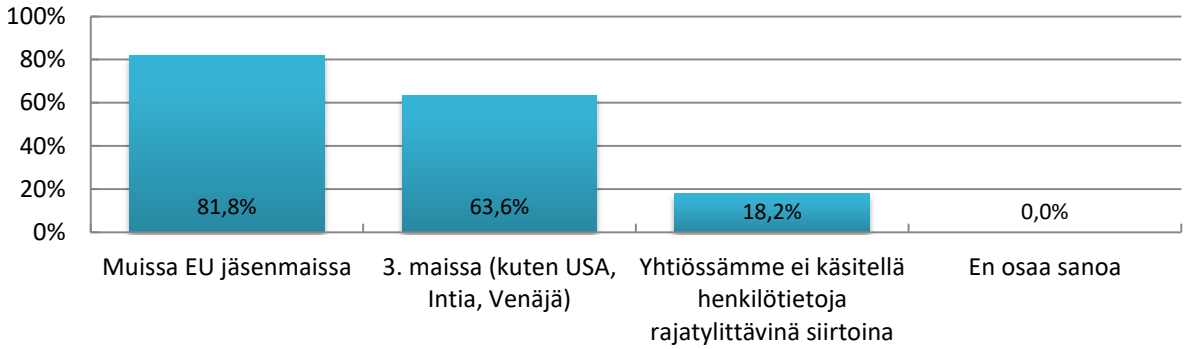
Taulukko 1. Yritysten käsittelemät henkilötiedot.

Kysymyksen toisessa osassa kysyttiin toimivatko yritykset Rekisterinpitäjänä vai Henkilötietojen käsittelijänä. Vastausvaihtoehdoista oli mahdollista valita myös molemmat vaihtoehdot. Vastauksista ilmenee, että vastaajista 81,8 % kertoi toimivansa Rekisterinpitäjänä sekä 72,7 % Henkilötietojen käsittelijänä. Toisin sanoen vastanneista yrityksistä reilu puolet (54,5 %) toimivat sekä Rekisterinpitäjänä että Henkilötietojen käsittelijänä.

Ensimmäisen osan viimeisessä kysymyksessä selvitettiin, oliko vastanneilla yrityksillä henkilötietojen käsittelyä rajatylittävinä siirtoina. Vastauksista on nähtävissä, että valtaosalla (81,8 %) vastanneista yrityksistä on liiketoimintaa muuallakin kuin Suomessa, erityisesti

[312] esimerkiksi koskien yhtiön omistajia, sijoittajia, kumppaneita.
[313] esimerkiksi luottokorttitietoja.

EU:n sisämarkkinoilla. Ainoastaan kaksi vastanneista vastasi, ettei yrityksellä ole rajatylittäviä henkilötietojen siirtoja.[314] (Taulukko 2)



Taulukko 2. Henkilötietojen käsittely rajatylittävinä siirtoina.

Toisen osan vastausten perusteella on nähtävissä, että kaikkien vastanneiden yritysten toiminnassa käsitellään useita erilaisia henkilötietoja. Vastauksista nousee esiin, että kaikissa tai lähes kaikissa käsiteltiin työntekijä-, toimittaja, ja asiakastietoja (koskien sekä business to business että business to consumer). Erityisiä johtopäätöksiä esimerkiksi siitä, lisääkö yrityksen kokoluokka tai toimiala sitä, kuinka paljon erilaisia henkilötietoja yrityksissä käsitellään, ei ole tehtävissä. Yli puolet vastaajista toimi sekä Rekisterinpitäjänä että Henkilötietojen käsittelijänä. Lisäksi lähes kaikki vastanneet yritykset kertoivat käsittelevänsä henkilötietoja rajatylittävinä siirtoina myös muissa EU maissa. Ainoastaan kaksi saman toimialan yritystä, joista toinen oli yritysluokaltaan mikro- ja toinen pieni yritys, vastasivat olevansa toiminnaltaan täysin kansallisia toimijoita. Kolmansissa maissa tapahtuvaa henkilötietojen käsittelyä oli myös usealla keskisuurella yrityksellä. On siten johdonmukaista, että yritykset arvioivat kyselyn kolmannessa osiossa hallinnollisen taakan lisääntyneen Asetuksen voimaantulon myötä. Henkilötietojen rajatylittävien siirtojen yleisyys ilmentänee myös henkilötietojen käsittelyn kansainvälisyyttä, erityisesti käsittelyn käytännön toteutuksen näkökulmasta.

5.2.3 Asetuksen aiheuttama hallinnollinen taakka

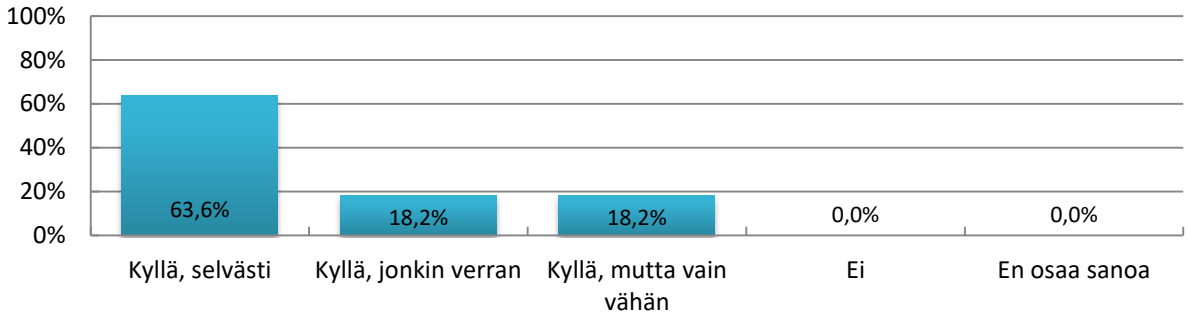
Kyselyn kolmannessa osiossa selvitettiin, onko henkilötietojen käsittelystä johtuva hallinnollinen taakka lisääntynyt yrityksissä Asetuksen voimaan tulon myötä ja pyydettiin yrityksiä arvioimaan artiklan 28 Sopimusvaatimusten osuutta taakasta. Osiossa haluttiin selvittää myös

[314] Vrt. Rajatylittäviä asioita oli EU:ssa vuonna 2018 yhteensä 591, joista Suomi osallistuvana valvontaviranomaisena 106 tapauksista, ja Suomi johtavana valvontaviranomaisena 5.ssä tapauksessa. *Tietosuojavaltuutetun toimisto* 2018a, s. 19.

tarkemmin sitä, mitkä seikat yritysten mukaan ovat lisänneet hallinnollisen taakan kasvua. Lisäksi vastausten perusteella voitaneen tehdä johtopäätöksiä Sopimusvaatimusten merkittävyydestä yrityksissä.

Ensimmäisessä kysymyksessä vastaajan tuli arvioida onko Asetus lisännyt yrityksen hallinnollista taakkaa. Vastausvaihtoehdoista oli mahdollista valita useampi vastausvaihtoehto. Mikäli vastaaja arvioi, että hallinnollinen taakka on lisääntynyt, tuli hänen lisäksi arvioida niitä seikkoja, jotka sitä ovat erityisesti aiheuttaneet. Vastausvaihtoehdot annettiin valmiina. Arvioitaessa hallinnollisen taakan aiheuttaneita seikkoja, vastaajat pystyivät valitsemaan valmiiden vaihtoehtojen lisäksi myös vaihtoehdon *”muu, mikä”*. Näin yrityksille annettiin mahdollisuus kertoa sanallisesti jokin listasta puuttunut vaihtoehto. Osan viimeisessä kysymyksessä tuli arvioida Sopimusvaatimusten osuutta hallinnollisesta taakasta.

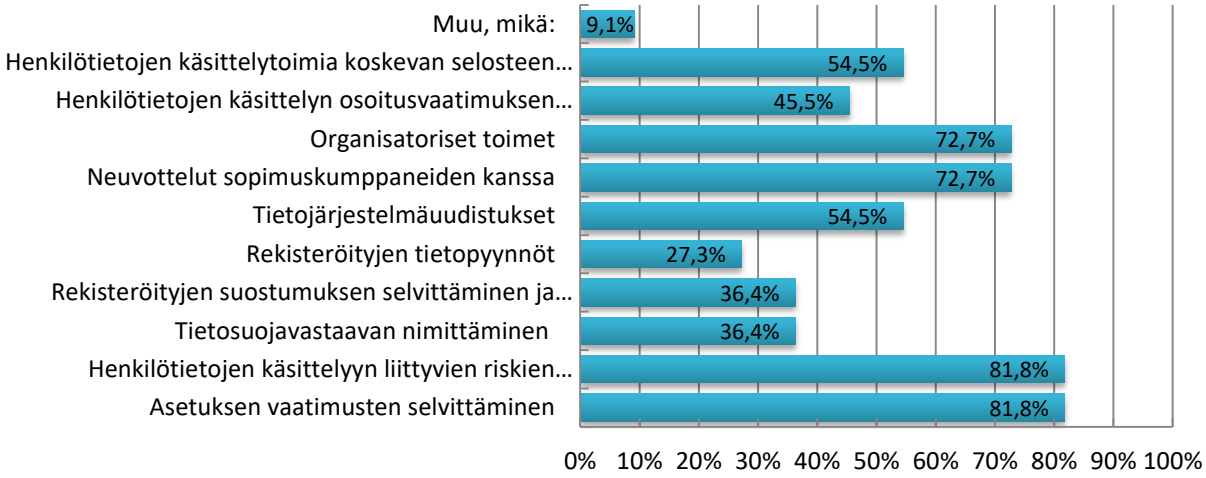
Ensimmäisen kysymyksen kohdalla on selkeästi nähtävissä, että Asetuksen jälkeen yritysten hallinnollinen taakka on lisääntynyt. Vastauksista ilmenee, että valtaosa (63,6 %) koki taakan lisääntyneen selvästi Asetusta edeltäneeseen aikaan verrattuna. Myös loput vastaajista kokivat taakan lisääntyneen niin, että vastanneet kertoivat taakan lisääntyneen jonkin verran (18,2 %) tai vain vähän (18,2 %). (Taulukko 3)



Taulukko 3. Asetuksen aiheuttama hallinnollisen taakan kasvu yrityksissä.

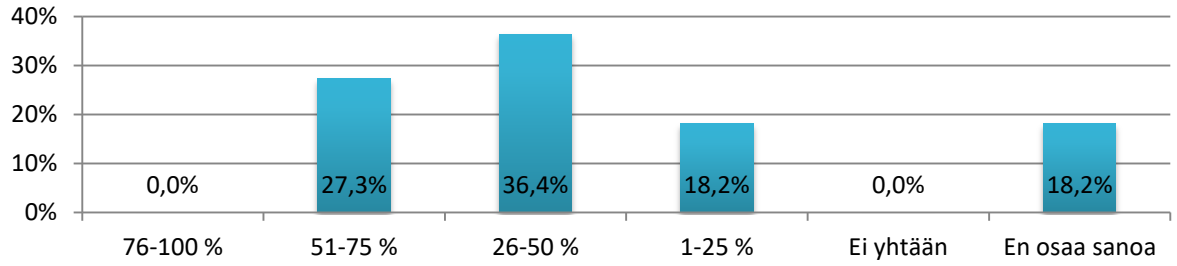
Koska kaikki vastanneet kokivat hallinnollisen taakan lisääntyneen, tuli kaikkien arvioida osion toisessa kysymyksessä mistä seikoista hallinnollisen taakan lisääntyminen heidän mukaansa johtui. Taulukosta 4 on nähtävissä, että erityisesti Asetuksen vaatimusten selvittäminen, henkilötietojen käsittelyyn liittyvien riskien kartoittaminen, tietojärjestelmäuudistukset, (kuten IT-järjestelmien ja tietojenkäsittelyohjelmien päivittäminen tai uusien hankita), neuvottelut sopimuskumppaneiden kanssa, (kuten palvelusopimusten päivittämistä tai vastuunrajoituksista sopiminen), sekä organisatoriset toimet (kuten henkilöstölle annettava ohjeistus ja

henkilötietoja käsittelevän henkilöstön koulutus ja henkilötietojen käsittelytoimia koskevan selosteen ylläpito) lisäsivät hallinnollista taakkaa. Prosentuaalisesti yli puolet (jakauman 54,5 % - 81,8 %) arvioivat hallinnollisen taakan lisääntyneen näiden vastausvaihtoehtojen osalta. Mainittujen lisäksi, osa yrityksistä arvioi (jakauma 27,3 % - 45,5 %), että hallinnollista taakkaa ovat lisänneet myös tietosuojavastaavan nimittäminen, Rekisteröityjen suostumuksen selvittäminen ja informointi, Rekisteröityjen tietosuojapyynnöt sekä henkilötietojen käsittelytoimia koskevan selosteen ylläpito. (Taulukko 4) Lisäksi yksi vastaaja kertoi taakan lisääntymisen johtuvan jostain muusta syystä kuin valmiiksi annetuissa vaihtoehdoissa oli valittavana. Vastaaja antoi tällöin avoimeen vastauskenttään vastaukseksi: ”*sopimusten tietosuojaliitteet*”.



