ASIANAJOTOIMISTON TIETOSUOJAVELVOITTEET DUE DILIGENCE -TARKASTUKSESSA – REKISTERINPITÄJÄ VAI HENKILÖTIETOJEN KÄSITTELIJÄ?

Armida Rantanen
Law and Information Society
Turun yliopiston oikeustieteellinen tiedekunta
Joulukuu 2019

TURUN YLIOPISTO
Oikeustieteellinen tiedekunta

ARMIDA RANTANEN: Asianajotoimiston tietosuojavelvoitteet due diligence -tarkastuksessa – rekisterinpitäjä vai henkilötietojen käsittelijä?

OTM-tutkielma, VIII+76 s.
Tietosuojaoikeus
Joulukuu 2019
Turun yliopiston laatujärjestelmän mukaisesti tämän julkaisun alkuperäisyys on tarkastettu Turnitin Originality Check -järjestelmällä.

Vuonna 2018 voimaan tullut yleinen tietosuoja-asetus toi mukanaan merkittäviä muutoksia henkilötietojen käsittelyyn ja käsittelystä aiheutuviin vastuisiin ja velvollisuuksiin. Vaikka asetuksen tarkoituksena on ollut vastata teknologiakehitykseen ja sen myötä muuttuneeseen henkilötietojen käsittelyyn, on asetus säädetty teknologianeutraaliksi. Sen vuoksi asetuksella on huomattavia vaikutuksia lähes kaikkien yhtiöiden toiminnan järjestämiseen – asetus on lisännyt niin hallinnollisia velvoitteita kuin henkilötietojen käsittelystä aiheutuvia kustannuksia.

Yrityksen vastuut ja velvoitteet riippuvat siitä, määritelläänkö yritys asetuksen nojalla rekisterinpitäjäksi vai henkilötietojen käsittelijäksi. Rekisterinpitäjän vastuu asetuksen noudattamisesta ja noudattamisen osoittamisesta on kokonaisvaltaisempaa ja laajempaa kuin henkilötietojen käsittelijän vastuu, minkä vuoksi käsittelyyn osallistuvien tahojen roolit on määriteltävä ennen käsittelyn aloittamista. Tässä tutkielmassa tarkastellaan asianajotoimiston roolia tietosuoja-asetuksen näkökulmasta silloin, kun se suorittaa asiakkaansa lukuun yrityskauppaa edeltävää due diligence -tarkastusta, jossa käsitellään henkilötietoja.

Kysymyksen problematiikka liittyy yhtäältä siihen, määritteleekö asianajotoimisto henkilötietojen käsittelyn tarkoitukset ja keinot, jolloin se olisi katsottava rekisterinpitäjäksi, sekä toisaalta siihen, että asianajotoimisto tekee tarkastusta asiakkaansa lukuun, mikä on yksi henkilötietojen käsittelijän määritelmään kuuluva kriteeri. Lisäksi on arvioitu, voisiko asianajotoimisto olla yhteisrekisterinpitäjä jonkun tarkastukseen osallistuvan tahon kanssa. Osakysymyksenä tutkielmassa tarkastellaan lisäksi sitä, millä tietosuoja-asetuksen mukaisella oikeusperusteella due diligence -tarkastuksessa voidaan käsitellä henkilötietoja.

Tutkielman metodi on lainopillinen ja keskittyy määritelmien arvioinnissa erityisesti sanamuodon mukaiseen tulkintaan. Lisäksi, EU-oikeuden lainopilliselle tarkastelulle tyypilliseen tapaan on kysymystä lähestytty myös teleologisella metodilla, eli lähestymällä normia sääntelyn tarkoituksen ja päämäärän kautta. Tämä näkyy erityisesti siinä, että kysymykseen vastaamiseksi on arvioitu, miten eri osapuolet kykenisivät toteuttamaan rekisterinpitäjän ja henkilötietojen käsittelijän vastuita.

Johtopäätöksenä tutkielmassa todetaan, että asianajotoimiston rooli tarkastuksessa henkilötietojen käsittelyn osalta on rekisterinpitäjä. Se, toimiiko asianajotoimisto yhteisrekisterinpitäjänä asiakkaansa kanssa, riippuu muun muassa asiakkaan ja asianajotoimiston välisestä sopimuksesta ja asiakkaan tosiasiallisesta osallistumisesta henkilötietojen käsittelyyn.

Asiasanat: tietosuoja, rekisterinpitäjä, yhteisrekisterinpitäjä, henkilötietojen käsittelijä, asianajotoimisto, due diligence -tarkastus

SISÄLLYS

LÄHTEET

Kirjallisuus

Blume, Peter, Controller and processor: is there a risk of confusion? International Data Privacy Law, Vol. 3, No 2, 2013, s. 140–145.

Calder, Alan, EU GDPR: A Pocket Guide (European). IT Governance Publishing 2016.

Crilly, William M. – Sherman, Andrew J., The AMA Handbook of Due Diligence. Amacom 2010.

Davis, Danny A. – Kummer, Christopher B., M&A Integration: How to Do It. Planning and Delivering M&A Integration for Business Success. John Wiley & Sons Ltd 2012.

Enroth, Timo – Neuvonen, Riku, EU:n tietosuoja-asetuksen yritysvaikutukset. Policy Brief 10/2017. Valtioneuvoston selvitys- ja tutkimustoiminta.

Feiler, Lukas – Forgó, Nikolaus – Weigl, Michaela, The EU General Data Protection Regulation (GDPR): A Commentary. Globe Law and Business 2018.

Gil González, Elena – de Hert, Paul, Understanding the legal provisions that allow processing and profiling of personal data—an analysis of GDPR provisions and principles. ERA Forum Vol. 19, Issue 4, April 2019, s. 597–621.

Hallberg, Pekka – Karapuu, Heikki – Ojanen, Tuomas – Scheinin, Martin – Tuori, Kaarlo – Viljanen, Veli-Pekka, Perusoikeudet. WSOYpro, 2011. (http://verkkokirjahylly.almatalent.fi Päivitetty 13.1.2011.)

Hanninen, Minna – Laine, Elli – Rantala, Kati – Rusi, Mari – Varhela, Markku, Henkilötietojen käsittely: EU-Tietosuoja-asetuksen vaatimukset. Kauppakamari 2017.

Harsu, Johanna, Due Diligence -toimeksianto ja asianajajayhtiön korvausvastuu. Oikeustiede-Jurisprudentia XXXVII:2004, s. 45–152.

Hintze, Mike, Data Controllers, Data Processors, and the Growing Use of Connected Products in the Enterprise: Managing Risks, Understanding Benefits, and Complying with the GDPR. Journal of Internet Law, August 2018, s. 17–31.

Hooke, Jeffrey C., M&A: A Practical Guide to Doing the Deal. Second edition. John Wiley & Sons, Inc. 2014.

Houser, Kimberly A. – Voss, Gregory, The End of Google and Facebook Or a New Paradigm in Data Privacy. Richmond Journal of Law & Technology, Vol. XXV, Issue 1, 2018.

Howson, Peter, The Critical Stage in Mergers and Acquisitions. First edition. Routledge 2003.

Husa, Jaakko – Mutanen, Anu – Pohjolainen, Teuvo, Kirjoitetaan juridiikkaa. Talentum 2008.

Information Commissioner's Office, Data controllers and data processors: what the difference is and what the governance implications are. (ICO.)

IT Governance Privacy Team, EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide. Second edition. IT Governance Publishing 2017.

IT Governance Privacy Team, EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide. Third edition. IT Governance Publishing 2019.

Kamara, Irene – De Hert, Paul, Understanding the Balancing Act Behind the Legitimate Interest of the Controller Ground: A Pragmatic Approach. Brussels Privacy Hub vol. 4, No 12, August 2018.

Katramo, Mikko – Lauriala, Jari – Matinlauri, Ismo – Niemelä, Jaakko E. – Svennas, Karin – Wilkman, Nina, Yrityskauppa. 2. painos. Sanoma Pro cop 2013. (http://verkkokirjahylly.almatalent.fi)

Korpisaari, Päivi – Pitkänen, Olli – Warma-Lehtinen, Eija, Uusi tietosuojalainsäädäntö. Alma Talent 2018. (http://verkkokirjahylly.almatalent.fi)

Lindroos-Hovinheimo, Susanna, Who controls our data? The legal reasoning of the European Court of Justice in *Wirtschaftsakademie Schleswig-Holstein* and *Tietosuojavaltuutettu v Jehovan todistajat.* Information & Communications Technology Law, 28:2, s. 225–238.

Mackay, Hugh – Maples, Wendy – Reynolds, Paul, Investigating the Information Society. Routledge 2001.

Meyer, Andreas Gard, Identifying Controllers and Processors Pursuant to the General Data Protection Regulation. University of Oslo 2018.

Mähönen, Jukka – Villa, Seppo, Osakeyhtiö III – Corporate Governance. Alma Talent Oy 2010. (http://verkkokirjahylly.almatalent.fi)

Mäkelä, Joni, Virhevastuu yrityskaupoissa erityisesti ostajan suorittaman due diligence -tarkastuksen näkökulmasta tarkasteltuna. Referee-artikkeli. Acta Legis Turkuensia 1/2011, s. 111–132.

Rauhofer, Judith, One Step Forward, Two Steps Back? Critical observations on the proposed reform of the EU data protection framework. Research Paper Series No 2013/7. University of Edinburgh.

Sher, Howard, Due diligence investigations. Juta's Business Law 6 (1) 1998), s. 15–19.

Soininen, Niko, Oikeudellisen argumentin rakentaminen kirjoitusprosessissa. Kokoelmateos Oikeustieteellinen opinnäyte – artikkeleita oikeustieteellisten opinnäytteiden vaatimuksista, metodista ja arvostelusta. Edita Publishing Oy 2016, s. 51–70.

Talus, Kim – Penttinen, Sirja-Leena, Eurooppaoikeudelliset oikeuslähteet ja niiden tulkinta oikeustieteellistä opinnäytettä kirjoittaessa. Kokoelmateos Oikeustieteellinen opinnäyte – artikkeleita oikeustieteellisten opinnäytteiden vaatimuksista, metodista ja arvostelusta. Edita Publishing Oy 2016, s. 223–245.

Treacy, Bridget, Challenging Times Ahead of Data Processors. Data Protection Ireland, Vol. 5, Issue 5. Pdp Journals 2012.

Vainio, Sonja, Rekisterinpitäjän osoitusvelvollisuus EU:n yleisessä tietosuoja-asetuksessa. 15 vuotta viestintäoikeutta – Viestintäoikeuden vuosikirja 2017. Referee-artikkeli.

Van der Sloot, Bart – Zuiderveen Borgesius, Frederik, The Eu General Data Protection Regulation: A New Global Standard For Information Privacy.

Vapaavuori, Tom, Liikesalaisuudet ja salassapitosopimukset. Alma Talent Oy 2019. (http://verkkokirjahylly.almatalent.fi)

Veale, Michael – Binns, Reuben – Ausloos, Jef, When data protection by design and data subject rights clash. Vol. 8, No. 2, International Data Privacy Law 2018.

Von Grafenstein, Maximilian, The Principle of Purpose Limitation in Data Protection Laws: The Risk-based Approach, Principles, and Private Standards as Elements of Regulating Innovation. Nomos Verlagsgesellschaft mbH, 2018.

Wilhelmsson, Thomas – Sevón, Leif – Koskelo, Pauliine, Kauppalain pääkohdat. 5., uudistettu painos. Talentum 2006. (http://verkkokirjahylly.almatalent.fi)

Virallislähteet

European Union Agency for Fundamental Rights, European Court of Human Rights, Council of Europe, European Data Protection Supervisor: Handbook on European data protection law, 2018 edition.

Komission tiedonanto Euroopan parlamentille, Neuvostolle, Euroopan talous- ja sosiaalikomitealle ja alueiden komitealle: Kattava lähestymistapa henkilötietojen suojaan Euroopan unionissa. Bryssel 4.11.2010. KOM(2010) 609.