Taulukko 4. Hallinnollisen taakan kasvun aiheuttajat.

Osan kolmannessa ja viimeisessä kysymyksessä, vastaajien tuli arvioida Sopimusvaatimusten osuutta Asetuksen aiheuttamasta hallinnollisesta taakasta. Vastauksista on nähtävissä, että Sopimusvaatimusten osuus hallinnollisesta taakasta arvioitiin melko suureksi. Yli puolet vastaajista arvioi Sopimusvaatimusten aiheuttavan 25 % -75 % Asetuksen hallinnollisesta taakasta. Muutama vastaaja arvioi Sopimusvaatimusten osuudeksi 1-25 %. Vastaajista vain kaksi eivät osanneet arvioida Sopimusvaatimusten osuutta Asetuksen hallinnollisesta taakasta. Kukaan vastaajista ei valinnut vaihtoehtoa ”*ei yhtään*”. (Taulukko 5)



Taulukko 5. Sopimusvaatimusten osuus hallinnollisesta taakasta.

Kolmannen osion vastausten perustella on nähtävissä, että kaikki yritykset arvioivat hallinnollisen taakan lisääntyneen Asetuksen voimaantulon myötä. Merkittävää on, että yli puolet vastaajista arvioi taakan lisääntyneen selvästi. Vastanneet yritykset kokivat, että hallinnollista taakkaa ovat lisänneet lähes kaikki kyselyssä esitetyt vaihtoehdot, mutta erityisen kuormittaviksi koettiin Asetuksen vaatimusten selvittäminen ja riskien kartoittaminen sekä organisatoriset toimet ja neuvottelut sopimuskumppaneiden kanssa. Sopimusvaatimusten osuus lisääntyneestä hallinnollisesta taakasta koettiin verrattain suureksi, mikä lienee selittyvän osaksi edellä esiin tulleista sopimusneuvotteluista. Vastausten perusteella on todennäköistä, että Asetus on aiheuttanut myös merkittäviä kuluja yrityksille.

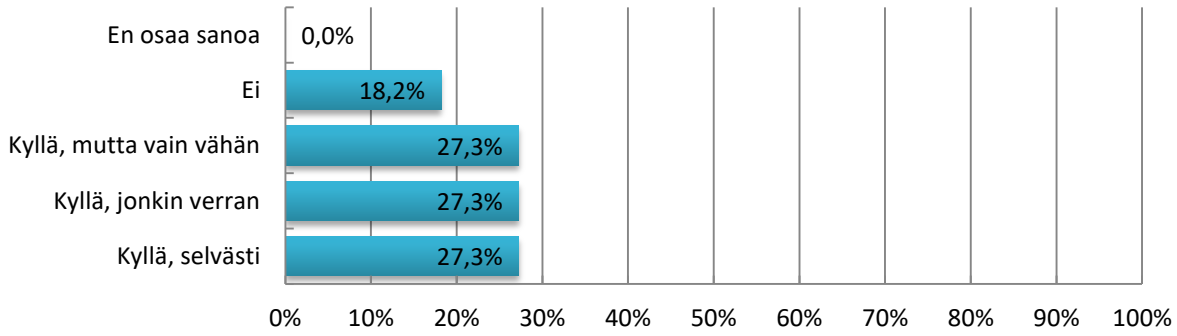
5.2.4 Asetuksen Sopimusvaatimukset

Neljännessä osiossa selvitettiin artiklan 28 mukaisten Sopimusvaatimusten vaikutuksia yritysten sopimusneuvotteluihin. Kysymyksillä pyrittiin selvittämään, mistä seikoista Sopimusvaatimusten mahdollisesti aiheuttama hallinnollinen taakka syntyy, miten yritykset suhtautuvat Tietojenkäsittelysopimuksiin sekä sitä, miten yritykset kokevat Asetuksen mahdollistamat, sopimusneuvotteluita tukevat mekanismit.

Ensimmäisessä kysymyksessä selvitettiin, ovatko Sopimusvaatimukset vaikuttaneet yritysten välisiin sopimusneuvotteluihin. Toinen kysymys oli jatkokysymys edelliseen, mikäli vastaaja vastasi Sopimusvaatimusten vaikuttaneen Sopimusneuvotteluihin. Tällöin tuli arvioida valmiista vastausvaihtoehdoista niitä asioita, jotka olivat vaikuttaneet sopimusneuvotteluihin. Viimeisenä vaihtoehtona tarjottiin vaihtoehtoa *”muuten, miten”*, jolloin yrityksillä oli mahdollisuutena antaa sanallinen vastaus. Vastaajan oli mahdollista valita useampi vastausvaihtoehto. Kolmannessa kysymyksessä selvitettiin vastaajien arviota Sopimusvaatimusten vaikutuksista Tietojenkäsittelysopimuksiin tulevaisuudessa, jossa valmiiden vastausvaihtoehtojen lisäksi oli mahdollista antaa sanallinen vastaus kohdassa *”muuten, miten”*. Vastaajan oli

mahdollista valita useampi vastausvaihtoehto. Neljännellä kysymyksellä selvitettiin yritysten suhtautumista sopimusneuvotteluissa hyödynnettäviin mekanismeihin ja sitä, kuinka todennäköisesti niitä käytettäisiin. Viidennellä kysymyksellä selvitettiin Sopimusvaatimusten aiheuttamia mahdollisia palvelusopimusten hintojen muutoksia. Viimeisen kysymyksen tarkoitus oli selvittää yritysten kokemukset sanktiouhan vaikutuksesta ennaltaehkäisevässä riskienhallinnassa. Kolmessa viimeisessä kysymyksessä vastaajilla oli mahdollista valita vain yksi vastausvaihtoehto.

Ensimmäisessä kysymyksessä suurin osa vastaajista (82,8 %) arvioi, että Asetuksen Sopimusvaatimukset ovat vaikuttaneet sopimusneuvotteluihin. Nämä vastaukset jakaantuivat tasaisesti ”*kyllä, selvästi*”, ”*kyllä, jonkin verran*”, ”*kyllä, mutta vain vähän*” vaihtoehtojen välille. Muutama vastaaja arvioi, ettei Sopimusvaatimuksilla ole ollut vaikutusta aikaisempaan verrattuna. (Taulukko 6)

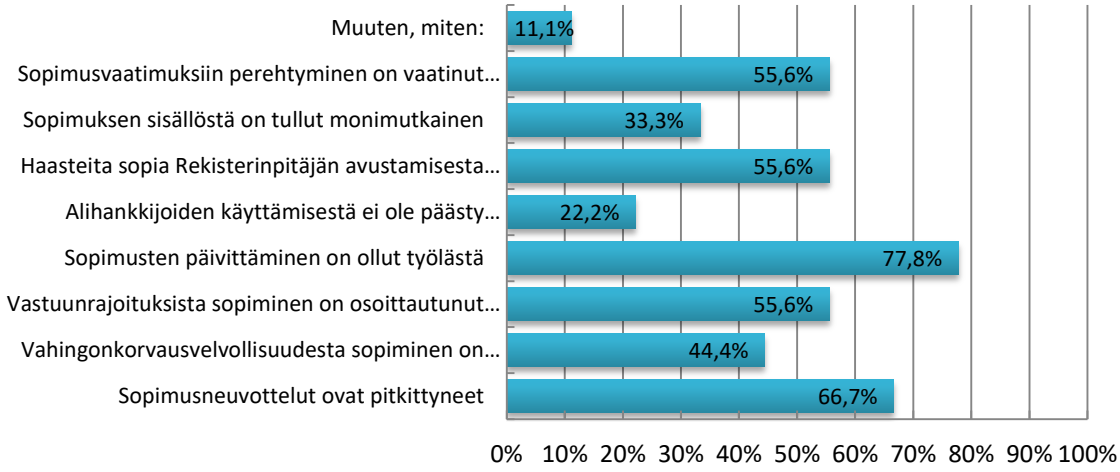


Taulukko 6. Sopimusvaatimusten vaikutus sopimusneuvotteluihin.

Toisessa kysymyksessä ne yritykset, jotka arvioivat Sopimusvaatimusten vaikuttaneen heidän sopimusneuvotteluihin, pyydettiin kertomaan miten vaikutukset ovat ilmenneet. Yli puolet vastaajista arvioi, että sopimusneuvottelut, ovat pitkittyneet, vastuunrajoituksista sopiminen on osoittautunut haastavaksi, olemassa olevien sopimusten päivittäminen on ollut työlästä, on ollut haasteita sopia Rekisterinpitäjän avustamisesta koituvien kustannusten korvaamisesta ja Sopimusvaatimuksiin perehtyminen on vaatinut paljon valmistelua (jakauma 55,6 % - 77,8 %). Osa vastaajista arvioi myös, että vahingonkorvausvelvollisuudesta sopiminen on vienyt aikaa, alihankkijoiden käyttämisestä ei ole päästy yhteisymmärrykseen ja sopimuksen sisällöstä on tullut monimutkainen (jakauma 22,2 % -44,4 %). (Taulukko 7) Lisäksi yksi vastaaja kertoi Sopimusvaatimusten aiheuttaneen muita vaikutuksia sopimusneuvotteluihin, kuin

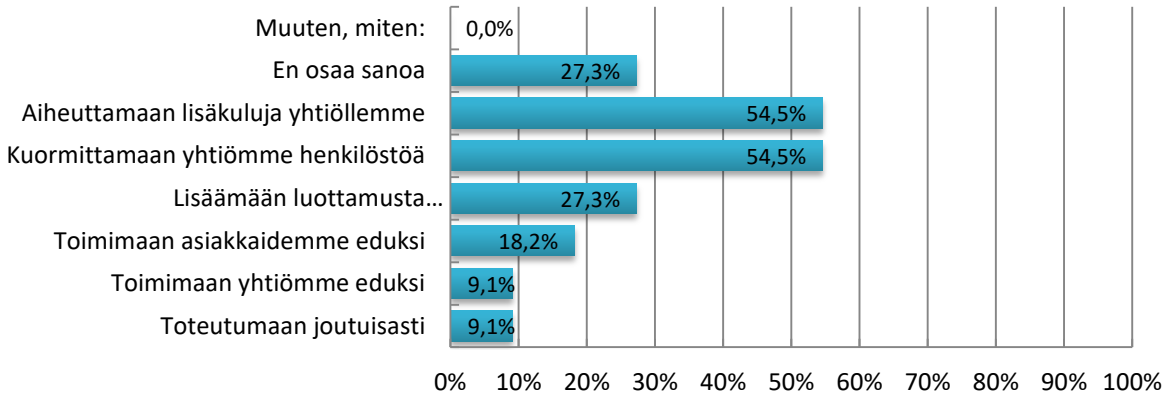
valmiiksi annetuissa vaihtoehdoissa oli valittavana. Vastaaja antoi tällöin avoimeen vastauskenttään vastaukseksi:

> ”*Asetuksen tulkinnasta vallitsee epäselvyyttä ja erimielisyyttä, mikä pitkittää neuvotteluja. Liitteiden määrä on lisääntynyt*”.



Taulukko 7. Sopimusvaatimusten ilmeneminen yrityksen sopimusneuvotteluissa.

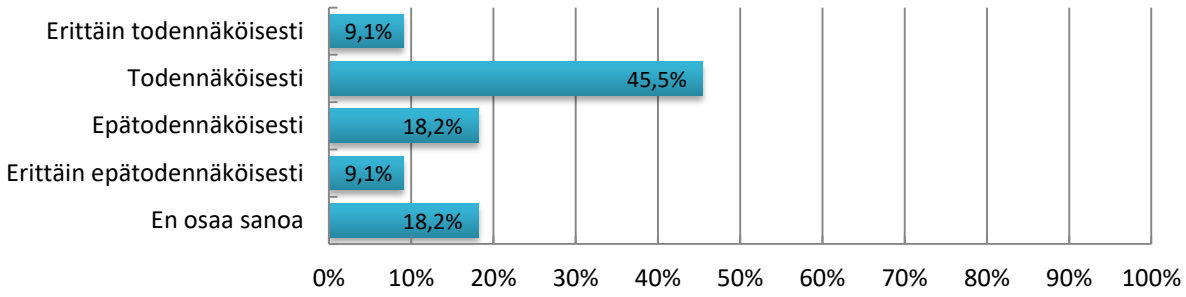
Kolmannessa kysymyksessä selvitettiin yritysten näkemyksiä Sopimusvaatimusten vaikutuksista Tietojenkäsittelysopimuksiin tulevaisuudessa. Vastaajien mielestä Sopimusvaatimukset tulevat jatkossakin kuormittamaan yrityksiä sekä aiheuttamaan lisäkuluja (54,5 %). Sopimusvaatimuksista koettiin olevan myös hyötyä; osa vastaajista arvioi, että Tietojenkäsittelysopimukset tulevat vaatimusten myötä toteutumaan joutuisasti, toimimaan vastanneen yrityksen ja sen asiakkaiden eduksi, sekä lisäämää luottamusta vastanneiden yritysten sopimuskumppaneita kohtaan (jakauma 9,1 % -27,3 %). Loput vastaajista (27,3 %) eivät osanneet arvioida Sopimusvaatimusten vaikutuksia Tietojenkäsittelysopimuksiin. (Taulukko 8)



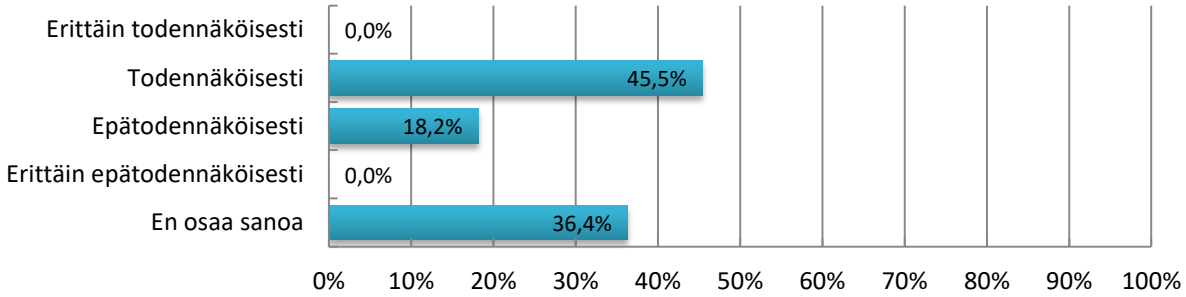
Taulukko 8. Yrityksen uskomukset Sopimusvaatimusten vaikutuksista Tietojenkäsittelysopimuksiin tulevaisuudessa.

Neljännessä kysymyksessä selvitettiin vastaajien suhtautumista sopimusneuvotteluissa hyödynnettäviin mekanismeihin, joita ovat hyväksytyt käytännesäännöt, sertifiointimekanismi ja vakiosopimuslausekkeet. Kysymys oli esitetty niin, että vastaajan tuli arvioida, kuinka todennäköisesti yrityksessä hyödynnettäisiin edellä mainittuja keinoja. Vastaukset tuli antaa asteikolla ”*Erittäin todennäköisesti” – ”Todennäköisesti” – ”Epätodennäköisesti” – ”Erittäin epätodennäköisesti” –* ”*En osaa sanoa*”.

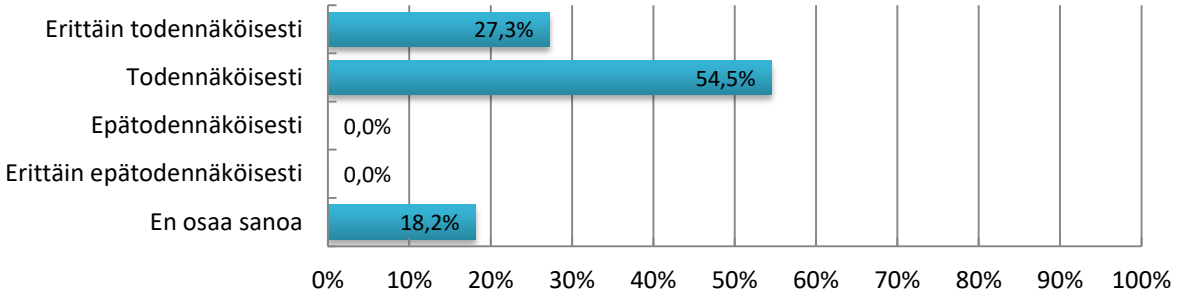
Vastaukset jakaantuivat seuraavalla tavalla: yli puolet vastaajista olisi valmis hyödyntämään käytännesääntöjä todennäköisesti tai erittäin todennäköisesti (54,6 %). Vähemmistö (27,3 %) vastaajista arvioi käytännesääntöjä hyödynnettävän epätodennäköisesti tai erittäin epätodennäköisesti. Loput (18,2 %) eivät osanneet sanoa hyödynnettäisiinkö käytännesääntöjä. (Taulukko 9) Sertifiointimekanismien osalta vastaajista hieman alle puolet (45,5 %) arvioivat, että sertifiointia hyödynnettäisiin todennäköisesti. Osa (18,2 %) vastaajista arvioi, että sertifiointimekanismeja käytettäisiin epätodennäköisesti. Yli kolmannes vastaajista ei osannut sanoa, hyödynnettäisiinkö sertifiointimekanismeja yrityksessä lainkaan (36,4 %). (Taulukko 10) Vakiosopimuslausekkeiden osalta lähes kaikki (81,8 %) yritykset hyödyntäisivät niitä sopimusneuvotteluissa todennäköisesti tai erittäin todennäköisesti. Vähemmistö (18,2 %) vastaajista ei osannut sanoa käyttäisivätkö he vakiosopimuslausekkeita sopimusneuvotteluissa. (Taulukko 11)



Taulukko 9. Käytännesäännöt.

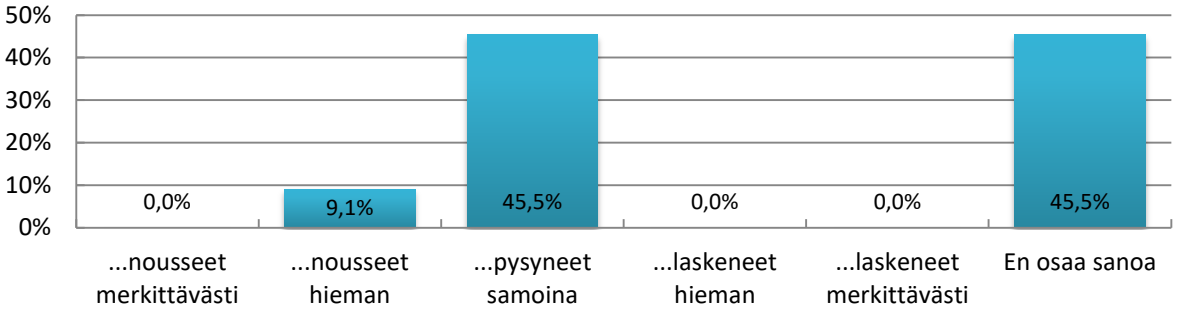


Taulukko 10. Sertifiointimekanismit.



Taulukko 11. Vakiosopimuslausekkeet.

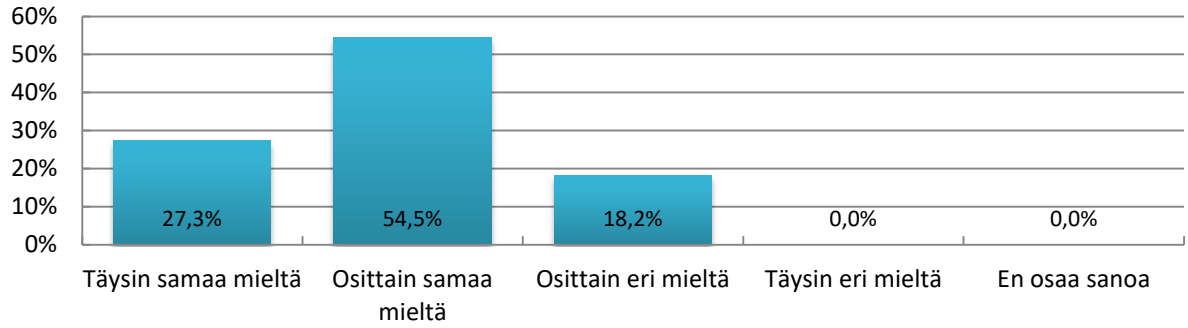
Viidennessä kysymyksessä selvitettiin palvelusopimusten hintojen muutosta. Vastaajien tuli jatkaa lausetta: *”henkilötietojen käsittelyn palvelusopimusten hinnat ovat Sopimusvaatimusten voimaantulon myötä…”* valmiiksi annettujen vastausvaihtoehtojen avulla. Lähes puolet (45,5 %) vastaajista arvioi, että palvelusopimusten hinnat olisivat pysyneet samoina Sopimusvaatimusten voimaantulon myötä. Toisaalta saman verran vastaajista eivät osanneet arvioida palvelusopimusten hintojen muutoksia. Yhden vastaajan mukaan hinnat ovat nousseet hieman (9,1 %). (Taulukko 12)



Taulukko 12. Palvelusopimusten hintojen muutos.

Viidennessä kysymyksessä yritysten tuli arvioida väitettä *”merkittävä sanktiouhka lisää ennaltaehkäisevän riskienhallinnan taloudellista panostusta”* valmiiden vastausvaihtoehtojen avulla. Vastaajista 81,8 % oli joko täysin samaa tai osittain samaa mieltä. Vain yksi vastaaja oli osittain eri mieltä väitteen kanssa. (Taulukko 13) Mielenkiintoista tässä on se, että eriävän mielipiteen sanonut vastaaja on myös ainoa Suomen ulkopuolelle kotipaikkansa ilmoittanut yritys.[315]

[315] Olisi mielenkiintoista selvittää tarkemmin eroavatko suomalaisten ja ruotsalaisten näkemykset sanktioiden ennaltaehkäisevästä vaikuttavuudesta myös laajemmin oikeusteoreettisella tasolla. Vaikka Ruotsin ja Suomen oikeusjärjestelmät ja yhteiskuntarakenteet ovat samankaltaisia, voiko erilaiset asenteet vaikuttaa yritysten mark-



Taulukko 13. Sanktiouhan vaikutus taloudelliseen panostukseen.

Neljännen osion vastausten perusteella on nähtävissä, että valtaosa yrityksistä koki Sopimusvaatimusten vaikuttaneen heidän sopimusneuvotteluihinsa. Mielenkiintoista oli, että kyselyyn vastanneet yritykset eivät nähneet juurikaan positiivisia vaikutuksia kysyttäessä heidän näkemyksiään Tietojenkäsittelysopimuksista tulevaisuudessa. Yritysten mukaan Tietojenkäsittelysopimukset tulevat tulevaisuudessa lähinnä kuormittamaan ja aiheuttamaan yrityksille lisäkuluja. Kysyttäessä sopimusneuvotteluita tukevista mekanismeista, vastaajista hieman yli puolet arvioi, että yritys tulisi hyödyntämään niitä. Mekanismeista korostui erityisesti vakiosopimuslausekkeet, joita selkeästi yli puolet vastaajista hyödyntäisi todennäköisesti tai erittäin todennäköisesti.[316]

Vastauksista voineekin päätellä, että Sopimusvaatimusten toteuttamista tukevat mekanismit ovat yrityksissä kaivattuja ja niiden avulla vaatimusten aiheuttama kuorma voisi keventyä. Tukevat mekanismit saattaisivat parhaimmillaan keventää sopimusneuvotteluita, mahdollisesti pienentämällä neuvotteluihin käytettyä aikaa, keventämällä niihin sidottuja resursseja, vaikuttaen siten myös positiivisesti Tietojenkäsittelysopimusten aiheuttamiin kuluihin. Huomattavaa kuitenkin on, että kyselyn vaihtoehdot sopimusneuvotteluihin vaikuttaneista seikoista, iso osa käsitteli aihealueita, jotka saattaisivat aiheuttaa haasteita, vaikka mekanismeja hyödynnettäisiinkin. Esimerkiksi vakiosopimuslausekkeiden hyödyntäminen ei välttämättä aina poista tarvetta neuvotella toisin muun muassa vastuunrajoituksista tai vahingonkorvausvelvollisuudesta. Sopimusvaatimusten haasteet voivat vaihdella paljonkin eri sopimusten välillä.

kinakäyttäytymiseen. Yleisesti Ruotsista oikeudellisena lähteenä, Ks. *Eduskunta* 2019b, kohta Ruotsi – oikeudellisia tiedonlähteitä.