Oikeusministeriö [ja Asianajotoimisto Dittmar & Indrenius]: EU:n yleisen tietosuoja-asetuksen vaikutukset suomalaisiin yrityksiin. (Oikeusministeriö ja Dittmar & Indrenius)

Article 29 Working Party (29 artiklan mukainen työryhmä), Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT). 01935/06/EN, WP 128, 22.11.2006. (WP 128)

Article 29 Working Party (29 artiklan mukainen työryhmä), The Future of Privacy - Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data. 02356/09/EN, WP 168, 1.12.2009. (WP 168)

Article 29 Working Party (29 artiklan mukainen työryhmä), Opinion 1/2010 on the concepts of ”controller” and ”processor”. 00264/10/EN, WP 169, 16.2.2010. (WP 169)

Article 29 Working Party (29 artiklan mukainen työryhmä), Opinion 3/2010 on the principle of accountability. 00062/10/EN, WP 173, 13.4.2010. (WP 173)

Article 29 Working Party (29 artiklan mukainen työryhmä), Opinion 05/2012 on Cloud Computing. 01037/12/EN, WP 196, 1.7.2012. (WP 196)

Article 29 Working Party (29 artiklan mukainen työryhmä), Opinion 03/2013 on purpose limitation. 00569/13/EN, WP 203, 2.4.2013. (WP 203)

Article 29 Working Party (29 artiklan mukainen työryhmä), Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC. 844/14/EN, WP 217, 9.4.2014. (WP 217)

Article 29 Working Party (29 artiklan mukainen työryhmä), Statement on the role of a risk-based approach in data protection legal frameworks. 14/EN, WP 218, 30.5.3014. (WP 218)

Article 29 Working Party (29 artiklan mukainen työryhmä), Guidelines on Consent under Regulation 2016/679. 17/EN, WP 259, 10.4.2018. (WP 259)

Oikeustapaukset

Euroopan unionin tuomioistuin

Asia C-131/12 Google Spain & Google Inc. v. Agencia Española de Protección de Datos (AEDP) & Mario Costeja González. Annettu 13.5.2014. (Google Spain)

Yhdistetyt asiat C-468/10 Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) ja C-469/10 Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administarción del Estado. Annettu 24.11.2011. (ASNEF)

Asia C-210/16 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein GmbH. Annettu 5.6.2018. (Wirtschaftsakademie Schleswig-Holstein)

Asia C-25/17 Tietosuojavaltuutettu v. Jehovan todistajat. Annettu 10.7.2018. (Tietosuojavaltuutettu v. Jehovan todistajat)

Asia C-40/17 Fashion ID GmbH & Co.KG v. Verbraucherzentrale NRW e.V. Julkisasiamies Michal Bobekin ratkaisuehdotus, 19.12.2018.

Asia C-40/17 Fashion ID GmbH & Co.KG v. Verbraucherzentrale NRW e.V. Annettu 29.7.2019. (Fashion ID)

Asia C-13/16 Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA "Rīgas satiksme". Annettu 4.5.2017. (Rigas Satiksme)

Internetlähteet

Finanssivalvonta: Liikkeeseenlaskijat ja sijoittajat – Listautuminen https://www.finanssivalvonta.fi/paaomamarkkinat/liikkeeseenlaskijat-ja-sijoittajat/listautuminen/ (Luettu 13.2.2019)

GDPR Appropriate Technical and Organisational Measures. Know Your Compliance 2018. https://www.knowyourcompliance.com/gdpr-technical-organisational-measures/ (Luettu 18.11.2019)

Guidance on the use of Legitimate Interests under the EU General Data Protection Regulation. Data Protection Network 2018. https://www.dpnetwork.org.uk/dpn-legitimate-interests-guidance/

Harroch, Richard, How To Negotiate A Business Acquisition Letter Of Intent. Forbes 2015. https://www.forbes.com/sites/allbusiness/2015/07/30/how-tonegotiate-a-business-acquisition-letter-of-intent/ (Luettu 22.1.2019)

Mergers Acquisitions M&A Process. Corporate Finance Institute. https://corporatefinanceinstitute.com/resources/knowledge/deals/mergers-acquisitions-ma-process/ (Luettu 25.1.2019)

Mora, Ronald N., Seller's Due Diligence. GR Review. Gould & Ratner Corporate and Commercial Group 2008. http://www.gouldratner.com/assets/publications/RNM_Business-Seller-Due-Diligence.pdf (Luettu 22.1.2019)

Oxford dictionary. https://en.oxforddictionaries.com/definition/due_diligence (Luettu 22.1.2019)

Tietosuojavaltuutetun toimisto, Osoita noudattavasi tietosuojasäännöksiä. https://tietosuoja.fi/osoitusvelvollisuus (Luettu 19.11.2019)

Tietosuojavaltuutetun toimisto, Perustuuko tekemäsi henkilötietojen käsittely suostumukseen? Tarkista, että suostumus vastaa tietosuoja-asetuksen vaatimuksia. 14.5.2018. https://tietosuoja.fi/artikkeli/-/asset_publisher/perustuuko-tekemasi-henkilotietojen-kasittely-suostumukseen-tarkista-etta-suostumus-vastaa-tietosuoja-asetuksen-vaatimuksia (Luettu 28.5.2019)

Tietosuojavaltuutetun toimisto: Rekisterinpitäjän oikeutettu etu. https://tietosuoja.fi/rekisterinpitajan-oikeutettu-etu (Luettu 1.6.2019)

Tietosuojavaltuutetun toimisto: Rekisteröidyn suostumus. https://tietosuoja.fi/rekisteroidyn-suostumus (Luettu 30.5.2019)

LYHENTEET

CJEU	Euroopan unionin tuomioistuin
HTL	Henkilötietolaki (523/1999)
KL	Kauppalaki (355/1987)
LSL	Liikesalaisuuslaki (595/2018)
OYL	Osakeyhtiölaki
WP29	29 artiklan mukainen tietosuojatyöryhmä

1 JOHDANTO

1.1 Yleinen tietosuoja-asetus ja henkilötietojen käsittely yrityksissä

Viime vuosikymmenien aikana informaatioyhteiskunnan kehittymisen myötä tiedon ja tietoverkkojen merkitys yhteiskunnalle on kasvanut nopeammin kuin koskaan.[1] Yhteiskunnallisen murroksen myötä myös lainsäädännölliset haasteet ja sääntelyn pysyminen ajantasaisena alati muuttuvassa maailmassa ovat olleet pinnalla niin kansallisella kuin EU:n tasollakin. Teknologia ja kehittyvät internet-palvelut ovat lisänneet merkittävästi myös luonnollisia henkilöitä koskevien henkilötietojen käsittelyä, jota suoritetaan yhä useammin automaattisesti ja massadataa *(big data)* hyödyntäen. Käsittely on 2000-luvun aikana herättänyt tarpeen henkilötietojen käsittelyä koskevan sääntelyn uudistamiselle ja tarpeeseen on pyritty vastaamaan vuonna 2018 sovellettavaksi tulleella, EU:n yleisellä tietosuoja-asetuksella (2016/679)[2].

Asetus tuli voimaan vuonna 2016, mutta sen valmistelun voidaan katsoa alkaneen komission tiedonannosta[3] jo vuonna 2011. Jo kyseisessä tiedonannossa ilmaistiin, että globalisaatio ja nopea tekniikan kehitys ovat luoneet henkilötietojen suojelulle haasteita, joiden vuoksi henkilötietodirektiivi (95/46/EY)[4] ei enää vastannut uutta tekniikkaa. Vaikka tietosuoja-asetuksen säätämisen taustalla on tarve vastata entistä paremmin tietoyhteiskunnan ja henkilötietojen käsittelyn muutoksiin, asetuksen soveltamisala haluttiin alusta lähtien pitää tekniikkaneutraalina henkilötietodirektiivin tavoin[5] ja siten se soveltuu niin manuaaliseen kuin automaattiseen henkilötietojen käsittelyyn muutamia soveltamisalaan otettuja poikkeuksia lukuun ottamatta.

Laajan soveltamisalansa vuoksi tietosuoja-asetus soveltuu lähes kaikkiin EU-alueella toimiviin yrityksiin, sillä lähes jokaisella yrityksellä on työntekijöitä, asiakkaita tai yhteistyökumppaneita, joiden henkilötietoja yritys käsittelee. Vaikka jo henkilötietodirektiivissä säädettiin useista velvoitteista samalla tavoin kuin tietosuoja-asetuksessa, direktiivin suora vaikutus yhti-

[1] Ks. esim. *Mackay – Maples – Reynolds* 2001 s. 10–11.
[2] Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus).
[3] KOM(2010) 609.
[4] Euroopan parlamentin ja neuvoston direktiivi 95/46/EY annettu 24 päivänä lokakuuta 1995, yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta.
[5] KOM(2010) 609, s. 3.

öiden toimintaan ja hallintoon jäi vähäisemmäksi muun muassa siksi, että direktiivin implementointi tapahtui eri tavoin EU:n jäsenvaltioissa. Suomessa direktiivi implementoitiin henkilötietolakiin (532/1999, kumottu, jäljempänä ”HTL”). Asetuksessa kansallista liikkumavaraa on jätetty vähän, minkä lisäksi sääntelyn noudattamista on tehostettu säätämällä hallinnollisesta sakosta, joka voi seurata asetuksen rikkomisesta.

Asetuksen voimaantulon voidaan katsoa muuttaneen EU:n alueella tapahtuvan henkilötietojen käsittelyn sääntelyä voimakkaasti. Harppaus henkilötietodirektiivistä tietosuoja-asetukseen on siksi aiheuttanut – ja tulee myös jatkossa aiheuttamaan – yrityksille niin kustannuksia kuin uusia hallinnollisia vaatimuksiakin.[6] Vaikka yksi asetuksen tavoitteista oli keventää henkilötietojen käsittelijöiden hallinnollista taakkaa direktiiviin verrattuna,[7] esimerkiksi Suomessa sen vaikutukset ovat olleet päinvastaiset: hallinnollinen taakka on lisääntynyt, koska direktiiviä implementoitaessa ei otettu käyttöön laajoja ilmoitus- tai rekisteröitymisvelvollisuuksia.[8] Hallinnollisen taakan kasvamisen lisäksi kustannuksia voi aiheutua mm. uusien tietosuojajärjestelmien kehittämisestä ja hankkimisesta, tietosuojavastaavan nimittämisestä, koulutuksista ja sanktiojärjestelmän aiheuttaman taloudellisen riskin näkymisestä erilaisten palvelujen hinnoissa.[9]

Edellä esitetyn lisäksi yrityksille voi lisäksi syntyä kustannuksia myös muista asetuksen mukaisista velvoitteista ja vastuista.. Se, mitä velvoitteita ja vastuita yritykselle syntyy, riippuu siitä, määritelläänkö yritys tietosuoja-asetuksen mukaan *rekisterinpitäjäksi* vai *henkilötietojen käsittelijäksi.* Rekisterinpitäjällä tarkoitetaan asetuksessa luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot (tietosuoja-asetuksen 4 artiklan 7 kohta). Henkilötietojen käsittelijä käsittelee henkilötietoja rekisterinpitäjän lukuun (tietosuoja-asetuksen 4 artiklan 8 kohta). Lähtökohtaisesti rekisterinpitäjän vastuu on kokonaisvaltaisempaa ja laajempaa, mutta myös henkilötietojen käsittelijän velvollisuudet ovat lisääntyneet henkilötietodirektiiviin (ja HTL:n) nähden. Asetus muuttaakin osapuolten välistä vastuunjakoa laajentamalla henkilötietojen käsittelijän vastuuta runsaasti aikaisempaan nähden. Näin on pyritty turvaamaan rekisteröidyn[10] oikeudet aikaisempaa paremmin ja aukottomammin.