[316] Huomioitava, että jokaisen mekanismin kohdalla vähintään kaksi vastaajaa ei osannut arvioida tarjotun vaihtoehdon käytettävyyttä yrityksessä. Voitanee arvioida, etteivät kaikki vastaajat välttämättä olleet tietoisia mekanismien sisällöstä tai niiden mahdollistamasta avusta sopimusneuvotteluissa. Jääkin nähtäväksi miten viranomaiset täyttävät velvollisuutensa kannustaa, avustaa ja tiedottaa näistä mahdollisuuksista jos ja kun mekanismit lopulta jalkautetaan yrityksille hyödynnettäviksi.

Vastanneiden yritysten vastausten perusteella, tukevat mekanismit, erityisesti vakiosopimuslausekkeet olisivat kuitenkin kaivattu lisä, ja toimisivat siten varmasti hyvänä sopimusneuvotteluiden aloitusrunkona.

Myös Asetuksen aiheuttama merkittävä sanktiouhka on vastaajien mielestä aiheuttanut taloudellista panostusta ennaltaehkäisevän riskienhallinnan vuoksi. Tämän voidaan arvioida johtuvan muun muassa merkittävän korkeiden sanktioiden ennaltaehkäisevästä vaikutuksesta tai pyrkimyksestä välttää tietosuojaloukkausten aiheuttamia mainehaittoja.

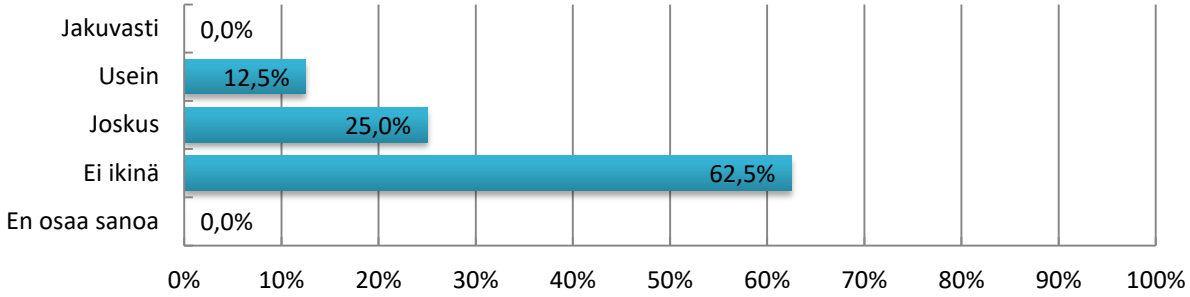
Vaikka edellä on nähtävissä, että Asetus on aiheuttanut kuormaa ja tämän myötä oletettavia kuluja yrityksille, vastaajat arvioivat, että palvelusopimusten hinnat ovat pysyneet samoina tai asiaa ei osattu arvioida. Koska kyselyssä pyydettiin vastaajilta parasta arviota vastauksissa tarkkojen lukujen sijaan, voitanee arvioida, etteivät vastaajat ole palvelusopimusten hintojen kanssa tekemisissä tai Asetuksen aiheuttamat kulut ja niiden kattaminen on siirretty muualle kuin palvelusopimusten hintoihin. Palvelusopimustenhintoja koskevaan kysymykseen voi myös suhtautua kriittisesti sen moniulotteisuuden vuoksi. Jotta kysymykseen on annettavissa edes karkea arvio toteutuneista hinnoista, vaatii se vastaajalta hyvin laajaa tuntemusta ja tietämystä yrityksen sopimuksista. Käytännössä yritysten sopimusten hallinta toteutetaan kuitenkin niin sanotusti tiimi-jakoisesti tai yksittäisten myyjien toimesta, tarkoittaen etteivät palvelusopimusten tapauskohtaiset ehdot ja hinnat ole varsinkaan isoissa yrityksissä laajasti tiedossa tai edes mahdollista jälkikäteen selvittää. Palvelusopimusten hintojen tarkempi selvittäminen vaatisikin yrityksissä ennakollista ja laajaa tiedottamista ennen empiirisen tutkimuksen aloittamista.

5.2.5 Kysymykset Henkilötietojen käsittelijöille

Kyselyn viimeinen osio oli suunnattu niille vastaajille, jotka käsittelevät henkilötietoja myös Henkilötietojen käsittelijöinä. Kysymysten tarkoituksena oli selvittää tarkemmin Henkilötietojen käsittelijöille kohdistunutta taakka Sopimusvaatimuksista johtuen.

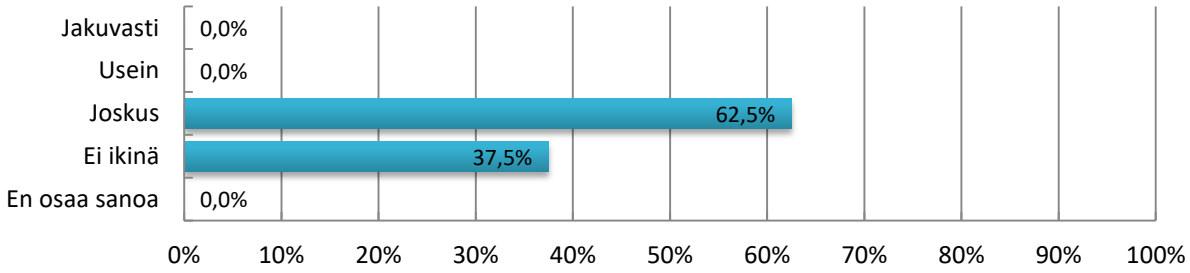
Kysymys on kolmiosainen ja sillä oli tarkoitus selvittää, kuinka usein yritys on tukenut Rekisterinpitäjiä erilaisissa tehtävissä. Artiklan 28 mukaisesti, näitä tehtäviä ovat Rekisteröityjen tietosuojapyynnöt, henkilötietojen tietoturvaloukkausten käsittely ja tietosuojaa koskevan vaikutusten arvioinnin toteuttaminen. Kyselyn tähän osioon vastasi kahdeksan yritystä.

Rekisteröityjen tietopyynnöissä 37,5 % yrityksistä oli tukenut Rekisterinpitäjiä usein tai joskus, mutta valtaosa vastaajista, eli 62,5 % ei ollut joutunut tukemaan Rekisterinpitäjiä ikinä Rekisteröityjen tietopyynnöissä (Taulukko 14). Kysymyksessä ei kysytty tarkemmin, millaista tukea Henkilötietojen käsittelijöiltä oli tosiasiassa pyydetty.



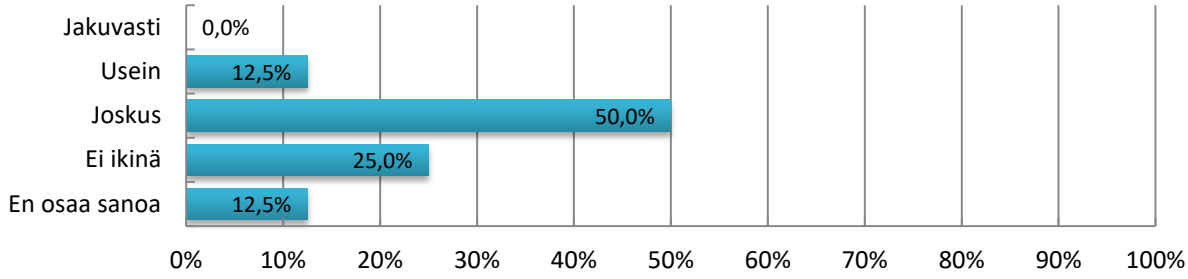
Taulukko 14. Rekisteröityjen tietopyynnöt.

Seuraavaksi vastaavasti selvitettiin, kuinka usein Henkilötietojen käsittelijöiden tukea on tarvittu henkilötietojen tietoturvaloukkausten käsittelyssä. Valtaosa vastaajista (62,5 %) oli joskus joutunut antamaan tukensa Rekisterinpitäjälle, kun taas loput vastaajista, eli 37,5 % ei ikinä (Taulukko 15).



Taulukko 15. Henkilötietojen tietoturvaloukkausten käsittely.

Osiossa viisi ja koko kyselyn viimeisessä kysymyksessä kysyttiin Henkilötietojen käsittelijän tukea tietosuojaa koskevan vaikutusarvioinnin toteuttamisessa. Yli puolet, eli 62,5 % vastaajista oli tukenut Rekisterinpitäjää usein tai jatkuvasti, 25 % ei ikinä ja loput, eli 12,5 % eivät tienneet oliko tukea jouduttu joskus antamaan (Taulukko 16).



Taulukko 16. Tietosuojaa koskevan vaikutusarvioinnin toteuttaminen.

Viidennen osion vastauksista on nähtävissä, että Henkilötietojen käsittelijöille ei ole vielä syntynyt merkittävää kuormaa Tietojenkäsittelysopimuksista. Kuitenkin vastaajat olivat antaneet tukeaan Rekisterinpitäjille vähintään joskus kaikissa tarjotuissa vaihtoehdoissa. Muita erityisiä johtopäätöksiä vastauksista ei ole tehtävissä.

5.3 Yhteenveto

Valtaosa vastanneista yrityksistä toimii sekä Rekisterinpitäjänä että Henkilötietojen käsittelijänä. Henkilötietojen käsitteleminen molemmissa rooleissa kertonee henkilötietojen käsittelyn moniulotteisesta rakenteesta, sekä siitä miten henkilötietojen käsittely käytännössä toteutetaan. Vaikkakin henkilötietojen käsittelyn tarve, hyöty ja velvoite voivat erota yritysten välillä suuresti, yritykset ovat silti monessa tapauksessa velvoitettuja toimimaan samojen säännösten mukaisesti. Tämä tarkoittaa käytännössä sitä, että esimerkiksi logistiikka-alan yritys, jonka toimenkuva on tarjota palveluitaan toisille yrityksille, ovat luultavasti samojen tietosuojasäännösten vuoksi velvollisia noudattamaan Asetusta kuin teknologia-alan yritys, jonka pääasiallinen toimenkuva rakentuu yksityisten henkilötietojen keräämisestä ja käsittelystä. Oleellista on siten henkilötietojen tosiasiallinen käsittely, ei käsittelyn luonne. Kyselyn tuloksista onkin nähtävissä, että kaikissa vastanneissa yrityksissä käsitellään paljon erilaisia henkilötietoja – riippumatta yrityksen toimialasta.

Vastausten perusteella valtaosa yrityksistä käsittelee henkilötietoja rajatylittävinä siirtoina. Kyselyn tuloksista on kuitenkin nähtävissä, että Sopimusvaatimusten vaikutukset yritysten sopimusneuvotteluihin korostuvat yrityksissä, jotka käsittelevät henkilötietoja rajatylittävinä siirtoina myös kolmansissa maissa. EU rajojen ulkopuolella käytävien sopimusneuvotteluiden haasteet näkyvät myös samaisten yritysten vastuksissa kysyttäessä heiltä heidän näkemyksiään Tietojenkäsittelysopimusten tulevista vaikutuksista. Lähes kaikki yritykset, jotka käsittelevät henkilötietoja myös kolmansissa maissa uskovat, että Tietojenkäsittelysopimukset tule-

vat tulevaisuudessa kuormittamaan heidän henkilöstöä ja aiheuttamaan lisäkuluja yritykselle. Vastaukset ilmentävät mahdollisesti jo koettua taakkaa; kaikkien vastanneiden yritysten mukaan henkilötietojen käsittelystä johtuva hallinnollinen taakka on kasvanut Asetuksen voimaan tulon myötä.[317] Oletettavasti hallinnollisen taakan kasvulla viitataan myös nousseisiin kuluihin. Mielenkiintoista kuitenkin oli, että vastausten perusteella palvelusopimusten hinnat eivät kuitenkaan ole nousseet. Voi myös olla, että on liian aikaista kysyä hallinnollisen taakan tulouttamisesta, sillä yrityksillä ei välttämättä ole vielä selvillä mitkä ja miten paljon Asetuksen velvoitteet aiheuttavat kuormaa heidän toiminnalleen. Kyselyssä yritykset arvioivat, että sopimusneuvotteluiden lisäksi hallinnollista taakkaa ovat aiheuttaneet myös Asetuksen vaatimusten selvittäminen, henkilötietojen käsittelyyn liittyvien riskien kartoittaminen sekä organisatoriset toimet. Myös Asetuksen merkittävän sanktiouhan nähtiin lisäävän taloudellista panostusta riskienhallintaan. Joten on mahdollista, että Asetuksen ja Sopimusvaatimusten aiheuttamat lisäkulut on siirretty henkilöstön koulutuksiin tai esimerkiksi uusien rekrytointeihin. Tutkielman kannalta merkittävä huomio oli, että valtaosa vastaajista arvioi Asetuksen aiheuttaman taakan johtuvan Sopimusvaatimuksista (26 – 75 %).

Valtaosa vastanneista yrityksistä koki Sopimusvaatimusten vaikuttaneen heidän neuvotteluihinsa haitallisesti. Mahdollisesti tästä johtuen, sopimusneuvotteluita tukevia mekanismeja kaivattiin monessa yrityksessä. Erityisesti vakiosopimuslausekkeet saivat eniten kannatusta. Vakiosopimuslausekkeiden korkea kannatus vahvistanee kyselystä saatuja tuloksia sopimusneuvotteluiden aiheuttamasta taakasta. Vakiosopimuslausekkeet voisivatkin parhaimmillaan keventää sopimusneuvotteluita karsien pois hienosäädön koskien lausekkeita, joista osapuolilla ei ole erimielisyyttä, jättäen jäljelle tapauskohtaiset erikoisuudet ja Sopimusvaatimusten ulkopuoliset sopimusvapauden piirissä olevat seikat. Lisäksi, Asetuksen tarkoituksena on yhtenäistää EU:n tietosuojakäytäntöjä, on mielenkiintoista, että yhdessä vastauksessa nimenomaisesti Asetuksen vaihtelevan tulkinnan nähtiin hidastavan sopimusneuvotteluita. Sääntelyn tulkinnan haastavuudesta johtuen, onkin ymmärrettävää, ettei Sopimusvaatimuksia välttämättä nähdä osapuolia tukevana instrumenttina, jolla selkeytetään Rekisterinpitäjän lukuun tehtävää henkilötietojen käsittelyä.

[317] Kyselyn ymmärrettävyyden varmistamiseksi, yrityksille annettiin kyselyn alustuksessa ohjeistus ja kuvaus hallinnollisen taakan käsitteestä, Ks. tutkielman liite 2 ja 3.

Koska kyselyyn saatiin vastauksia melko niukasti, verraten koko yrityskentän suuruuteen[318], ei vastausten perusteella voida tehdä yleistettävissä olevia johtopäätöksiä. Kyselyn onnistumisen näkökulmasta olisi ollut arvokasta saada tietoon, kuinka moni on keskeyttänyt kyselyyn vastaamisen. Tämän perusteella olisi voinut tehdä johtopäätöksiä kyselyn haastavuudesta ja nähdä onko mahdollisesti jokin tietty kysymys vaikuttanut yritysten vastaushalukkuuteen. Vastausmäärän lisäämiseksi kirjoittaja olisi voinut toimia myös aggressiivisemmin, pyrkimällä lähestymään henkilökohtaisesti useampaa yritystä ja mainostamalla kyselyä aktiivisemmin sosiaalisessa mediassa. Kyselyn tulosten hyödyntämistä olisi voinut parantaa kohdistamalla kysely yhdelle toimialalle, jolloin vastaukset olisivat olleet suoraan verrattavissa toisiinsa. Tulosten taso olisi myös korkeampi, jos kysymykset olisi esitetty tarkempina ja vastaukseksi olisi saatu tarkkoja ja euromääräisiä lukuja yritysten Asetukseen ja Sopimusvaatimuksiin kohdistuneista kuluista. Kysely haluttiin kuitenkin jättää suuntaa-antavaksi, jotta yritysten vastauskynnys ei nousisi liian suureksi.

[318] Suomessa oli vuonna 2017 yhteensä 286 934 yritystä pois lukien maa-, metsä- ja kalatalous. *Suomen Yrittäjät* 2019, kohta Yrittäjyys Suomessa.

6 JOHTOPÄÄTÖKSET

Asetuksen 28 artiklan mukaan, jos henkilötietojen käsittely suoritetaan Rekisterinpitäjän lukuun, asianosaisten yritysten on laadittava käsittelystä kirjallinen sopimus. Lisäksi Rekisterinpitäjänä toimivan yrityksen tulee varmistaa, että valittu Henkilötietojen käsittelijä täyttää Asetuksen vaatimukset toteuttamalla riittävät suojatoimet asianmukaisten teknisten ja organisatoristen toimien täytäntöönpanemiseksi (artikla 28.1). Rekisterinpitäjän ja Henkilötietojen käsittelijän tulee vahvistaa Tietojenkäsittelysopimuksella Asetuksenmukaiset Sopimusvaatimukset koskien käsittelyn kohdetta ja kestoa, käsittelyn luonnetta ja tarkoitusta, henkilötietojen tyyppiä, Rekisteröityjen ryhmiä, Rekisterinpitäjän velvollisuuksia ja oikeuksia, sekä Henkilötietojen käsittelijältä vaadittavia toimia (28.3 artiklan (a-h) alakohdat). Sopimusvaatimusten tarkoituksena on suojella Rekisteröityjen oikeuksia ja varmistaa osapuolten keskinäinen ymmärrys vaadittavista konkreettisista toimista. Tietojenkäsittelysopimusten avulla osapuolten väliset vastuut ja riskien jakaantuminen ovat myös läpinäkyvämmin osoitettavissa[319]. Sopimusvaatimusten noudattamisen tärkeyttä korostaa Asetuksen 83.4 artiklan asettama hallinnollinen sakko, joka voi olla sopimusrikkomuksen laiminlyönnistä enintään 10 miljoonaa euroa, tai 2 % yrityksen edeltävän tilikauden vuotuisesta maailmanlaajuisesta kokonaisliikevaihdosta sen mukaan, kumpi näistä määristä on suurempi.

Sopimusvaatimusten noudattaminen vaatii yrityksiltä huomattavaa perehtymistä vaatimusten sisältöön ja käytännön toteuttamiseen - niin organisatorisella kuin sopimusteknisellä tasolla. Merkittävä huomio Sopimusvaatimusten toteuttamisessa on sääntelyn eräänlainen taannehtiva vaikutus myös vanhoihin, voimassaoleviin henkilötietojen käsittelyä koskeviin sopimuksiin. Tietojenkäsittelysopimusten päivittäminen, uusien neuvotteleminen, valvonta ja hallinta voivatkin aiheuttaa merkittäviä vaikutuksia yritysten toiminnalle. Yritysvaikutusten selvittäminen onkin otettu osaksi sääntelyn valmistelua ja täytäntöönpanoon kuuluvaa vaikutusarviointia. Yritysvaikutuksia selvitetään markkinoiden toimivuuden ja yritysten kilpailukyvyn varmistamiseksi. Yritysvaikutusten arviointi jakaantuu eri vaiheisiin, alkaen säädösehdotuksen valmistelusta, jatkuen lopulta lain täytäntöönpanon jälkiseurantaan.[320] Yritysvaikutuksia arvioitaessa tarkastellaan erityisesti sääntelyn toteuttamisvaihtoehtojen vaikutuksia yritysten hallinnolliseen taakkaan – esimerkiksi sääntelyn aiheuttamiin kustannuksiin tai tuottoihin, vaikutuksia pieniin tai keskisuuriin yrityksiin, yritystoiminnan aloittamiseen ja yritysten kas-

[319] *Lilja* 2019, s. 213.
[320] Ks. tutkielman kuva 1.

vumahdollisuuksiin, investointeihin ja innovointiin, sekä mahdollisia vaikutuksia yritysten kansainväliseen kilpailukykyyn.[321]

Asetuksen vaikutusarviointi on tutkielman kirjoituksen päättyessä jälkiseuranta vaiheessa. Oikeusministeriö on kerännyt kokemuksia Asetuksen toimivuudesta kansallisilta etujärjestöiltä ja viranomaisilta. Annettujen lausuntojen mukaan, Sopimusvaatimusten noudattaminen on osoittautunut haastavaksi. Haasteita koettiin erityisesti Tietojenkäsittelysopimusten laadinnassa, jossa erityisesti vastuista sopiminen sekä Rekisterinpitäjä-käsittelijäsuhteiden määrittely on osoittautunut työlääksi. Myös yritykseltä vaadittu alihankintaketjun selvittämisvelvollisuuden toteuttaminen kyseenalaistettiin haastavana ja jopa mahdottomana ketjuutuvien sopimusjärjestelyiden kattaessa kymmeniä ja jopa satoja alihankittuja Henkilötietojen käsittelijöitä[322]. Sopimusvaatimusten vuoksi vastaajat ovat joutuneet turvautumaan myös ulkopuolisten asiantuntijoiden apuun. Oikeusministeriölle annettuja lausuntoja vahvistavat komission asiantuntijaryhmän näkemykset Sopimusvaatimuksista. Myös komission asiantuntijaryhmän mukaan Tietojenkäsittelysopimuksia koskevat sopimusneuvottelut ovat olleet aikaa vieviä ja pitkiä prosesseja, sekä Rekisterinpitäjä-käsittelijäsuhteiden määrittely on aiheuttanut epäselvyyttä.

Tutkielmassa toteutetun kyselytutkimuksen mukaan, käsittelystä johtuva hallinnollinen taakka on kasvanut Asetuksen voimaan tulon myötä. Sopimusvaatimusten osuus Asetuksen yrityksille aiheuttamasta hallinnollisesta taakasta on vastausten perusteella huomattava. Vastauksista on tulkittavissa, että Tietojenkäsittelysopimusten laadinta on ollut haasteellista ja sitonut yritysten resursseja. Vastanneiden yritysten mukaan, Sopimusvaatimukset ovat vaikuttaneet yritysten välisiin neuvotteluihin negatiivisesti, muun muassa vaikeuttamalla vastuukysymyksistä sopimista ja pitkittämällä sopimusneuvotteluiden kestoa. Myös sopimusten päivittäminen Asetuksenmukaisiksi on ollut työlästä. Lisäksi Rekisterinpitäjän avustamisesta koituvien kustannusten korvaamisesta sopiminen on ollut haastavaa ja Sopimusvaatimuksiin perehtyminen on vaatinut paljon valmistelua. Sopimusvaatimusten vaikutukset korostuivat erityisesti yrityksissä, jotka käsittelivät henkilötietoja rajatylittävinä siirtoina myös kolmansissa maissa. Kansainvälisten yritysten kokemukset Sopimusvaatimusten aiheuttamasta taakasta ilmenee myös heidän tulevaisuudennäkemyksistään; heidän mukaansa Tietojenkäsittelysopimukset tulevat

[321] *Oikeusministeriö* 2007, s. 18–21.
[322] Kuten Konttinen Senaatti-Kiinteistöiltä asian ilmaisee. *Oikeusministeriön selvitys* 2019, kohta Lausunnonantajien lausunnot.

myös tulevaisuudessa kuormittamaan heidän henkilöstöä ja aiheuttamaan lisäkuluja yritykselle.

Sopimusvaatimusten aiheuttaman taakan keventämiseksi, yritykset olivat kiinnostuneita erityisesti vakiosopimuslausekkeiden hyödyntämisestä. Vastausten mukaan vakiosopimuslausekkeet saattaisivat keventää sopimusneuvotteluita ja edesauttaa osoitusvelvollisuuden toteuttamista. Vakiosopimuslausekkeiden uskottiin vähentävän Tietojenkäsittelysopimusten yrityksille aiheuttamaa kuormaa. Lisäksi sopimusosapuolien tarkempi määrittäminen viranomaisohjein korostui kaikissa selvityksissä. Epäselvyydet säännöksen sisällöstä ja tulkinnasta vaikeuttaa lain soveltamista käytännössä, aiheuttaen ylimääräisiä kustannuksia sekä Sopimusvaatimuksiin nähden virheellisiä sopimuksia. Lisäksi, Oikeusministeriön saamissa lausunnoissa tuotiin esille epäilyksiä siitä, että riskiperusteinen sopiminen nostaisi tietojenkäsittelyä koskevien palvelusopimusten hintoja. Kyselytutkimuksen mukaan tällaista ei kuitenkaan ole vielä havaittu. Se, nousevatko palvelusopimusten hinnat tulevaisuudessa, kun yrityksille selviää tarkemmin Sopimusvaatimusten aiheuttamat kustannukset, ratkeaa ajan kuluessa. Palvelusopimusten mahdollista hintojen nousua voitaisiin pyrkiä myös ennaltaehkäisemään mainittujen vakiosopimuslausekkeiden ja viranomaisohjeistusten avulla.