[6] Ks. esim. *Oikeusministeriö ja Dittmar & Indernius* sekä *Enroth – Neuvonen* 2017.
[7] KOM(2010) 609, s. 10.
[8] *Oikeusministeriö ja Dittmar & Indrenius* s. 11.
[9] *Enroth – Neuvonen* 2017, s. 6–9.
[10] Rekisteröidyllä tarkoitetaan tietosuoja-asetuksessa tunnistettavaa tai tunnistettavissa olevaa luonnollista henkilöä, jonka henkilötietoja käsitellään.

Vaikka tietosuoja-asetus on henkilötietodirektiiviin verrattuna selkeyttänyt rekisterinpitäjän ja henkilötietojen käsittelijän välistä vastuun jakautumista ja lisännyt henkilötietojen käsittelijään kohdistuvia velvollisuuksia, käsitteiden määritelmät ovat pysyneet muuttumattomina. Vakiintuneista määritelmistä huolimatta ongelmia voi kuitenkin tuottaa sen määrittäminen, onko yritys henkilötietoja käsitellessään rekisterinpitäjä vai henkilötietojen käsittelijä. Periaatteessa roolin määrittäminen ei vaikuta haasteelliselta: ensin on mietittävä, määrittääkö yritys käsittelyn tarkoitukset ja keinot. Jos määrittää, se on rekisterinpitäjä. Jos vastaus on kieltävä, yritys toimii todennäköisesti henkilötietojen käsittelijänä. Tällöin on kuitenkin hahmotettava se, käsitteleekö yritys henkilötietoja jonkun toisen tahon – eli rekisterinpitäjäksi määriteltävän tahon – lukuun.

Toimijoiden rooleista on löydettävissä jonkin verran esimerkkejä muun muassa viranomaisten ohjeistuksista ja oikeuskäytännöstä, mutta niiden avulla ei voida määrittää kaikkien henkilötietoja käsittelevien tahojen roolia. Määrittely voi olla ongelmallista esimerkiksi silloin, kun yritys käsittelee henkilötietoja toisen tahon lukuun, mutta osallistuu jollakin tasolla myös henkilötietojen käsittelyn tarkoitusten tai keinojen määrittelyyn. Tällainen voi olla tilanne esimerkiksi asianajotoimiston (tai muun asiantuntijapalveluita tarjoavan yrityksen) kohdalla, kun se käsittelee henkilötietoja asiakkaansa lukuun toimeksiantoa täyttäessään, mutta saattaa myös osallistua käsittelyn tarkoitusten tai ainakin keinojen määrittelyyn.

Yksiselitteistä vastausta siihen, onko asianajotoimisto toimeksiantoa täyttäessään rekisterinpitäjä vai henkilötietojen käsittelijä, ei voitane antaa. Rooli riippuu nähdäkseni yhtäältä siitä, mistä asianajotoimiston ja asiakkaan välisessä toimeksiantosopimuksessa on sovittu (sopimuksen laajuus voi ratkaista sen, ketkä osallistuvat tarkoituksen ja keinojen määrittelyyn) sekä toisaalta siitä, millaista prosessia toimeksianto koskee: kysymys voi olla esimerkiksi yksittäisen rikosasian hoitamisesta tai vaikkapa yrityksen työ- tai vero-oikeudellisten asioiden hoitamisesta. Tässä tutkielmassa asianajotoimiston roolia tarkastellaan sellaisessa asiakassuhteessa, jossa asianajotoimisto hoitaa yrityskauppaan liittyvää juridiikkaa ostajayrityksen toimeksiannosta. Erityisesti keskitytään rooliin due diligence -tarkastuksen[11] näkökulmasta, jossa henkilötietoja käsitellään – tai on ainakin aiemmin käsitelty – laajassa määrin.

[11] Englanninkielestä lainattu termi due diligence, eli suomeksi *asianmukainen huolellisuus*, on vakiintunut liikeelämän termi, jolla tarkoitetaan ennen yrityskauppaa tehtävää liiketoiminnan kokonaisvaltaista arviointia erityisesti sen varojen ja velkojen määrittämiseksi sekä kaupallisen potentiaalin arvioimiseksi. [Lähde: Oxford dictionary, https://en.oxforddictionaries.com/definition/due_diligence]

1.2 Tutkimuskysymys ja sen rajaaminen

Tämän tutkielman tutkimuskysymys on:

> Toimiiko asianajotoimisto rekisterinpitäjänä vai henkilötietojen käsittelijänä tehdessään due diligence -tarkastusta yrityskaupan ostajan edustajana ja mitä velvoitteita rooliin liittyy?

Kysymykseen vastatakseen on syytä arvioida ensinnäkin sitä, osallistuuko asianajotoimisto tarkastuksessa henkilötietojen käsittelyn tarkoitusten ja/tai keinojen määrittelyyn. Jos se ei osallistu, kyseessä on henkilötietojen käsittelijä. Jos taas keinojen tai tarkoitusten määrittely kuuluu asianajotoimistolle, se käsittelee henkilötietoja rekisterinpitäjänä. On myös mahdollista, että asianajotoimisto toimii *yhteisrekisterinpitäjänä* toisen tahon – kuten asiakkaansa – kanssa, jos keinojen ja/tai tarkoitusten määrittelyn katsotaan kuuluvan asianajotoimistolle ja toiselle taholle. Toisaalta oikeuskirjallisuudessa on katsottu, että myös henkilötietojen käsittelijä voi jossakin määrin osallistua käsittelyn keinojen määrittämiseen ja se voi tehdä ratkaisuja muun muassa käsittelyn tekniseen toteutukseen liittyen.[12]

On selvää, että asianajotoimisto toimii tarkastusta tehdessään ostajan lukuun. Tarkastuksessa käsiteltävät tiedot saadaan kuitenkin myyjältä (tai usein myyjää edustavalta asianajotoimistolta) ja siksi on mielestäni tärkeää pohtia, miten vastuu henkilötietojen käsittelystä jakautuu, kun käsiteltäviä tietoja ei anna asianajotoimiston oma asiakas, vaan vastapuoli. Ostajan tietosuoja-asetuksen mukaista roolia arvioitaessa on syytä ottaa huomioon myös se, ettei yrityskauppa ole välttämättä varmistunut vielä tarkastusta tehtäessä (esimerkiksi huutokauppana toteutettavissa yrityskaupoissa, joissa tarkastuksen voi tehdä useampi ostajakandidaatti). Tutkimuskysymyksen kannalta on siis relevanttia arvioida ns. alakysymyksenä tai lähestymistapana sitä, *kuka toimii rekisterinpitäjänä, jos asianajotoimisto katsotaan henkilötietojen käsittelijäksi?*

Jaottelu rekisterinpitäjän ja henkilötietojen käsittelijän välillä voi sinänsä tuntua akateemiselta erityisesti silloin, jos käsittelyn osapuolet joka tapauksessa huolehtivat yhdessä käsittelyn hallinnollisesta puolesta ja muun muassa rekisteröidyn tiedonsaantioikeuksista. Eron tekeminen on kuitenkin tärkeää esimerkiksi tietoturvaloukkausten vuoksi, sillä sekä toimijoiden että viranomaisten tulee kyetä määrittämään se, miten vastuu osapuolten välillä jakautuu.[13]

[12] Ks. Handbook on European data protection law, s. 108 ja *Korpisaari – Pitkänen – Warma-Lehtinen* 2018, s. 293.
[13] ICO., s. 6.

Jotta tietosuoja-asetuksen mukaista roolia voidaan arvioida, tutkimuksen osakysymyksenä selvitetään lisäksi, onko henkilötietojen käsittelylle olemassa tietosuoja-asetuksen mukainen oikeusperuste ja mitä henkilötietoja tarkastuksessa voidaan sen nojalla käsitellä. Sen vuoksi tutkielmassa käydään lyhyesti ja melko yleisellä tasolla läpi tietosuoja-asetuksen 6 ja 7 artiklat (käsittelyn lainmukaisuus ja suostumuksen edellytykset). Artikloiden osalta paneudutaan niihin kohtiin, jotka ennakko-oletuksen mukaan voisivat soveltua tarkastuksen tekemiseen.

Asianajotoimisto käsittelee henkilötietoja myös muuten kuin due diligence -tarkastuksessa ja tutkielman johtopäätökset voivat jossakin määrin soveltua myös muihin käsittelytapauksiin, mutta due diligence -tarkastuksen erityispiirre on se, että käsiteltäviä henkilötietoja ei saada asianajotoimiston asiakkaalta, vaan vastapuolelta. Asianajotoimiston roolin määrittämiseksi on siis jossain määrin syytä kiinnittää huomiota myös muihin yrityskauppaan ja due diligence -tarkastukseen liittyviin tahoihin ja siihen, millaisia tehtäviä ja sitä kautta rooleja tahoilla on. Erityisesti tällaisia tahoja ovat asianajotoimiston kanssa toimeksiantosopimuksen tehnyt ostaja, kohdeyhtiö ja/tai sen myyjä ja näiden mahdollinen edustaja. Tutkielman tarkoituksena ei kuitenkaan ole määrittää kaikkien tahojen rooleja, mutta niiden välisiä suhteita on välttämätöntä käsitellä jossain määrin, jotta voidaan arvioida asianajotoimiston asemaa.

Tietosuoja-asetuksen tavoitteita ja taustaa vasten peilaten mielenkiintoinen kysymys liittyy myös tietojen säilytykseen due diligence -tarkastuksessa. Tarkastusta varten perustetaan nimittäin yleensä virtuaalinen datahuone, johon käsiteltävä aineisto ladataan. Datahuoneet ovat siis pilvipalveluita, joita tarjoaa yleensä kolmas osapuoli. Pilvipalveluiden asemasta tietosuoja-asetuksen näkökulmasta löytyy jonkin verran oikeuskirjallisuutta ja aihe on luonnollisesti kiinnostava juuri asetuksen yhden tarkoituksen – eli teknologian kehitykseen vastaamisen – näkökulmasta. Tässä tutkielmassa ei kuitenkaan paneuduta tarkemmin pilvipalveluihin ja datahuoneen rooliin, vaan lähtökohtana on asianajotoimiston roolin määritteleminen teknologianeutraalisti.

Tutkielman laajuutta on rajattu myös siten, että käsitellään ainoastaan yrityskauppoja, joissa kaikki osapuolet toimivat EU:n sisällä. Asetus sisältää useita säännöksiä tapauksista, joissa tietoja siirretään EU:n ulkopuolelle tai joku käsittelyyn osallistuvista toimii EU:n ulkopuolella. Tilanteet ovat yleisiä ja esimerkiksi datahuonepalveluita tarjoavat yritykset ovat usein sijoittautuneet EU:n ulkopuolelle, mutta tässä tutkielmassa rajan yli toimintaa ei käsitellä. Rajan yli toiminta ei näet muuttaisi asianajotoimiston roolia vaan ainoastaan sitä, mitä velvollisuuksia asianajotoimistolla olisi.

Vaikka due diligence -tarkastus suoritetaan myös monissa muissa tilanteissa kuin yrityskaupoissa, tässä tutkielmassa keskitytään yrityskaupassa tehtävään tarkastukseen. Sillä, onko kyseessä esimerkiksi osake- vai liiketoimintakauppa, ei ole merkitystä tutkimuskysymyksen kannalta ja usein kaupan muoto myös tarkentuu vasta tarkastuksen jälkeen. Tutkielman ulkopuolelle on jätetty julkisesti noteeratut yhtiöt, sillä niiden osalta yrityskauppoihin liittyy sellaista erityissääntelyä, jonka vuoksi julkisten yhtiöiden käsittely ei tutkielman laajuus huomioiden ole mahdollista. Due diligence -tarkastukseen ja tietosuojaan liittyen on syytä tuoda esiin myös se seikka, ettei tässä tutkielmassa käsitellä aihetta siitä näkökulmasta, miten ostettavan yhtiön tietosuoja on due diligence -tarkastuksessa otettava huomioon.

1.3 Tutkielman rakenne, lähdemateriaali ja metodi

Tutkielman alussa käsitellään lyhyesti due diligence -tarkastusta ja sen osapuolia yleisellä tasolla, minkä lisäksi käydään läpi ne henkilötietoryhmät, joita tarkastuksessa yleisimmin käsitellään. Tarkastuksen ajankohta yrityskauppaprosessissa sekä se, ketkä tarkastukseen osallistuvat, nousee väistämättä esiin asianajotoimiston roolia arvioitaessa. Lisäksi se, mitä henkilötietoryhmiä tarkastuksessa käsitellään, on keskeinen asia yleisemminkin tietosuoja-asetuksen kannalta. Huomiota kiinnitetään tutkielman edetessä myös siihen, voidaanko kaikkia henkilötietoryhmiä käsitellä samalla tavoin kuin aiemmin. Koska due diligence -tarkastus pohjautuu pitkälti yleiseen käytäntöön eikä sen toteutusta ohjaa lainsäädäntö, on tarkastusta käsittelevässä luvussa nojauduttu pitkälti yrityskauppoja ja tarkastusta käsittelevään kirjallisuuteen.

Ennen asianajotoimiston roolin käsittelyä tutkielmassa tarkastellaan aiemmin mainitsemaani osakysymystä eli sitä, mitä oikeusperusteita käsittelylle on tietosuoja-asetuksen mukaan olemassa ja mitkä niistä voivat soveltua due diligence -tarkastukseen (luku 3). Luvussa on huomioitu tarkastuksen kohteena olevan yhtiön työntekijöiden ja johdon erilaiset asemat, joilla on merkitystä mm. sen osalta, tietävätkö käsittelyn kohteena olevat henkilöt käsittelystä.

Rekisterinpitäjän, yhteisrekisterinpitäjien ja henkilötietojen käsittelijän välisiä suhteita käsitellään kahdessa pääluvussa. Itse roolien määritelmien (luku 4) lisäksi käydään läpi myös roolien välistä vastuunjakoa (luku 5). Vastuunjakoa käytetään apuna itse tutkimuskysymykseen vastaamisessa, kun punnitaan, miten tietosuoja-asetuksen mukainen vastuunjako voisi osapuolten välillä tosiasiassa toteutua. Roolin punnitsemisessa käytetään siis avuksi myös käänteistä järjestystä, sillä henkilötietojen käsittelijöiden keskinäiset roolit muodostuvat niiden tosiasiallisten tehtävien perusteella. Vastuualueita ja jakoa tarkastellaan kuitenkin vain siltä osin, kuin se

nimenomaisesti on roolien määrittämisen tai tarkastuksen itsensä kannalta olennaista, eikä tutkielman tarkoituksena ole luoda tyhjentävää kuvaa rekisterinpitäjän tai henkilötietojen käsittelijän vastuista ja velvollisuuksista.

Tutkielmassa käytetty lähdemateriaali koostuu sekä henkilötietodirektiivin että tietosuoja-asetuksen aikaisesta materiaalista. Koska asetus on uusi, esimerkiksi oikeuskäytäntöä ei ole vielä saatavilla sen soveltamisesta. Henkilötietodirektiivin aikainen oikeuskäytäntö on kuitenkin monin paikoin soveltuvaa myös tietosuoja-asetuksen tulkinnassa ja sen vuoksi ratkaisuja käytetään myös tässä tutkielmassa. Luonnollisesti myös oikeuskirjallisuudessa direktiiviä on ehditty käsitellä asetusta enemmän. Virallislähteitä on kuitenkin käytössä myös myös tietosuoja-asetuksen soveltamisesta.

Erityisesti rekisterinpitäjän ja henkilötietojen käsittelijän määritelmiä arvioitaessa tutkielmassa on kiinnitetty huomiota määritelmien kehitykseen ja tarkastelu ulottuu aina 80-luvulle, jolloin Euroopan neuvoston jäsenvaltiot allekirjoittivat yleissopimuksen yksilöiden suojelusta henkilötietojen automaattisessa tietojenkäsittelyssä (ETS nro 108, SopS 36/1992, jäljempänä *tietosuojasopimus*). Luonnollisesti myös säädösten – erityisesti tietosuoja-asetuksen – valmisteluasiakirjat ovat tarkastelun kohteena. Roolien määritelmissä erityistä painoarvoa on lisäksi annettu henkilötietodirektiivin aikaisen tietosuojatyöryhmän (WP29) kannanotolle[14] rekisterinpitäjän ja henkilötietojen käsittelijän käsitteistä.

Tutkimuskysymykseen vastaamiseksi tässä tutkielmassa käytetään lainopillista metodia, sillä tarkoitus on selvittää, mikä on voimassa olevan oikeuden sisältö ja kuinka lakia tulee konkreettisessa tilanteessa – eli due diligence -tarkastuksessa – soveltaa.[15] Rekisterinpitäjän ja henkilötietojen käsittelijän määritelmiä tulkittaessa tutkielmassa käytetään etenkin sanamuodon mukaista tulkintaa. On kuitenkin huomattava, että lainopillisessa tutkielmassa sanamuodon mukainen tulkinta tarkoittaa ennen kaikkea sanojen oikeudellisten merkitysten analyysia ja esiintuomista, jolloin analyysi tapahtuu muun muassa oikeuslähteiden, tulkintaoppien ja argumentaation kautta.[16] Tutkielmassa käytetään hyväksi erityisesti tietosuojatyöryhmän kannanottoja sekä Euroopan unionin tuomioistuimen ennakkoratkaisuja, joiden nojalla käsitteiden merkityssisältöä arvioidaan.

[14] WP 169.
[15] *Husa – Mutanen – Pohjolainen* 2008, s. 20.
[16] *Soininen* 2015, s. 61–62.

Vaikka ydinkysymys tutkielmassa on asianajotoimiston roolin määrittelyssä, on tutkielmassa selvitetty myös muiden tietosuoja-asetuksen säännösten välisiä suhteita ja pyritty systematisoimaan sitä kokonaisuutta, joka due diligence -tarkastuksessa tulee henkilötietojen käsittelyn osalta huomioida.

Tutkimuskysymyksen ratkaisussa on lisäksi nojauduttu monelta osin teleologiseen tulkintaan, jossa normia lähestytään tarkoituksen ja päämäärän kautta. Teleologia onkin luonnollinen metodi erityisesti EU-oikeudessa, sillä sen avulla voidaan tarkastella koko sääntelyn tavoitteita yksittäisten normien sijaan.[17] Tietosuoja-asetuksen ydintavoite on luonnollisten henkilöiden perusoikeuksien ja -vapauksien, erityisesti henkilötietojen suojan, turvaaminen. Asianajotoimiston roolin määrittelyssä on siten kiinnitetty erityistä huomiota siihen, mikä vaikutus roolilla henkilötietojen käsittelijänä tai rekisterinpitäjänä on henkilötietojen suojan ja muiden rekisteröidyn oikeuksien turvaamiseen.

[17] *Talus – Penttinen* 2015, s. 241–242.

2 DUE DILIGENCE -TARKASTUS JA HENKILÖTIETOJEN KÄSITTELY

2.1 Due diligence -tarkastus ja sen osapuolet

Vaikka tutkielman tutkimuskysymykset keskittyvät henkilötietojen käsittelyyn ja tietosuojaan, valitun näkökulman vuoksi on tärkeää ymmärtää, mitä due diligence -tarkastuksella tarkoitetaan. Englanninkielestä lainattu termi due diligence, eli suomeksi *asianmukainen huolellisuus*, on vakiintunut liike-elämän termi, jolla tarkoitetaan ennen yrityskauppaa tehtävää liiketoiminnan kokonaisvaltaista arviointia erityisesti sen varojen ja velkojen määrittämiseksi sekä kaupallisen potentiaalin arvioimiseksi.[18] Due diligence on terminä vakiintunut suomalaisessa liikemaailmassa, mutta tarkastuksesta voitaisiin käyttää myös esimerkiksi nimitystä kaupan kohteen ennakkotarkastus. Yleensä due diligence -tarkastus liitetään nimenomaan yrityskauppoihin *(M&A due diligence),* mutta sillä voidaan tarkoittaa tarkastusta myös muunlaisissa yhteistyösuhteissa, jotka edellyttävät molemminpuolista luottamusta.[19] Tutkielmassa käsitellään kuitenkin juuri yrityskaupassa[20] tehtävää due diligence -tarkastusta.

Yksinkertaistettuna due diligence -tarkastuksessa arvioidaan kaupan kohteena olevaa yritystä kaupallisesta, taloudellisesta ja oikeudellisesta näkökulmasta. Sen tarkoituksena on varmistaa, että kaupan kohde vastaa ostajan odotuksia ja sitä, mitä myyjä ja ostaja ovat sopineet. Tarkastuksen tavoitteena on myös oppia ymmärtämään kohdeyritystä ja yrityskauppaan liittyviä nykyisiä tai tulevia riskejä sekä löytää ne seikat, jotka kaupasta neuvoteltaessa kannattaa ottaa huomioon.[21] Usein tarkastus on niin laaja, ettei ostajayhtiöllä ole mahdollisuutta tehdä tarkastusta itse. Etenkin suurissa yrityskaupoissa tarkastuksen tekeminen saatetaan ulkoistaa. Oikeudellista osuutta tarkastuksesta hoitaa usein asianajotoimisto ja taloudellisen sekä kaupallisen tarkastuksen tekeminen voidaan antaa esimerkiksi tilintarkastus- tai konsulttiyritykselle. Tyypillisesti toimeksiantosopimus, jossa on sovittu tarkastuksen tekemisestä, pitää sisällään myös muita yrityskauppaan liittyviä toimia, kuten kauppakirjan laatimisen. Onkin tavallista, että niin ostajaa kuin myyjääkin edustaa kaupassa asianajotoimisto, joka hoitaa prosessia yrityksen puolesta.

[18] Oxford dictionary https://en.oxforddictionaries.com/definition/due_diligence
[19] *Katramo – Lauriala – Matinlauri – Niemelä – Svennas – Wilkman* 2013, s. 50.
[20] Yrityskauppa ei ole käsitteenä täsmällinen, vaan yrityskaupasta puhuttaessa voidaan tarkoittaa erilaisia transaktioita, kuten osakekauppana toteutettavaa yrityskauppaa, liiketoimintakauppaa tai kahden yhtiön sulautumista. Tässä tutkielmassa yrityskaupan muoto ei ole tutkimuskysymyksen kannalta merkityksellinen ja monesti se, toteutuuko kauppa esimerkiksi liiketoiminta- vai osakekauppana voi riippua myös due diligence -tarkastuksen lopputuloksesta.
[21] *Howson* 2003, s. 3.