Selvitysten perusteella Sopimusvaatimukset kuormittavat Suomessa toimivien yritysten toimintaa ja kasvattavat yrityksiin kohdistunutta hallinnollista taakkaa ja compliance-kustannuksia. Asetuksen ja Sopimusvaatimusten yritysvaikutukset ovat selvitysten valossa merkittäviä, joiden kustannukset yrityksille ovat luultavasti huomattavia. Asetusta koskevien kansallisten arvioiden mukaan, Asetuksen täytäntöönpano on maksanut suurille yrityksille keskimäärin 2,5 miljoonaa euroa. Alkuinvestointien jälkeen kustannusten arvioitiin laskevan 900 000 euron vuositasolle. Mutta ilman määrällisiä tuloksia, Sopimusvaatimusten osuus Asetuksen aiheuttamasta taakasta ja toteutuneista yritysvaikutuksista ovat monessa suhteessa vain arvioita. Vaikka yksilöllisten Tietojenkäsittelysopimusten tarjoaminen voi olla kannattamatonta niin taloudellisesti kuin sopimushallinnankin näkökulmasta, Oikeusministeriön lausunnoissa esiin tulleet huomiot neuvotteluvoiman eriarvoisuuden vaikutuksesta Tietojenkäsittelysopimusten sisältöön antavat aihetta selvittää tarkemmin Sopimusvaatimusten kilpailuoikeudellisia vaikutuksia[323]. Jotta Sopimusvaatimusten vaikutukset kilpailukykyyn ja markkinoiden toimivuuteen voitaisiin selvittää riittävällä tasolla, toteutuneiden yritysvaikutusten selvittämi-

[323] Tietosuojasääntelyn vaikutuksista kilpailupolitiikkaan, sekä kilpailuoikeuden murroksesta ja sen tarpeesta digitaalisen talouden haasteissa Ks. *Wasastjerna* 2019, s. 23–24 ja 29–34.

nen vaatisi kattavaa ja yksityiskohtaisempaa selvitystä yrityskentältä. Yrityksille kohdistunut hallinnollinen taakka tulisi selvittää euromääräisesti, jotta tulokset olisivat vertailukelpoisia keskenään. Ilman määrällistä arviota Sopimusvaatimusten aiheuttamat yritysvaikutukset ovat suuriltaosin vain suuntaa-antavia ja kyseenalaistettavissa vastaajien subjektiivisiksi näkemyksiksi.[324] Selvitys tulisi toteuttaa empiirisenä tutkimuksena jaoteltuna markkina-alojen mukaan, jolloin yritysten kohtaamat vaikutukset ja hallinnollinen taakka olisivat vertailukelpoisia keskenään.

[324] Kuten lainsäädännön arviointineuvoston lausunnossa todetaan; jos toisenlaiset arviot toteutuvat, Asetuksen Suomen 283 000 pk-yritykselle aiheuttamat kokonaiskustannukset voivat olla 850 miljoonaa - 2 miljardia (vrt. komission arvio unionin yrityskentän 2,3 miljardin euron säästöihin). *Lainsäädännön arviointineuvoston lausunto (VNK/133/32/2018)* 2018, s. 4.

LIITTEET

Liite 1. Artikla 28

28 artikla / Henkilötietojen käsittelijä

1. *Jos käsittely on määrä suorittaa rekisterinpitäjän lukuun, rekisterinpitäjä saa käyttää ainoastaan sellaisia henkilötietojen käsittelijöitä, jotka toteuttavat riittävät suojatoimet asianmukaisten teknisten ja organisatoristen toimien täytäntöönpanemiseksi niin, että käsittely täyttää tämän asetuksen vaatimukset ja sillä varmistetaan rekisteröidyn oikeuksien suojelu.*

2. *Henkilötietojen käsittelijä ei saa käyttää toisen henkilötietojen käsittelijän palveluksia ilman rekisterinpitäjän erityistä tai yleistä kirjallista ennakkolupaa. Kun kyse on kirjallisesta ennakkoluvasta, henkilötietojen käsittelijän on tiedotettava rekisterinpitäjälle kaikista suunnitelluista muutoksista, jotka koskevat muiden henkilötietojen käsittelijöiden lisäämistä tai vaihtamista, ja annettava siten rekisterinpitäjälle mahdollisuus vastustaa tällaisia muutoksia.*

3. *Henkilötietojen käsittelijän suorittamaa käsittelyä on määritettävä sopimuksella tai muulla unionin oikeuden tai jäsenvaltion lainsäädännön mukaisella oikeudellisella asiakirjalla, joka sitoo henkilötietojen käsittelijää suhteessa rekisterinpitäjään ja jossa vahvistetaan käsittelyn kohde ja kesto, käsittelyn luonne ja tarkoitus, henkilötietojen tyyppi ja rekisteröityjen ryhmät, rekisterinpitäjän velvollisuudet ja oikeudet. Tässä sopimuksessa tai muussa oikeudellisessa asiakirjassa on säädettävä erityisesti, että henkilötietojen käsittelijä*

   a) *käsittelee henkilötietoja ainoastaan rekisterinpitäjän antamien dokumentoitujen ohjeiden mukaisesti, mikä koskee myös henkilötietojen siirtoja kolmanteen maahan tai kansainväliselle järjestölle, paitsi jos henkilötietojen käsittelijään sovellettavassa unionin oikeudessa tai jäsenvaltion lainsäädännössä toisin vaaditaan, missä tapauksessa henkilötietojen käsittelijä tiedottaa rekisterinpitäjälle tästä oikeudellisesta vaatimuksesta ennen käsittelyä, paitsi jos tällainen tiedottaminen kielletään kyseisessä laissa yleistä etua koskevien tärkeiden syiden vuoksi;*
   b) *varmistaa, että henkilöt, joilla on oikeus käsitellä henkilötietoja, ovat sitoutuneet noudattamaan salassapitovelvollisuutta tai heitä koskee asianmukainen lakisääteinen salassapitovelvollisuus;*
   c) *toteuttaa kaikki 32 artiklassa vaaditut toimenpiteet;*
   d) *noudattaa 2 ja 4 kohdassa tarkoitettuja toisen henkilötietojen käsittelijän käytön edellytyksiä;*
   e) *ottaen huomioon käsittelytoimen luonteen auttaa rekisterinpitäjää asianmukaisilla teknisillä ja organisatorisilla toimenpiteillä mahdollisuuksien mukaan täyttämään rekisterinpitäjän velvol-*

lisuuden vastata pyyntöihin, jotka koskevat III luvussa säädettyjen rekisteröidyn oikeuksien käyttämistä;

f) auttaa rekisterinpitäjää varmistamaan, että 32–36 artiklassa säädettyjä velvollisuuksia noudatetaan ottaen huomioon käsittelyn luonteen ja henkilötietojen käsittelijän saatavilla olevat tiedot;

g) rekisterinpitäjän valinnan mukaan poistaa tai palauttaa käsittelyyn liittyvien palveluiden tarjoamisen päätyttyä kaikki henkilötiedot rekisterinpitäjälle ja poistaa olemassa olevat jäljennökset, paitsi jos unionin oikeudessa tai jäsenvaltion lainsäädännössä vaaditaan säilyttämään henkilötiedot;

h) saattaa rekisterinpitäjän saataville kaikki tiedot, jotka ovat tarpeen tässä artiklassa säädettyjen velvollisuuksien noudattamisen osoittamista varten, ja sallii rekisterinpitäjän tai muun rekisterinpitäjän valtuuttaman auditoijan suorittamat auditoinnit, kuten tarkastukset, sekä osallistuu niihin.

Ensimmäisen alakohdan h alakohdan osalta henkilötietojen käsittelijän on välittömästi ilmoitettava rekisterinpitäjälle, jos hän katsoo, että ohjeistus rikkoo tätä asetusta tai muita unionin tai jäsenvaltion tietosuojasäännöksiä.

4. Kun henkilötietojen käsittelijä käyttää toisen henkilötietojen käsittelijän palveluksia erityisten käsittelytoimintojen suorittamiseksi rekisterinpitäjän puolesta, kyseiseen toiseen henkilötietojen käsittelijään sovelletaan sopimuksen tai unionin oikeuden tai jäsenvaltion lainsäädännön mukaisen muun oikeudellisen asiakirjan mukaisesti samoja tietosuojavelvoitteita kuin ne, jotka on vahvistettu 3 kohdassa tarkoitetussa rekisterinpitäjän ja henkilötietojen käsittelijän välisessä sopimuksessa tai muussa oikeudellisessa asiakirjassa erityisesti antaen riittävät takeet siitä, että käsittelyyn liittyvät asianmukaiset tekniset ja organisatoriset toimet toteutetaan niin, että käsittely täyttää tämän asetuksen vaatimukset. Kun toinen henkilötietojen käsittelijä ei täytä tietosuojavelvoitteitaan, alkuperäinen henkilötietojen käsittelijä on edelleen täysimääräisesti vastuussa toisen henkilötietojen käsittelijän velvoitteiden suorittamisesta suhteessa rekisterinpitäjään.

5. Jäljempänä 40 artiklassa tarkoitettujen hyväksyttyjen käytännesääntöjen tai 42 artiklassa tarkoitetun hyväksytyn sertifiointimekanismin noudattamista voidaan käyttää osatekijänä, jolla osoitetaan, että tämän artiklan 1 ja 4 kohdassa tarkoitetut riittävät takeet on annettu.

6. Sanotun rajoittamatta rekisterinpitäjän ja henkilötietojen käsittelijän yksittäistä sopimusta, tämän artiklan 3 ja 4 kohdassa tarkoitettu sopimus tai muu oikeudellinen asiakirja voi perustua kokonaan tai osittain tämän artiklan 7 ja 8 kohdassa tarkoitettuihin vakiosopimuslausekkeisiin; tämä koskee myös tilannetta, jossa ne ovat osa rekisterinpitäjälle tai henkilötietojen käsittelijälle 42 tai 43 artiklan mukaisesti myönnettyä sertifiointia.

7. *Komissio voi laatia vakiosopimuslausekkeita tämän artiklan 3 ja 4 kohdassa tarkoitettuja seikkoja varten ja 93 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.*

8. *Valvontaviranomainen voi hyväksyä vakiosopimuslausekkeita tämän artiklan 3 ja 4 kohdassa tarkoitettuja seikkoja varten ja 63 artiklassa tarkoitetun yhdenmukaisuusmekanismin mukaisesti.*

9. *Edellä 3 ja 4 kohdassa tarkoitetun sopimuksen tai muun oikeudellisen asiakirjan on oltava kirjallinen, mukaan lukien sähköisessä muodossa.*

10. *Jos henkilötietojen käsittelijä rikkoo tätä asetusta määrittämällä käsittelyn tarkoitukset ja keinot, kyseistä henkilötietojen käsittelijää on pidettävä tämän käsittelyn rekisterinpitäjänä, sanotun kuitenkaan rajoittamatta 82, 83 ja 84 artiklan soveltamista.*

Liite 2. Kyselytutkimus suomeksi

Euroopan unionin yleisen tietosuoja-asetuksen sopimusvaatimusten yritysvaikutuksia Suomessa toimiville yhtiöille

Arvoisa vastaaja,

Kyselyllä kartoitetaan 25.5.2018 sovellettavaksi tulleen Euroopan unionin yleisen tietosuoja-asetuksen sopimusvaatimusten (artikla 28) yritysvaikutuksia Suomessa toimiville yhtiöille. Kyselyn avulla selvitetään mainittujen sopimusvaatimusten yhtiöille aiheuttamaa hallinnollista taakkaa ja niiden vaikutuksia yhtiöiden sopimusneuvotteluihin.

Vastauksia antaessasi riittää paras arviosi asiasta, sillä kyselyllä kartoitetaan tietoa sopimusvaatimusten tämän hetken kuormittavuudesta tarkkojen lukujen sijaan.