Due diligence -tarkastuksen toteuttamistapa on sinänsä vapaamuotoinen, ettei tarkastuksen sisällöstä tai tarkastusprosessista säännellä suoraan laissa.[22] Tarkastuksen tekemisen taustalla on kuitenkin ostajan huolellisuusvelvollisuus ja siitä riippuva virhevastuu. Huolellisuusvelvollisuus käy ilmi esimerkiksi kauppalaista (355/1987, jäljempänä KL). Ostaja ei saa vedota virheenä sellaiseen seikkaan, josta hänen täytyy olettaa tienneen kauppaa tehtäessä (KL 20 § 1 mom.) tai – jos ostaja on ennen kauppaa tarkastanut tavaran tai laiminlyönyt myyjän kehotuksen tarkastaa tavara – sellaiseen seikkaan, joka hänen olisi pitänyt tarkastuksessa havaita (KL 20 § 2 mom.). Ostajalla ei siis KL:n perusteella ole yleistä ennakkotarkastusvelvollisuutta, mutta myyjän kehottaessa ostajaa tarkastamaan kaupan kohteen, velvollisuus syntyy.[23] Toisaalta due diligence -tarkastusta on yrityskaupoissa pidetty myös vakiintuneena kauppatapana, joka ei perustu myyjän kehotukseen.[24]

Se, millaista huolellisuutta tarkastukselta vaaditaan, riippuu muun muassa ostajan asiantuntemuksesta.[25] Kun tavaran tarkastuksen tekee asiantuntija, huolellisuusvelvoitteen voidaan katsoa asettuvan korkealle ja tarkastuksen tulee siten olla perusteellinen. Huomionarvoista on, että asianajotoimiston hoitaessa due diligence -tarkastusta, sitoo asianajotoimistoa myös huolellisuusvelvoite ja tietyissä tapauksissa myös asianajotoimisto voi joutua vahingonkorvausvastuuseen myöhemmin ilmi tulevasta virheestä, joka tarkastuksessa olisi tullut havaita.[26]

Myös myyjä voi tehdä yrityskaupan yhteydessä oman, ostajaa koskevan tarkastuksensa. Myyjä voi ottaa selvää ostajan maineesta, taloudellisesta tilasta ja hankinnan syystä. Myyjä saattaa vaatia ostajan pankilta, taloudellisilta neuvonantajilta tai esimerkiksi asiakkailta suosituksia. Myyjä voi myös haluta selvittää ostajan aikomukset jatkaa kohdeyhtiön liiketoimintaa ja säilyttää yhtiön työntekijät sekä heidän etuutensa. Mikäli liiketoiminta kuuluu lailla säänneltävään toimialaan, myyjä voi selvittää ostajan mahdolliset rajoitteet toimia kyseisellä alalla.[27] Myyjä

[22] Tietynlaatuisissa tarkastuksissa on kuitenkin myös sitovia sääntöjä tarkastuksen sisällöstä. Esimerkiksi yrityksen listautumisessa tehtävässä due diligence -tarkastuksessa on kartoitettava yhtiön toiminnalliset ja rakenteelliset edellytykset listayhtiönä toimimiseen. (Lähde: Finanssivalvonta https://www.finanssivalvonta.fi/paaomamarkkinat/liikkeeseenlaskijat-ja-sijoittajat/listautuminen/)
[23] *Wilhelmsson – Sevón – Koskelo* 2006, s. 110.
[24] Ks. *Mäkelä* 2011.
[25] *Wilhelmsson – Sevón – Koskelo* 2006, s. 109.
[26] Ks. esim. *Harsu,* 2004. Asianajotoimisto voi olla vahingonkorvausvastuussa suhteessa ostajaan. Vastuu perustuu tällöin sopimusvelvoitteen rikkomiseen ja siihen, että työprosessista on poikettu. Pelkkä väärän neuvon antaminen ei siten johtane korvausvastuuseen. Jos prosessissa ei ole noudatettu hyvää asianajajatapaa tai muuta ammatillista standardia, korvausvastuu voi realisoitua.
[27] *Mora* 2008.

voi toisaalta teettää due diligence -tarkastuksen myös myytävästä yhtiöstä, kuten seuraavassa alaluvussa on tuotu esiin.

2.2 Due diligence -tarkastus osana yrityskauppaa

Onnistuneen yrityskaupan syntyminen vaatii perusteellisen due diligence -tarkastuksen lisäksi myös muutoin huolellista toimintaa koko kauppaan liittyvän prosessin ajan. Kaupanteon vaiheet ja rakenne riippuvat siitä, tekeekö kaupantekoprosessia koskevan aloitteen myyjä vai ostaja. Mikäli ajatus yrityskaupasta tulee myyjän puolelta, prosessi aloitetaan päättämällä ensiksi menetelmästä, jolla sopiva ostaja valitaan. Myyjä voi neuvotella kaupasta sopivaksi katsomansa ostajan kanssa suoraan kahdenkeskisesti tai järjestää kaupan kohteesta rajoitetun tai avoimen huutokaupan. Rajoitetussa huutokaupassa prosessiin valitaan yleensä 5-20 ostajaehdokasta, joista prosessin aikana karsitaan ostajaehdokkaita pois, kunnes kauppa syntyy. Rajoitettu huutokauppa voi alkaa esimerkiksi investointipankin tekemällä ennakkotiedustelulla, joka lähetetään potentiaalisille ostajille.[28] Avoimessa huutokaupassa ensimmäiselle kierrokselle pääsevät kaikki halukkaat ostajaehdokkaat ja karsinta alkaa vasta myöhemmässä vaiheessa.[29]

Ostajan alkaessa suunnitella yhtiön hankkimista, prosessi lähtee liikkeelle hankintastrategian kehittämisestä. Strategiassa tuodaan esiin hankinnan syy, joka voi olla esimerkiksi uusille markkinoille pääseminen tai kasvu muuten, sekä odotukset, joita yrityskaupan toteutumiseen liittyy.[30] Syy yrityskaupalle voi olla myös esimerkiksi sellaisen tuotteen saaminen yhtiön valikoimaan, joka täydentää yhtiön nykyistä tuotevalikoimaa tai jota yhtiö voi helposti myydä jo olemassa oleville asiakkailleen.[31] Strategian lisäksi ostaja asettaa hankittavalle yritykselle kriteerejä, joita voivat olla esimerkiksi hankittavan yrityksen voittomarginaali, yrityksen käyttämä teknologia, asiakaskunta ja maantieteellinen sijainti.[32] Strategia ja kriteerit määrittävät myös sitä, millaisiin asioihin due diligence -tarkastuksessa tulee kiinnittää huomiota.

Kun ostaja on päättänyt hankintastrategiasta ja kriteereistä, se alkaa etsiä sopivaa kohdetta. Ostaja voi etsiä sopivaa kohdetta joko itsenäisesti tai käyttäen apunaan erilaisia välikäsiä, kuten investointipankkia, tilitoimistoa tai asianajotoimistoa, joiden kautta tieto ostajan ostoaikeista

[28] *Katramo – Lauriala – Matinlauri – Niemelä – Svennas – Wilkman* 2013, s. 335.
[29] *Katramo – Lauriala – Matinlauri – Niemelä – Svennas – Wilkman* 2013, s. 61–63.
[30] Corporate Finance Institute, Mergers Acquisitions M&A Process.
[31] *Davis – Kummer* 2012, s. 4.
[32] *Hooke* 2014, s. 43.

leviää markkinoille helpommin ja saattaa herättää potentiaalisten myyjien kiinnostuksen.[33] On myös mahdollista, että ostaja lähestyy kohdeyhtiötä tai sen omistajia suoraan ilman, että omistajalla on ollut suunnitelmia kohdeyrityksen myymiseksi.[34]

Riippumatta siitä, miten ja kumman osapuolen aloitteesta yrityskauppaprosessi on alkanut, on kaupantekoprosessi monivaiheinen. Sekä ostajan (tai ostajaehdokkaiden) että myyjän on yrityskauppaa suunnitellessaan kiinnitettävä tahoillaan huomiota ensinnäkin transaktiorakenteen suunnitteluun. Kaupan rakenteella on vaikutusta muun muassa maksettaviin veroihin, investointitarpeisiin sekä pääoma- ja konsernirakenteisiin. Neuvotteluprosessin aikana osapuolten tavoite on päästä yhteisymmärrykseen kaupan kohteesta ja yrityskaupan ehdoista. Neuvottelut voivat kestää pitkäänkin, sillä tarkoituksena on muun muassa identifioida kaupan kohde, varmistaa myyjän oikeus tehdä kauppa ja ottaa alustavasti selvää ostettavan yrityksen taustasta ja tilasta.[35] Neuvottelujen aikana käydäänkin läpi ostajan ja myyjän kesken samoja asioita, jotka ostaja (tai huutokaupassa useampi ostajaehdokas) sittemmin varmistaa due diligence -tarkastuksessa.

Tarkastuksen ajankohta ja rakenne riippuvat siitä, onko kyseessä suora osto- tai myyntitarjous vai huutokauppa. Huutokaupassa tarkastuksen tekoon voi ryhtyä useampi ostajakandidaatti, joiden kanssa myyjä solmii salassapitosopimuksen ennen tietojen luovuttamista. Etenkin huutokaupoissa myyjä teettää usein myös itse due diligence -tarkastuksen yhtiöstään. Tarkastuksen avulla myyjä saa tilaisuuden korjata raportissa mahdollisesti esiin tulleita ongelmia ja lisäksi tarkastus voi sisältää arvokasta tietoa kohdeyhtiöstä etenkin niissä tilanteissa, joissa kohdeyhtiö on osa konsernia ja myyjäpuolta edustaa esimerkiksi konsernin emoyhtiön hallitus, jolla ei ole tarkkoja tietoja kohdeyhtiöstä.[36] Tarkastuksen tehtyään myyjä voi toimittaa tarkastuksesta saadun raportin ostajakandidaateille, mikä vähentää ostajapuolen työn määrää tarkastuksessa.[37]

Due diligence -tarkastus vaatii yleensä ostajalta huomattavaa taloudellista panostusta, minkä vuoksi huutokauppaprosessi ei välttämättä ole ostajaehdokkaalle kannattavin vaihtoehto. Koska ostajaehdokkaiden tekemän due diligence -tarkastuksen jälkeen kandidaatteja karsitaan yhä, tarkastukseen liittyy riski siitä, että siihen on käytetty resursseja turhaan.[38] Usein ostaja haluaa

[33] *Hooke* 2014, s. 48–49.
[34] *Mora* 2008.
[35] *Katramo – Lauriala – Matinlauri – Niemelä – Svennas – Wilkman* 2013, s. 46–47.
[36] *Sher* 1998, s. 15.
[37] *Katramo – Lauriala – Matinlauri – Niemelä – Svennas – Wilkman* 2013, s. 336.
[38] *Katramo – Lauriala – Matinlauri – Niemelä – Svennas – Wilkman* 2013, s. 336.

etukäteen varmistua siitä, ettei prosessia aloiteta turhaan ja että kaupan toteutumista voidaan pitää varmana, mikäli tarkastuksessa ei ilmene mitään poikkeavaa. Tämän vuoksi kahdenkeskiset yrityskauppaneuvottelut ovatkin ostajan kannalta kannattavampia. Lisäksi pitkälle edennyt due diligence -tarkastus parantaa usein ostajan neuvotteluasemaa sen saadessa lisätietoa kaupan kohteesta[39], mikä lisää myyjän tarvetta varmistua kaupasta.

Kahdenkeskisissä neuvotteluissa osapuolet solmivat usein ennen tarkastusta ns. aiesopimuksen (*letter of intent),* josta käyvät ilmi ainakin suunnitellun yrityskaupan pääasialliset ehdot ja alustavasti sovittu hinta, mutta sopimuksen laajuus ja yksityiskohtaisuus vaihtelevat. Joskus kaupan ehdoista voidaan sopia jo aiesopimuksessa tarkastikin. Aiesopimuksessa on yleensä mainittu, ettei se ole sitova sopimus lukuun ottamatta tiettyjä, erikseen määriteltyjä kohtia, jotka liittyvät usein esimerkiksi aiheutuneiden kustannusten jakoon, luottamuksellisuuteen ja salassapitovelvollisuuteen.[40] Salassapidosta on tarpeellista sopia tiukasti viimeistään ennen due diligence -tarkastuksen aloittamista, sillä on myyjän intressi varmistua siitä, että hankkeen mahdollisesti kariutuessa sen liikesalaisuudet ovat turvassa.[41]

Kun salassapito- tai aiesopimus on tehty, ryhtyvät osapuolet tahoillaan tekemään due diligence -tarkastusta. Se, että kohdeyritys vastaa sovittua, vaikuttaa paitsi yrityksen arvoon ja siten kaupasta maksettavaan hintaan myös siihen, voiko ostaja käyttää kaupan kohdetta suunnittelemallaan tavalla. Mikäli tarkastuksessa tulee ilmi ennakko-odotuksista poikkeavia seikkoja, vaikuttaa se ostajaehdokkaiden tarjouksiin ja lopulta toteutettavan yrityskaupan ehtoihin. Niin huutokaupassa kuin suorassa kaupassa on myös mahdollista, että due diligence -tarkastus on jaettu useampaan vaiheeseen, jolloin sensitiivisimmät tiedot annetaan ostajalle vasta kauppakirjan allekirjoittamisen jälkeen. Kauppakirja on tällaisissa tapauksissa ehdollinen siten, että mikäli vielä esiin tulevat tiedot vaikuttavat kohteeseen ja sen arvoon negatiivisesti, ostaja voi vetäytyä kaupasta.[42]

Kun due diligence -tarkastus on suoritettu, saatetaan kauppaneuvottelut loppuun.[43] Se, miten laajoja neuvotteluja tarkastuksen jälkeen käydään, riippuu sekä tarkastuksen tuloksista että teh-

[39] *Katramo – Lauriala – Matinlauri – Niemelä – Svennas – Wilkman* 2013, s. 51.
[40] *Harroch* 2015.
[41] *Vapaavuori* 2019, s. 636–637. Myyjän on tarpeen huolehtia myös siitä, että ns. ilmaisukiellon lisäksi tarkastuksen tekijä sitoutuu olemaan itse käyttämättä saamiaan tietoja liiketoiminnassaan, jos yrityskauppa ei toteudu.
[42] *Katramo – Lauriala – Matinlauri – Niemelä – Svennas – Wilkman* 2013, s. 51–52.
[43] *Katramo – Lauriala – Matinlauri – Niemelä – Svennas – Wilkman* 2013, s. 52.

dyn aiesopimuksen tarkkuudesta. Mikäli ostaja tarkastuksen jälkeen toteaa kohdeyrityksen vastaavan ennakko-odotuksia ja aiesopimuksessa ehdot on neuvoteltu yksityiskohtaisesti, eivät lopulliset neuvottelut oletettavasti osoittaudu hankaliksi. Mikäli taas ostaja on tarkastuksessa saanut tietoonsa yllättäviä, ostohalukkuuteen negatiivisesti vaikuttavia tekijöitä, joiden vuoksi ostajan hankintastrategia tai kriteerit eivät täyty, neuvoteltavaa on enemmän. Myös laveasti ja epätarkasti kirjoitettu aiesopimus vaikuttaa samalla tavoin.

2.3 Due diligence -tarkastus ja henkilötiedot

2.3.1 Johto ja omistajat

Kuten edellä due diligence -tarkastusta määriteltäessä on todettu, tarkastus tehdään yleensä ainakin kaupallista, taloudellista ja oikeudellista näkökulmaa käyttäen. Näkökulmajaottelun lisäksi due diligence -prosessi voidaan jakaa vielä yksityiskohtaisemmin eri lajeihin. Lajit riippuvat yrityskaupan kohteesta, käytettävistä resursseista ja transaktion muodosta.[44] Yrityskaupan kohde ja sen toimiala määrittelevät, tuleeko tarkastuksessa ottaa huomioon joitakin erityisalueita, kuten immateriaalioikeuksia. Resurssit taas vaikuttavat esimerkiksi siihen, kuinka paljon tarkastuksesta ostajan kannattaa tehdä itse ja mitä tarkastuksessa ulkoistetaan. Transaktion muoto taas vaikuttaa laajuuteen: osakekaupassa tarkastuksen on syytä olla tarkempi ja laajempi kuin liiketoimintakaupassa, jossa esimerkiksi yhtiön varat ja velat jäävät yleensä kaupan ulkopuolelle. Koska tutkielmassa käsitellään asianajotoimiston tietosuojavelvoitteita, tässä luvussa tarkastelu on rajattu niihin keskeisimpiin oikeudellisen due diligencen lajeihin, joiden tarkastamisesta asianajotoimisto yleensä vastaa ja joissa useimmiten käsitellään henkilötietoja.

Yksi tärkeimmistä henkilötietoja sisältävästä lajista due diligence -tarkastuksessa on kohdeyhtiön johtoa koskeva due diligence (*management due diligence*). Koska yhtiöt voivat yleensä päättää melko vapaasti toimintansa organisoinnista, myös johtoon kuuluvat elimet ja henkilöt vaihtelevat. Osakeyhtiössä ainoa pakollinen, johtoon kuuluva toimielin on hallitus (OYL 6:1.1). Mikäli hallitukseen kuuluu vähemmän kuin kolme varsinaista jäsentä, hallituksella on oltava yksi varajäsen (OYL 6:8.1). Useimmiten yrityskaupoissa, joissa due diligence -tarkastus on ulkoistettu, kohdeyhtiöt ovat kuitenkin suurempia ja myös hallituksen jäseniä on useampia. Lisäksi OYL 6 luvun 1 §:n 1 momentissa säädetään, että yhtiöllä voi olla toimitusjohtaja ja hallintoneuvosto. Laissa mainittujen johtoon kuuluvien elinten lisäksi yhtiössä voi olla myös muita

[44] *Katramo – Lauriala – Matinlauri – Niemelä – Svennas – Wilkman* 2013, s. 51.

johto-organisaatioita, kuten erilaisia valiokuntia ja johtoryhmä, jonka kautta yhtiön operatiivinen johto voi olla järjestetty.[45]

Johtoa koskevassa due diligence -tarkastuksessa käydään läpi niin johtoa yleisesti koskevia asioita kuin johtohenkilöiden työtehtäviin ja ammattitaitoon liittyviä seikkoja. Koko johtoa tarkasteltaessa kiinnitetään huomiota muun muassa siihen, kuinka paljon johdon jäsenillä on heille suoraan raportoivia henkilöitä ja miten työtehtävät on yhtiössä delegoitu. Lisäksi esimerkiksi johdon päivittäisen toiminnan toteutuminen ja palkkioiden määräytyminen koskevat koko johtoa.[46] Henkilötasolla tarkastuksessa käydään läpi johtoa koskevia perustietoja, kuten johtoon kuuluvien henkilöiden ikää, palvelusvuosia ja osallistumista johdon komitearyhmiin ja mahdollisia omistusosuuksia kohdeyhtiöstä sekä mahdollisesti muista yhtiöistä.[47] Tarkastus tehdään keräämällä yhtiön johdosta kirjallista tietoa, kuten ansioluetteloita, arvioita ja suosituksia sekä yhtiön organisaatiokaavioita ja muita asiakirjoja, mutta laajuudesta riippuen tarkastukseen voi sisältyä myös esimerkiksi johtohenkilöiden haastatteluja tai työskentelyn tarkkailua.[48] Tarkastuksessa voidaan myös selvittää johtohenkilöiden mielipiteitä yrityskaupasta.[49]

Luonnollisesti erityisesti yksittäisiä johtohenkilöitä koskevat tiedot sisältävät henkilötietoja ja niiden käsittelyyn on siten sovellettava tietosuoja-asetusta. Useimmiten johtoon kuuluvat henkilöt ovat kuitenkin tietoisia suunnitteilla olevasta yrityskaupasta ja henkilöt ovat antaneet suostumuksensa henkilötietojen käsittelyyn. Tältä osin johdon due diligence -tarkastus on tietosuoja-asetuksen näkökulmasta joiltakin osin eri asemassa kuin esimerkiksi työntekijöitä koskeva tarkastus.

Johdon lisäksi due diligence -tarkastuksessa käsitellään myös kohdeyhtiön omistajien henkilötietoja. Jotta transaktio voidaan toteuttaa onnistuneesti ja jotta sen lopputulos on oikeudellisesti pätevä, tulee ostajan varmistua ensinnäkin siitä, että tahot, joilta kohdeyhtiön osakkeet hankitaan, ovat varmasti osakkeiden laillisia omistajia.[50] Jos yhtiön osakkeet on liitetty arvo-osuusjärjestelmään, omistajatiedot käyvät ilmi järjestelmästä ja muussa tapauksessa tiedot saadaan yhtiön hallituksen pitämästä osakasluettelosta (OYL 3:15.1). Osakasluettelo tulee osakeyhtiölain mukaan pitää kaikkien nähtävissä joko yhtiön pääkonttorissa tai, mikäli yhtiö on liitetty

[45] *Mähönen – Villa* 2010, s. 217.
[46] *Crilly – Sherman* 2010, s. 70.
[47] *Crilly – Sherman* 2010, s. 68–69, 73.
[48] *Howson* 2003, s 127–128.
[49] *Crilly – Sherman* 2010, s. 84.
[50] *Howson* 2003, s. 70.

arvo-osuusjärjestelmään, arvopaperikeskuksen toimipaikassa Suomessa (OYL 3:17.1). Omistajatiedot ovat siis julkisia. Vaikka kaikilla omistajilla ei tarkastuksen aikana olisi tietoa suunnitellusta yrityskaupasta, he ovat tietoisia siitä, että heidän omistusosuutensa ovat saatavilla ja kuka tahansa voi tarkastella niitä.[51]

2.3.2 Kohdeyhtiön työntekijät

Johdon ja omistajien lisäksi yksi merkittävimmistä – kenties merkittävin – due diligencen lajeista henkilötietojen käsittelyn näkökulmasta on kohdeyhtiön työntekijöitä koskeva due diligence. Tarkastusta ja sen laajuutta suunniteltaessa on hyvä huomioida ainakin yrityskaupan syy ja liiketoiminnan luonne: mikäli yhtiö ostetaan esimerkiksi sen vuoksi, että sen toiminta voidaan lopettaa ja siten karsia kilpailua, tulee tarkastuksessa pohtia erityisesti irtisanomisista aiheutuvia kustannuksia. Liiketoiminnan luonne taas ratkaisee sen, tuleeko tarkastuksessa ottaa huomioon esimerkiksi työtapaturmien määrä tai vaikkapa työntekijöille mahdollisesti annetut optio-oikeudet yhtiön osakkeiden hankkimiseen.[52]

Yrityskauppakohtaisten selvitysten ja tarkastusten lisäksi lähes kaikissa yrityskaupoissa tarkastetaan henkilöstöön liittyviä perusasioita, joihin kuuluvat esimerkiksi työntekijöiden palkat, työsuhde-edut, työsuhteiden luonne (mahdolliset osa-aikaiset tai määräaikaiset työntekijät), päällekkäiset työtehtävät ostaja- ja kohdeyhtiössä sekä työnantajan piilevät vastuut ja velvollisuudet.[53] Kohdeyhtiön työntekijöistä luovutetaan siis huomattava määrä tietoja due diligence -tarkastusta tekevälle taholle, sillä edellä lueteltuja asioita pystytään arvioimaan ainoastaan työsopimusten ja muun kirjallisen dokumentaation, kuten erillisten optiosopimusten, nojalla.

Vaikka työ- ja optiosopimukset sisältävät poikkeuksetta henkilötietoja, useissa tapauksissa henkilötietojen luovuttamista voidaan – tai on tietosuoja-asetuksen noudattamisen vuoksi jopa välttämätöntä – rajoittaa esimerkiksi luovuttamalla tarkastuksen tekijälle ainoastaan sopimuspohjat (ja niiden työntekijöiden lukumäärä, joiden työsuhteeseen kutakin sopimusta käytetään), joista tarkastuksen kannalta tarpeelliset tiedot käyvät ilmi. Tällöin tarkastuksessa ei ns. rivityönteki-

[51] CJEU on katsonut, että se, että henkilötiedot ovat jo yleisön saatavilla, voidaan ottaa huomioon esimerkiksi jäljempänä käsiteltävää oikeutettua etua punnittaessa. Julkisuus voi vaikuttaa muun muassa rekisteröidyn perusoikeuksiin henkilötietojen käsittelyn vuoksi mahdollisesti kohdistuvan loukkauksen vakavuuteen. (Yhdistetyt asiat C-468/10 ja C-469/10, *ASNEF,* kohta 44 ja asia C-13/16, kohta 32.)
[52] *Howson* 2003, s. 106–107.
[53] *Howson* 2003, s. 110–112.

jöiden osalta käsiteltäisi lainkaan henkilötietoja, mikä osaltaan helpottaa muun muassa henkilötietojen käsittelyn lainmukaisuuden perustelemista tarkastuksessa. Käsittelyn lainmukaisuuden edellytysten täyttyminen on nimittäin hankalinta juuri työntekijöiden osalta.