Vastaaminen vie noin 15 minuuttia.

Kysely on osa oikeustieteen opintojen pro gradu -tutkielmaa. Kaikki vastaukset ovat anonyymejä. Halutessanne kysely on mahdollista toteuttaa myös haastatteluna.

Kysely koostuu erilaisista kysymystyypeistä, vastausohjeet ovat kysymysten ohessa.

Kyselyssä käytetty verkkokyselypohja on toteutettu yhteistyössä Roschier Asianajotoimisto Oy:n kanssa, osana heidän tarjoamaa Thesis -ohjelmaa.

Jos kyselyä tai haastatteluita koskien tulee kysymyksiä tai ongelmia, olethan yhteydessä tutkielman tekijään sähköpostitse osoitteeseen: nanttala@ulapland.fi

Vastauksistanne kiittäen,
Niina Tukia

Vastaat tähän kyselyyn nimettömänä. Kun piilotettua identiteettiä käytetään kyselyissä, vastauksen yhteyteen ei tallenneta tunnistetietoja, kuten selain- ja käyttöjärjestelmätietoja, vastaajan IP-osoitetta tai sähköpostiosoitetta. Piilotettu identiteetti suojaa vastaajan henkilöllisyyttä.

Annathan yhteystietosi jos haluat osallistua kyselyyn haastattelun muodossa, niin kyselyn tekijä on teihin yhteydessä haastattelun ajankohdan ja toteutustavan sopimiseksi. Annettuja yhteystietoja käytetään vain haastattelun toteutusta varten, ja poistetaan kyselytutkimuksen päätyttyä.

Jos vastaat kyllä, kysely päättyy tähän, ja tutkimuksen toteuttaja on yritykseenne erikseen yhteydessä. Jos vastaat ei, kysely jatkuu normaalisti.

*** Yhtiömme haluaa osallistua kyselyyn, mutta haastattelun muodossa.**

a. Kyllä
b. Ei

YHTEYSTIETOSI (vastatessasi kyllä)

a. Yhtiö:_____
b. Yhteyshenkilön nimi: _____
c. Toivon, että minuun ollaan yhteydessä joko
    i. Sähköpostitse osoitteeseen:_____
    ii. tai puhelimitse numeroon:_____
d. Paras aika tavoitella on:_____

Osa 1 - Yhtiön taustatiedot

1. Yhtiön toimiala: _____
2. Yhtiön liikevaihto: _____
3. Yhtiön kotipaikan maantieteellinen sijainti:_____
4. Henkilöstön määrä: _____
5. Vastaajan tehtävänimike ja työkokemusvuodet yhtiössä:_____

Osa 2 – Henkilötietojen käsittely yhtiössä

Huomaathan seuraavat määritelmät vastatessanne kyselyyn:

Rekisterinpitäjä: *rekisterinpitäjä on muun muassa yritys tai organisaatio, joka määrittelee, mihin tarkoitukseen ja millä tavalla henkilötietoja käsitellään. Rekisterinpitäjä voi olla esimerkiksi jäsenistään tietoja keräävä yhdistys, potilastietoja käsittelevä sairaala, verkkokauppa tai sosiaalisen median palvelu (”**Rekisterinpitäjä**”).*

Henkilötietojen käsittelijä: *tietosuoja-asetuksen mukaan henkilötietojen käsittelijällä tarkoitetaan luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, joka käsittelee henkilötietoja rekisterinpitäjän lukuun. Henkilötietojen käsittelijä voi näin ollen olla esimerkiksi toisen yrityksen markkinointia hoitava markkinointitoimisto tai IT-palveluntarjoaja, jolla on pääsy Rekisterinpitäjän henkilötietoihin (**”Henkilötietojen käsittelijä”**).*

6. Henkilötietojen käsittely tarkoittaa muun muassa henkilötietojen keräämistä, säilyttämistä, käyttöä, siirtämistä ja luovuttamista. Kaikki henkilötietoihin kohdistuvat toimenpiteet henkilötietojen käsittelyn suunnittelusta henkilötietojen poistamiseen ovat henkilötietojen käsittelyä. Henkilötiedoilla tarkoitetaan kaikkia tunnistettuun tai tunnistettavissa olevaan henkilöön liittyviä tietoja (”Rekisteröity”). Henkilötietoja ovat esimerkiksi asiakkaan nimi, henkilötunnus, sijaintitiedot, verkkotunnistetiedot, taikka sairauksia koskevat tiedot.

    a. <u>Mitä henkilötietoja yhtiönne käsittelee?</u> *(voit valita useamman vastausvaihtoehdon)*
        i. Asiakastietoja (B2C)

ii. Asiakastietoja (B2C) liittyen asiakkaan profilointiin ja/tai kanta-asiakastietoihin
iii. Asiakastietoja (B2B)
iv. Työntekijätietoja
v. Toimittajatietoja
vi. Erityisiin tietoryhmiin kuuluvia tietoja (kuten terveystiedot)
vii. Muuten sensitiivisiä tietoja kuten taloudellisia tietoja (esim. luottokorttitiedot)
viii. Sidosryhmiä koskevia tietoja (esim. koskien yhtiön omistajia, sijoittajia, kumppaneita)
ix. Sijaintitietoja
x. Verkkotunnistetietoja
xi. Muuta, mikä: _____

b. Yhtiömme toimii henkilötietojen osalta: (*voit valita useamman vastausvaihtoehdon)*

i. Rekisterinpitäjänä
ii. Henkilötietojen käsittelijänä

7. Suomen lisäksi, yhtiömme käsittelee henkilötietoja rajatylittävinä siirtoina myös: *(voit valita useamman vastausvaihtoehdon)*
i. muissa EU jäsenmaissa
ii. 3.maissa (kuten USA, Intia, Venäjä)
iii. yhtiössämme ei käsitellä henkilötietoja rajatylittävinä siirtoina
iv. en osaa sanoa

Osa 3 – Asetuksen aiheuttama hallinnollinen taakka

8. Euroopan unionin yleinen tietosuoja-asetus tuli sovellettavaksi 25.5.2018 (”Asetus”), josta alkaen muun muassa EU:ssa toimivien yritysten on tullut noudattaa Asetuksen määräyksiä käsitellessään henkilötietoja. Sääntelyn muutoksen myötä Asetuksen vaikutukset voivat näkyä yritysten hallinnollisessa taakassa. Tällä tarkoitetaan yritysten toimia, joita ei toteuteta omaehtoisesti vaan yksinomaan lainsäädännön velvoitteiden vuoksi. Hallinnollinen taakka sisältää siten myös hallinnollisia kustannuksia koskien yritysten jatkuvaluonteisia menoja, joita aiheuttavat muun muassa viranomaisille tai kolmansille osapuolille toimitetut tiedot yrityksen toiminnasta tai tuotantotavoista.

a. Onko henkilötietojen käsittelystä johtuva hallinnollinen taakka yhtiössänne kasvanut Asetuksen voimaan tulon myötä? Huomioithan vastauksessasi muun muassa yhtiössä toteutetut tekniset ja organisatoriset muutokset, mahdollisen koulutuksen lisäämisen, uuden henkilökunnan palkkaamisen, ulkoistamisen tai ulkopuolisen konsultaation tarpeen. (*valitse vain yksi vastausvaihtoehto)*

i. kyllä, selvästi
ii. kyllä, jonkin verran
iii. kyllä, mutta vain vähän
iv. ei
v. en osaa sanoa

b. Jos vastasit edelliseen kysymykseen kyllä, mitkä Asetuksesta johtuvat seikat ovat erityisesti aiheuttaneet hallinnollisen taakan kasvua yhtiössänne? *(voit valita useamman vastausvaihtoehdon)*

   i. Asetuksen vaatimusten selvittäminen
   ii. Henkilötietojen käsittelyyn liittyvien riskien kartoittaminen
   iii. Tietosuojavastaavan nimittäminen
   iv. Rekisteröityjen suostumuksen selvittäminen ja informointi
   v. Rekisteröityjen tietopyynnöt
   vi. Tietojärjestelmäuudistukset, kuten IT-järjestelmien ja tietojenkäsittely ohjelmien päivittäminen tai uusien hankinta
   vii. Neuvottelut sopimuskumppaneiden kanssa, kuten palveluiden päivittämistä tai riskien jakoa koskien
   viii. Organisatoriset toimet, kuten henkilöstölle annettava ohjeistus ja henkilötietoja käsittelevän henkilöstön koulutus
   ix. Henkilötietojen käsittelyn osoitusvelvollisuuden noudattaminen
   x. Henkilötietojen käsittelytoimia koskevan selosteen ylläpito
   xi. Muu, mikä: _____

c. Asetuksen mukaan Rekisterinpitäjän ja Henkilötietojen käsittelijän on solmittava kirjallinen tietojenkäsittelysopimus, kun Henkilötietojen käsittelijä käsittelee henkilötietoja rekisterinpitäjän lukuun. Sopimuksessa tulee vahvistaa käsittelyn kohde ja kesto, käsittelyn luonne ja tarkoitus, henkilötietojen tyyppi ja rekisteröityjen ryhmät, sekä Rekisterinpitäjän velvollisuudet ja oikeudet (”Sopimusvaatimukset”). Osaatko arvioida kuinka suuri osuus Asetuksen aiheuttamasta hallinnollisesta taakasta johtuu mainituista Sopimusvaatimuksista, sisältäen muun muassa Sopimusvaatimusten ylläpidon? (*valitse vain yksi vastausvaihtoehto)*

   i. 76–100 %
   ii. 51–75 %
   iii. 26–50 %
   iv. 1-25 %
   v. ei yhtään
   vi. en osaa sanoa

Osa 4 – Asetuksen Sopimusvaatimukset

9. Kun Henkilötietojen käsittelijä käsittelee henkilötietoja Rekisterinpitäjän lukuun, tulee yritysten huomioida Asetuksen asettamat Sopimusvaatimukset sopimuksissaan.

   a. Ovatko Sopimusvaatimukset vaikuttaneet yhtiönne sopimusneuvotteluihin?

      i. kyllä, selvästi
      ii. kyllä, jonkin verran
      iii. kyllä, mutta vain vähän
      iv. ei
      v. en osaa sanoa

   b. Jos vastasit edelliseen kysymykseen kyllä, miten Sopimusvaatimukset ovat vaikuttaneet sopimusneuvotteluihin? *(voit valita useamman vastausvaihtoehdon)*

i. Sopimusneuvottelut ovat pitkittyneet
ii. Vahingonkorvausvelvollisuudesta sopiminen on vienyt aikaa
iii. Vastuunrajoituksista sopiminen on osoittautunut haastavaksi
iv. Olemassa olevien sopimusten päivittäminen on ollut työlästä
v. Alihankkijoiden käyttämisestä ei ole päästy yhteisymmärrykseen
vi. Haasteita sopia Rekisterinpitäjän avustamisesta koituvien kustannusten korvaamisesta
vii. Sopimuksen sisällöstä on tullut monimutkainen
viii. Sopimusvaatimuksiin perehtyminen on vaatinut paljon valmistelua
ix. Muuten, miten: _____

c. Koetko, että Sopimusvaatimusten myötä yhtiönne tietojenkäsittelysopimukset tulevat tulevaisuudessa: *(voit valita useamman vastausvaihtoehdon)*

i. Toteutumaan joutuisasti
ii. Toimimaan yhtiömme eduksi
iii. Toimimaan asiakkaidemme eduksi
iv. Lisäämään luottamusta sopimuskumppaneitamme kohtaan
v. Kuormittamaan yhtiömme henkilöstöä
vi. Aiheuttamaan lisäkuluja yhtiöllemme
vii. En osaa sanoa
viii. Muuten, miten: _____

10. Asetuksen mukaan yritysten sopimusneuvotteluita voitaisiin keventää hyväksyttyjen käytännesääntöjen, sertifiointimekanismien ja vakiosopimuslausekkeiden avulla. Näiden avulla jokaisen yrityksen ei tarvitsisi laatia ja neuvotella Asetuksen vaatimia Sopimusvaatimuksia erikseen, tai yritykset voisivat yhteistyökumppaneita valitessaan hyödyntää sertifioitujen yritysten palveluja tai tuotteita. Kuinka todennäköistä olisi, että yhtiönne hyödyntäisi edellä mainittuja keinoja?

a. Hyväksytyt käytännesäännöt (*valitse vain yksi vastausvaihtoehto)*
i. Erittäin todennäköisesti
ii. Todennäköisesti
iii. Epätodennäköisesti
iv. Erittäin epätodennäköisesti
v. En osaa sanoa

b. Sertifiointimekanismit (*valitse vain yksi vastausvaihtoehto)*
i. Erittäin todennäköisesti
ii. Todennäköisesti
iii. Epätodennäköisesti
iv. Erittäin epätodennäköisesti
v. En osaa sanoa

c. Vakiosopimuslausekkeet (*valitse vain yksi vastausvaihtoehto)*
i. Erittäin todennäköisesti
ii. Todennäköisesti
iii. Epätodennäköisesti
iv. Erittäin epätodennäköisesti
v. En osaa sanoa

11. Jatka väittämää käsityksesi mukaisesti: ”Henkilötietojen käsittelyn palvelusopimusten hinnat ovat Sopimusvaatimusten voimaan tulon myötä…” (*valitse vain yksi vastausvaihtoehto)*

    a. …nousseet merkittävästi
    b. …nousseet hieman
    c. …pysyneet samoina
    d. …laskeneet hieman
    e. …laskeneet merkittävästi
    f. En osaa sanoa

12. Mitä mieltä olet väittämästä: ”Merkittävä sanktiouhka lisää ennaltaehkäisevän riskienhallinnan taloudellista panostusta.” (*valitse vain yksi vastausvaihtoehto)*

    a. Täysin samaa mieltä
    b. Osittain samaa mieltä
    c. Osittain eri mieltä
    d. Täysin eri mieltä
    e. En osaa sanoa

Osa 5 - Kysymykset henkilötietojen käsittelijöille

Jos yhtiönne käsittelee henkilötietoja myös Henkilötietojen käsittelijänä, vastaathan alla oleviin kysymyksiin. Jos näin ei ole, voit siirtyä suoraan kyselyn loppuun painamalla alhaalla lähetä-painiketta.

13. Asetus velvoittaa Henkilötietojen käsittelijää tukemaan Rekisterinpitäjää henkilötietojen käsittelyssä. Kuinka usein yhtiönne on tukenut Rekisterinpitäjiä seuraavissa tehtävissä Asetuksen voimaan tulon jälkeen?

    a. Rekisteröityjen tietopyynnöissä (*valitse vain yksi vastausvaihtoehto)*
        i. Jatkuvasti
        ii. Usein
        iii. Joskus
        iv. Ei ikinä
        v. En osaa sanoa

    b. Henkilötietojen tietoturvaloukkausten käsittelyssä (*valitse vain yksi vastausvaihtoehto)*
        i. Jatkuvasti
        ii. Usein
        iii. Joskus
        iv. Ei ikinä
        v. En osaa sanoa

    c. Tietosuojaa koskevan vaikutusarvioinnin toteuttamisessa (*valitse vain yksi vastausvaihtoehto)*

i. Jatkuvasti
ii. Usein
iii. Joskus
iv. Ei ikinä
v. En osaa sanoa

Liite 3. Kyselytutkimus englanniksi

Survey on the business impact of the contractual requirements posed by the General Data Protection Regulation of the European Union on companies operating in Finland

Dear respondent,

This survey will be used to analyse the business impact that the contractual requirements posed by the General Data Protection Regulation of the European Union (Article 28) has had on companies that operate in Finland. The regulation came into force on 25 May 2018. To be more precise, the survey will help to analyse the administrative burden caused by the contractual requirements for the companies and the effect of these requirements on the contract negotiations of the companies.

When answering, your best estimate on the subject matter is sufficient, as the aim for this survey is to collect information on how burdensome the contractual requirements on companies are instead of exact figures.

The survey is a part of a Master's thesis in Law. All responses will be anonymous. If you wish, the survey may also be conducted as an interview.

The survey consists of different types of questions. The instructions for answering can be found in connection to the questions.

Filling in the survey takes approximately 15 minutes.

The online survey form used here has been implemented in co-operation with Roschier, Attorneys Ltd. as a part of their thesis program.

If you have any questions or problems regarding the survey or the interviews, please contact the researcher by email at nanttala@ulapland.fi.

Thank you for your response!

Best regards,

Niina Tukia

Your identity will be hidden. When hidden identity is used in surveys, no identifiable information, such as browser type and version, internet IP address, operating system, or e-mail address, will be stored with the answer. This is to protect the respondent's identity.

I wish that the creator of the survey contacts our company for arranging the interview. Please fill in your contact information so that the creator of the survey may contact you to arrange the time and method for the interview. The contact information will only be used for the arrangement of the interview and it will be deleted after the survey has ended.

If you choose yes, the survey will end and you will be guided to fill in your contact details. If you choose no, the survey begins on the next page.

* Our company will participate in the survey, but preferably in the form of an interview.

c. Yes
d. No

Your contact details (when answering yes)

e. Company:_____
f. Name of the contact person: _____
g. I wish to be contacted
    i. through email at the address:_____
    ii. through telephone at the number:_____
h. The best time to contact me:_____

Part 1. Company background information

1. Sector of the company: _____
2. Company turnover: _____
3. Geographical location of the company's place of residence:_____
4. Number of employees: _____
5. Respondent's title and years of experience at the company:_____

Part 2. Personal data processing in your company

Please note the following definitions when responding to the survey:

Controller: *a controller is a company or organisation which will define the purpose and manner of processing personal data. The controller may be an association collecting information on its members, a hospital processing patient information, a webshop or a social media service, for example (**the "Controller"**).*

Processor*: according to the General Data Protection Regulation, a processor is a natural person or legal person, authority, office or another type of body who processes personal data on behalf of the Controller. The processor may be a marketing agency which takes care of the marketing of another company or an IT service provider which has access to the personal data of the Controller, for example (**the "Processor"**).*

6. The processing of personal data refers to the collection, storage, use, transfer and disclosure of personal data. All actions concerning personal data, from the planning of the processing to the deletion of personal data, is personal data processing. Personal data means all data concerning an identified or identifiable person (the "Data Subject"). Personal da-

ta may include, for example, the name, personal identity code, location data, network identification data or health data of a client.

a. Which types of personal data does your company process? *(you can choose more than one option)*
   i. Customer data (B2C)
   ii. Customer data (B2C) on profiling of customers and/or customer loyalty programs
   iii. Customer data (B2B)
   iv. Employee data
   v. Supplier information
   vi. Information on special categories of personal data (e.g. data concerning health)
   vii. Otherwise sensitive information, such as financial data (e.g. credit card information)
   viii. Information on stakeholders (concerning e.g. company owners, investors, partners)
   ix. Location data
   x. Online identifiers
   xi. Other, please specify: _____

b. In terms of personal data, our company is: *(you can select more than one option)*

   i. A Controller
   ii. A Processor

7. In addition to processing personal data in Finland, our company processes cross-border transfers of personal data: *(you can select more than one option)*
   i. In other EU member states
   ii. In third countries (such as USA, India, Russia)
   iii. Our company does not process cross-border transfers of personal data
   iv. I do not know

Part 3. Administrative burden caused by the General Data Protection Regulation

8. The General Data Protection Regulation of the European Union ("GDPR") came into force on 25 May 2018, after which actors such as companies operating in the EU have been obligated to adhere to GDPR when processing personal data. The effects of GDPR may be seen in the administrative burden of companies. Administrative burden refers to the actions of companies that are not taken of the companies' own volition but solely because of the obligations set by the legislation. As such, administrative burden also involves administrative costs caused by information delivered to the authorities or third parties regarding the operations or production methods of the company.

   a. Has the administrative burden regarding the processing of personal data increased in your company after GDPR came into force? Please consider in your answer any technical and organisational measures, additional trainings, recruitment of new employees, outsourcing or the need for external consulting in your company. (*please select only one option)*

      i. Yes, clearly

ii. Yes, somewhat
iii. Yes, but only a little
iv. No
v. I do not know

b. If you answered 'yes' in the previous question, which matters caused by GDPR have particularly increased the administrative burden in your company? *(you can select more than one option)*

i. Finding out the requirements of GDPR
ii. Surveying the risks related to the processing of personal data
iii. Appointing a Data Protection Officer
iv. Seeking consent from the Data Subjects and informing them
v. Requests from Data Subjects
vi. Upgrades to data systems, such as updates to IT systems and data processing software, or the purchase of new systems or software
vii. Negotiations with contractual partners on matters such as updates to the services or the distribution of risks
viii. Organisational measures, such as instructions given to employees or training provided to the employees who process personal data
ix. Adhering to the accountability for personal data processing
x. Maintaining records of processing activities
xi. Other, please specify: _____

c. According to GDPR, the Controller and the Processor shall make a written data processing agreement when the Processor is processing personal data on behalf of the Controller. The contract shall confirm the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and the categories of Data Subjects, as well as the obligations and rights of the Controller ("Contractual Requirements"). Can you estimate what percentage of the administrative burden caused by GDPR is due to the Contractual Requirements mentioned above, including the maintenance of Contractual Requirements? *(please select only one option)*

i. 76–100%
ii. 51–75%
iii. 26–50%
iv. 1-25%
v. 0%
vi. I do not know

Part 4. Contractual Requirements set by GDPR

9. When the Processor processes personal data on behalf of the Controller, the companies need to take the Contractual Requirements set by GDPR into account in their mutual contracts.

a. Have the Contractual Requirements affected the contract negotiations of your company?

i. Yes, clearly
ii. Yes, somewhat
iii. Yes, but only a little
iv. No
v. I do not know

b. If you answered 'yes' in the previous question, how have the Contractual Requirements affected your contract negotiations? *(you can select more than one option)*

i. Negotiations have taken longer
ii. Agreeing on liabilities has taken more time
iii. Agreeing on limitations of risk has proven challenging
iv. Updating existing contracts has become laborious
v. We have not reached an understanding on using subcontractors
vi. Agreeing on compensation for the costs of assisting the Controller has been challenging
vii. The contents of the contract have become overly complex
viii. Studying the Contractual Requirements has required a lot of preparations
ix. In other ways, please specify: _____

c. Do you feel that, due to the Contractual Requirements, the data processing agreements of your company will: *(you can choose more than one option)*

i. Function smoothly
ii. Work in favour of our company
iii. Work in favour of our clients/customers
iv. Increase trust towards our contractual partners
v. Burden the employees of our company
vi. Cause additional costs for our company
vii. I do not know
viii. Other, please specify: _____

10. According to GDPR, the contract negotiations of companies could be facilitated by means of approved codes of conduct, certification mechanisms or standard contractual clauses. With the help of these, every company would not need to prepare and negotiate on the Contractual Requirements set by GDPR individually, or companies could use the services or products of certified companies when choosing partners. How likely is your company to use the means specified above?

a. Approved codes of conduct *(please select only one option)*
i. Very likely
ii. Likely
iii. Unlikely
iv. Very unlikely
v. I do not know

b. Certification mechanisms *(please select only one option)*
i. Very likely
ii. Likely
iii. Unlikely

iv. Very unlikely
v. I do not know

c. Standard contractual clauses *(please select only one option)*
   i. Very likely
   ii. Likely
   iii. Unlikely
   iv. Very unlikely
   v. I do not know

11. Please continue the following sentence according to the best of your knowledge: "After the Contractual Requirements came into force, the prices of service agreements regarding the processing of personal data have…" (*please select only one option)*

    a. ...increased significantly
    b. ...increased slightly
    c. ...remained the same
    d. ...decreased slightly
    e. ...decreased significantly
    f. I do not know

12. What do you think of this statement: "A significant threat of penalty increases financial investments into preventive risk management." (*please select only one option)*

    a. Completely agree
    b. Somewhat agree
    c. Somewhat disagree
    d. Completely disagree
    e. I do not know

Part 5. Questions for Processors

If your company also processes personal data as a Processor, please answer the questions below. If this is not applicable to you, please proceed to sending your answers by pressing the send button on the bottom of the page.

13. GDPR requires that the Processor support the Controller in the processing of personal data. After GDPR came into force, how often has your company supported Controllers in the following tasks?

    a. Requests from Data Subjects *(Please select only one option)*
       i. Constantly
       ii. Often
       iii. Occasionally
       iv. Never
       v. I do not know

b. Dealing with data security breaches regarding personal data *(please select only one option)*
    i. Constantly
    ii. Often
    iii. Occasionally
    iv. Never
    v. I do not know

c. Assessing the impact of data protection *(please select only one option)*
    i. Constantly
    ii. Often
    iii. Occasionally
    iv. Never
    v. I do not know