Yrityskaupassa voi toisinaan olla kysymys myös erityisen tietotaidon tai osaamisen hankkimisesta. Tällaisissa tapauksissa kohdeyhtiön työntekijät – tai osa heistä – voivat olla yrityskaupan kannalta niin tärkeitä, että tarkastuksessa on välttämätöntä käsitellä kyseisten työntekijöiden henkilötietoja. Työntekijät voivat olla yhtiön avainhenkilöitä esimerkiksi suuren vastuualueensa, osaamisensa tai laajojen verkostoidensa vuoksi. Tällöin on tavallista, että tarkastuksessa halutaan saada selville muun muassa avainhenkilöiden halukkuus jatkaa työtehtävissään myös yrityskaupan jälkeen. On tavallista, että tällaisille henkilöille on jo ennen due diligence -vaihetta annettu tieto suunnitteilla olevasta yrityskaupasta,[54] sillä avainhenkilöiden sitouttaminen yritykseen ja yrityskauppaan voivat olla jopa edellytyksenä kaupan toteutumiselle ostajaehdokkaan näkökulmasta.[55]

Kohdeyrityksen liiketoiminnan luonteesta riippuen myös muihin due diligence -tarkastuksen lajeihin liittyy vaihteleva määrä henkilötietojen käsittelyä. Jos yrityskaupan kohteeseen kuuluu esimerkiksi kiinteistöjä, tarkastellaan muun muassa maanomistajien ja erityisten oikeuksien haltijoiden henkilötietoja. Tutkimuskysymysten kannalta ei kuitenkaan ole oleellista käydä läpi kaikkia mahdollisia henkilötietoryhmiä, vaikkakin samat tietosuojasäännökset ja -periaatteet soveltuvat myös muuhun henkilötietojen käsittelyyn due diligence -tarkastuksessa. Kun tutkielmassa käsitellään työntekijöiden henkilötietojen käsittelyä, voidaan samoja periaatteita soveltaa myös osittain myös esimerkiksi sellaisiin osakkeenomistajiin, joilla ei ole tietoa yrityskaupasta.

[54] Lisäksi avainhenkilöt voivat olla samalla myös johtoon kuuluvia henkilöitä, jolloin heillä on tieto suunnitellusta kaupasta valmiiksi.
[55] *Mäkelä* 2011, s. 121. Avainhenkilöiden pysyminen kohdeyhtiössä on syytä ottaa huomioon jo tarkastuksessa.

3 HENKILÖTIETOJEN KÄSITTELYN OIKEUSPERUSTA DUE DILIGENCE -TARKASTUKSESSA

3.1 Oikeus käsitellä henkilötietoja

Henkilötietojen käsittelylle tulee olla lainmukainen peruste. Vaatimus lainmukaisuudesta on yksi käsittelyä koskevista periaatteista ja se on sisällytetty tietosuoja-asetuksen 5 artiklan 1(a) kohtaan. Käsittelyn lainmukaisuus puolestaan on määritelty tietosuoja-asetuksen 6 artiklassa, jonka 1 kohdassa on säädetty kuusi perustetta henkilötietojen käsittelylle. Käsittely on lainmukaista ainoastaan, jos – ja vain siltä osin, kuin – vähintään yksi artiklan edellytyksistä täyttyy. Ennen tietosuoja-asetuksen voimaantuloa käsittelyn lainmukaisuus oli määritelty henkilötietodirektiivin 7 artiklassa, jossa lainmukaisuuden edellytykset oli määritelty lähes samalla tavoin kuin tietosuoja-asetuksessa.

Mikäli käsiteltävät tiedot kuuluvat erityisiin henkilötietoryhmiin eli ovat arkaluontoisia, käsittely on lähtökohtaisesti kiellettyä (tietosuoja-asetuksen 9 artiklan 1 kohta). Saman artiklan 2 kohdassa on kuitenkin säädetty poikkeukset kieltoon ja arkaluontoisten tietojen käsittelylle on siten omat lisäedellytyksensä.[56] Arkaluonteisten tietojen käsittely on jätetty tämän tutkielman ulkopuolelle, sillä tarve käsitellä arkaluontoisia tietoja due diligence -tarkastuksessa lienee harvinaista, ellei kokonaan poissuljettavaa.[57]

Henkilötietojen käsittely voi tietosuoja-asetuksen 6 artiklan 1 kohdan mukaan olla laillista kuudella eri perusteella. Perusteena voi olla rekisteröidyn suostumus, sopimuksen täytäntöönpano tai valmistelu, rekisterinpitäjän lakisääteisen velvoitteen noudattaminen, elintärkeiden etujen suojaaminen, yleinen etu tai julkisen vallan käyttö sekä rekisterinpitäjän tai kolmannen osapuolen oikeutettujen etujen toteutuminen. Joissakin tapauksissa henkilötietojen käsittelyyn voi soveltua myös useampi edellytys, kuten suostumus ja oikeutettu etu, yhtä aikaa.[58] Lisäksi saman artiklan 4 kohdassa on säädetty lisäedellytyksiä, jotka rekisterinpitäjän on huomioitava, mikäli tietoja käsitellään muussa tarkoituksessa, kuin mihin ne on kerätty. Due diligence -tarkastuksessa suuri osa tiedoista – kuten työntekijöitä koskevat tiedot – on alun perin kerätty muuta tarkoitusta, kuin yrityskauppaa varten. Sen vuoksi useissa tilanteissa on 1 kohdan edellytysten lisäksi sovellettava myös artiklan 4 kohtaa.

[56] *Hanninen – Laine – Rantala – Rusi – Varhela* 2017, s. 29.
[57] Lisäksi mahdollisuus käsitellä arkaluontoisia tietoja due diligence -tarkastuksessa sulkeutuisi todennäköisesti pois jo sillä perusteella, ettei 9 artiklan mukaisten edellytysten täyttyminen tarkastuksessa liene mahdollista.
[58] *Hanninen – Laine – Rantala – Rusi – Varhela* 2017, s. 29.

Kun kyseessä on kahden yksityispuolella toimivan yrityksen kauppa ja siihen liittyvä due diligence -tarkastus, käsittelyperusteena voidaan selkeimmin pitää suostumusta ja/tai rekisterinpitäjän tai kolmannen oikeutettua etua. Kyseiset edellytykset ovat siirtyneet tietosuoja-asetukseen henkilötietodirektiivistä lähes sellaisenaan, minkä vuoksi muun muassa henkilötietodirektiivin ajalta olevaa oikeuskäytäntöä voidaan käyttää apuna myös tietosuoja-asetuksen 6 artiklaa sovellettaessa ja tulkittaessa. Suostumukseen, oikeutettuun etuun ja henkilötietojen käsittelyyn muussa kuin alkuperäisessä tarkoituksessa pureudutaan tarkemmin seuraavissa alaluvuissa.

Suostumuksen ja oikeutetun edun lisäksi asetuksen 6 artiklassa on neljä muuta käsittelyperustetta, jotka eivät näyttäisi soveltuvan henkilötietojen käsittelyyn due diligence -tarkastuksessa. Selkeimmin tarkastukseen soveltumaton peruste lienee artiklan 1(d) kohta, jonka mukaan käsittely on lainmukaista, jos käsittely on tarpeen rekisteröidyn tai toisen luonnollisen henkilön elintärkeiden etujen suojaamiseksi. Tällaisia etuja voivat olla yksilön henkeen liittyvät edut ja esimerkiksi henkilötietojen käsittely epidemioiden tai luonnonkatastrofien yhteydessä voi olla oikeutettu kyseisen edellytyksen perusteella.[59] Muun muassa matkustamiseen ja lentoliikenteeseen liittyvät vaaratilanteet voivat antaa perusteen käsitellä henkilötietoja tämän edellytyksen nojalla.[60] Yrityskaupoissa kyseistä edellytystä ei siten voida soveltaa.

Myöskään 6 artiklan 1(c) tai 1(e) kohdissa mainittavien edellytysten ei voitane katsoa täyttyvän yrityskaupassa. Alakohdassa c edellytyksenä käsittelylle on, että se on tarpeen rekisterinpitäjän lakisääteisen velvoitteen noudattamiseksi. Alakohdassa e taas edellytetään käsittelyn tarpeellisuutta yleisen edun tai rekisterinpitäjälle[61] kuuluvan julkisen vallan käyttämiseksi. Nähdäkseni alakohdat ovat ainakin osin päällekkäisiä ja ne soveltuvat usein myös yhtä aikaa. Esimerkiksi julkisen vallan käyttö perustuu lakiin ja on siten ainakin osin katsottavissa myös lakisääteisen velvoitteen noudattamiseksi. Ajatusta tukee myös tietosuoja-asetuksen johdanto-osio, jossa kyseisiä alakohtia käsitellään samassa kohdassa.

[59] Tietosuoja-asetuksen johdanto, kohta 46.
[60] *Hanninen – Laine – Rantala – Rusi – Varhela* 2017, s. 31.
[61] Sekä c että d alakohtien soveltuvuutta arvioitaessa on kiinnitettävä erityistä huomiota siihen, mitkä tahot tarkastusta tehtäessä ovat *rekisterinpitäjiä*. Jotta alakohtien soveltumista due diligence -tarkastukseen voitaisiin tarkemmin arvioida, tulisi ensin ratkaista, missä roolissa yrityskaupan osapuolet ovat tietosuoja-asetuksen näkökulmasta. Kyseisten käsittelyperusteiden osalta syvempää arviota ei kuitenkaan ole tarpeellista tehdä, sillä ne eivät muilta osin näyttäisi soveltuvan perusteeksi due diligence -tarkastuksessa.

Peruste käsittelylle tulee olla unionin tai jäsenvaltion lainsäädännössä ja esimerkiksi terveydenhuoltopalveluiden hallinto voidaan katsoa tällaiseksi tilanteeksi.[62] Edellytykset ovat useimmiten käytettävissä julkisen sektorin puolella tapahtuvassa henkilötietojen käsittelyssä, mutta myös yksityisoikeudellisilla toimijoilla voi olla oikeus käsitellä tietoja jommankumman lainkohdan nojalla.[63] Vaikka monet tarkastuksessakin käsiteltävistä tiedoista on alun perin saatettu kerätä lakisääteisen velvoitteen vuoksi (esimerkiksi tiedot yhtiön osakkeista ja omistajista), tilanteet, joissa yrityskauppa tai sitä edeltävä due diligence -tarkastus tehtäisiin lakisääteisen velvoitteen noudattamiseksi, lienevät harvinaisia elleivät mahdottomia. Yrityskaupan toteuttaminen yleistä etua koskevan tehtävän suorittamiseksi tai julkisen vallan käyttämiseksi tuntuvat myös kaukaa haetuilta ja siksi myöskään e alakohdan ei lähtökohtaisesti voida katsoa olevan oikeusperusta henkilötietojen käsittelylle due diligence -tarkastuksessa.

Neljäs edellytys, jonka täyttyminen due diligence -tarkastuksessa on epätodennäköistä, on artiklan 1 kohdan b alakohta, jonka mukaan käsittely on sallittua sellaisen sopimuksen, jossa rekisteröity on osapuolena, täytäntöön panemiseksi tai valmistelemiseksi rekisteröidyn pyynnöstä. Lähtökohtaisesti yrityskaupan osapuolia ovat oikeushenkilöt, jonka puolesta luonnolliset henkilöt toimivat. Näin ollen rekisteröity ei ole sopimuksen osapuoli. Lisäksi, kuten aiemmin luvussa 2.3.2 on todettu, rekisteröity (esimerkiksi työntekijä) ei välttämättä tiedä suunnitteilla olevasta yrityskaupasta, eikä rekisteröity voisi siten muutenkaan pyytää toimenpiteiden toteuttamista sopimuksen tekemiseksi. Oikeuskirjallisuudessa 1(b) kohdan edellytyksen on katsottu täyttyvän lähinnä asiakas- tai potilassuhteissa.[64]

3.2 Tarkastuksen kohteen suostumus

3.2.1 Suostumuksen käsite

Henkilötietojen käsittely on tietosuoja-asetuksen 6 artiklan 1 kohdan a alakohdan mukaan lainmukaista, mikäli rekisteröity on antanut siihen suostumuksensa. Suostumus tulee antaa tiettyä, erityistä tarkoitusta varten. Tämä tarkoittaa, että due diligence -tarkastuksessa henkilötietoja

[62] Tietosuoja-asetuksen johdanto, kohta 45.
[63] *Korpisaari – Pitkänen – Warma-Lehtinen* 2018, s. 103–104. Esimerkkinä yksityisoikeudellisesta toimijasta voidaan pitää esimerkiksi yhdistystä, jolla on lakisääteinen velvollisuus pitää jäsenrekisteriä, josta käyvät ilmi jokaisen jäsenen nimi ja kotipaikka.
[64] Ks. esim. *Hanninen – Laine – Rantala – Rusi – Varhela* 2017, s. 30 ja *Korpisaari – Pitkänen – Warma-Lehtinen* 2018, s. 102–103.

saa käsitellä suostumuksen nojalla ainoastaan, jos suostumus on annettu nimenomaisesti tarkastusta varten. Mikäli henkilötiedot on kerätty suostumuksen nojalla jotakin muuta tarkoitusta – kuten työsuhdetta – varten ja niitä halutaan käyttää tarkastuksessa, olisi rekisteröidyltä tarkastusta varten pyydettävä uusi suostumus.[65]

Lainkohta eroaa aikaisemmin voimassa olleesta henkilötietodirektiivistä siten, että direktiivissä käsittelyn lainmukaisuuden perusteena oli *yksiselitteisesti* annettu suostumus (7 artiklan a kohta). Suostumus oli lisäksi määritelty direktiivin 2 artiklassa vapaaehtoiseksi, yksilöidyksi ja tietoiseksi tahdon ilmaisuksi. Tietosuoja-asetuksen myötä suostumus on pysynyt oikeusperusteena melko samankaltaisena kuin direktiivissäkin[66], mutta asetuksessa suostumus on pyritty määrittelemään direktiiviä tarkemmin. Erona henkilötietodirektiiviin on erityisesti se, että asetuksessa on määritelmän ja lainmukaisuuden lisäksi artikla, joka käsittelee suostumuksen edellytyksiä. Edellytykset ovat menettelytapoja[67], joiden noudattaminen on suostumuksen pätevyyden edellytys. Edellytyksiä ja niiden täyttymistä due diligence -tarkastuksessa käsitellään seuraavassa alaluvussa.

Tietosuoja-asetuksen 4 artiklan 11 kohdan mukaan suostumuksen tulee olla vapaaehtoinen, yksilöity, tietoinen ja yksiselitteinen. Samat kriteerit kävivät selkeästi ilmi myös direktiivin suostumusta käsittelevistä artikloista. Suostumus voidaan antaa sitä ilmaisevalla lausumalla tai toteuttamalla toimi, joka ilmaisee suostumuksen selkeästi. Due diligence -tarkastuksessa tällaisen toimen toteuttamisena voitaneen pitää esimerkiksi avainhenkilön tai johdon jäsenen osallistumista haastatteluun tarkastuksen osana. Haastateltavalla henkilöllä tulee tällöin olla tieto siitä, mitä tarkoitusta (suunnitteilla olevaa yrityskauppaa tai due diligence -tarkastusta) varten haastattelua tehdään.

Myös esimerkiksi itseään koskevien tietojen lähettäminen tarkastuksen tekijälle tai tietojen lataaminen datahuoneeseen voitaisiin katsoa sellaisen toimen toteuttamiseksi, jolla ilmaistaan suostumus. Tietojen lähettäminen voidaan kuitenkin katsoa suostumukseksi vain, jos lähetetyt

[65] Tietosuoja-asetuksen johdanto-osan mukaan, jos henkilötietojen käsittelyllä on useita tarkoituksia, suostumus on annettava kaikkia niitä varten. Tämä on toisaalta pääteltävissä myös asetuksen 6 artiklassa käytettävästä sanamuodosta, jonka mukaan suostumus on annettava yhtä tai useampaa tarkoitusta varten.
[66] Tietosuojavaltuutetun toimisto 14.5.2018.
[67] Tietosuojavaltuutetun toimisto 14.5.2018.

tiedot koskevat itse lähettäjää; jos lähettäjä toimittaa tietoja myös muista henkilöistä, lähettämistä ei voida pitää asetuksen mukaisena suostumuksena.[68] On myös mahdollista, että rekisteröidyiltä pyydetään tarkastusta varten kirjallisesti suostumukset henkilötietojen käsittelyyn (tietosuoja-asetuksen mukainen suostumusta ilmaiseva lausuma).

Suostumus tulee asetuksen mukaan antaa vapaaehtoisesti. Jos suostumuksen antajan katsotaan olevan heikommassa asemassa kuin suostumuksen pyytäjän, ei suostumusta ole välttämättä annettu aidosti vapaaehtoisesti.[69] Koska työntekijän ja työnantajan välillä on usein suhde, jossa työntekijä on alemmassa asemassa ja mahdollisesti riippuvainen työnantajasta, ei työntekijän haastattelua todennäköisesti voitaisi katsoa asetuksen mukaiseksi suostumukseksi. Työntekijöiden henkilötietojen käsittelyperusteen tulisikin lähtökohtaisesti olla jokin muu kuin suostumus.[70] Tämä tarkoittaa siis, että suostumus toiminee due diligence -tarkastuksessa käsittelyperusteena ainoastaan johdon henkilötietoja käsiteltäessä. Mikäli työntekijöiden henkilötietoja halutaan käsitellä, käsittelyperusteen tulisi nähdäkseni olla jokin muu kuin suostumus. Toisaalta suostumuksen pyytäminen työntekijöiltä tulisi due diligence -tarkastuksessa vastaan ani harvoin muutenkin, sillä kuten aiemmin on todettu, tarkastusvaiheessa yrityskauppa ei useimmiten ole julkista tietoa ja siten vain johdon ja mahdollisesti omistajien tiedossa.

3.2.2 Suostumuksen edellytykset

Kuten edellisessä luvussa todettiin, suostumuksen pätevyydelle on asetettu tietosuoja-asetuksen 7 artiklassa omat edellytyksensä. Edellytyksiä on neljä ja niistä kaikkien on toteuduttava, jotta suostumus voidaan katsoa lainmukaiseksi perusteeksi henkilötietojen käsittelylle. Kuten aiemmin on todettu, tietosuoja-asetuksen säännökset näyttävät useissa tapauksissa kirjoitetun uutta teknologiaa ja digitalisaatiota silmällä pitäen ja asetuksen tarkoitus on vastata niiden kehityksen aiheuttamiin uusiin haasteisiin. Tämä voidaan havaita myös suostumuksen edellytyksiä tarkasteltaessa ja edellytysten täyttymistä pohdittaessa huomataan, ettei edellytysten täyttymättä jääminen vaikuta due diligence -tarkastuksessa kovinkaan todennäköiseltä.

[68] Tietosuoja-asetuksen johdanto-osan (32) mukaan suostumusta ei pitäisi voida antaa vaikenemalla, valmiiksi rastitetuilla ruuduilla tai jättämällä jokin toimi toteuttamatta. Vaikka voitaisiin olettaa, että lähettäjällä on lupa myös muiden henkilöiden tietojen antamiseen, ei henkilötietojen käsittelijä voine riittävästi varmistua asiasta. Suostumuksen käsitteeseen liittyy vahvasti rekisteröidyn aktiivinen toiminta.
[69] Tietosuojavaltuutetun toimisto: Rekisteröidyn suostumus.
[70] WP 259, s. 7.

Artiklan 1 kohdan mukaan *rekisterinpitäjän* on osoitettava, että suostumus on annettu. Tätä kutsutaan rekisterinpitäjän *osoitusvelvollisuudeksi.* Rekisterinpitäjän on siis syytä dokumentoida kaikki suostumukseen liittyvät seikat, kuten suostumuksen antaja ja se, milloin suostumus on annettu sekä ne tiedot, jotka suostumuksen antaneelle henkilölle on suostumusta pyydettäessä henkilötietojen käsittelystä annettu.[71] Luonnollisesti myös se, että suostumus on asetuksen 4 artiklan 11 kohdan määritelmän mukainen, on pystyttävä osoittamaan. Jos kysymyksessä on due diligence -tarkastuksen mukainen haastattelu, osoitusvelvollisuus voisi vaatia esimerkiksi haastattelun nauhoittamista, pöytäkirjan pitämistä tai kirjallisen suostumuksen pyytämistä.

Toinen suostumuksen edellytys on, että kirjallisesti annettavan suostumuksen kohdalla pyyntö suostumuksesta on esitetty selvästi erillään muista ilmoituksessa mahdollisesti olevista asioista. Edellytyksenä on lisäksi, että pyyntö on selkeä ja yksinkertaisesti esitetty. (Tietosuoja-asetuksen 7 artiklan 2 kohta.) Kyseessä oleva edellytys näyttäisi olevan yksi niistä, jotka on kirjoitettu teknologian kehityksen vuoksi. Usein verkkopalveluiden käyttäjä joutuu hyväksymään erilaisia ehtoja, jotka ovat ennen asetuksen voimaantuloa saattaneet sisältää henkilötietojen käsittelyyn liittyviä lupia ilman, että pitkien ehtojen hyväksyjä on edes tiennyt asiasta. Edellytyksen noudattaminen due diligence -tarkastusta varten pyydettävän suostumuksen osalta ei todennäköisesti aiheuttaisi ongelmia, sillä todennäköisesti suostumuksen ohella henkilön ei tarvitse hyväksyä muita ehtoja, eikä ilmoituksessa siten olisi muita tietoja.

Rekisteröidyllä on lisäksi oikeus perua antamansa suostumus. Perumisen tulee olla yhtä helppoa kuin suostumuksen antamisen, mutta peruminen ei vaikuta ennen sitä tehdyn käsittelyn lainmukaisuuteen. (Tietosuoja-asetuksen 7 artiklan 3 kohta.) Due diligence -tarkastuksessa suostumuksen peruminen ei todennäköisesti realisoituisi kovinkaan usein. Lisäksi, jos suostumus liittyy haastatteluun, tehdään arvioita yleensä ottaen jo haastattelua tehtäessä, eikä jälkikäteen tehty suostumuksen peruutus siten vaikuta lopputulokseen. Jos taas suostumus olisi kerätty rekisteröidyiltä suostumusta ilmaisevalla lausumalla, myöhempi peruminen johtaisi siihen, ettei tietoja voitaisi hyödyntää tarkastuksessa. Tilanne voi realisoitua lähinnä, jos suostumuksen antaneen rekisteröidyn tiedot olisi luovutettu tarkastuksen tekijälle, mutta tarkastusta ei vielä olisi ehditty tehdä kyseisten tietojen osalta.

Artiklan neljäs edellytys liittyy suostumuksen vapaaehtoisuuteen. Edellytyksen mukaan vapaaehtoisuutta arvioitaessa olisi otettava huomioon se, onko rekisteröidyltä pyydetty suostumusta

[71] *Hanninen – Laine – Rantala – Rusi – Varhela* 2017, s. 38.

sellaisten henkilötietojen käsittelyyn, jotka eivät ole sopimuksen täytäntöön panemiseksi tarpeen, mutta joiden käsittelyyn suostuminen olisi ehtona sopimukselle. Näyttövelvollisuus käsiteltävien tietojen tarpeellisuudesta on rekisterinpitäjällä.[72] Due diligence -tarkastuksen osalta edellytyksen täyttymistä voitaneen pitää lähtökohtana. Tarkastusta varten kerättävät henkilötiedot ovat tarkastuksissa usein samanlaisia, eikä tarkastuksen tekijällä yleensä ole muuta motiivia tietojen keräämiselle kuin onnistuneen yrityskaupan varmistaminen. Säännöksen sanamuoto viittaa lisäksi tilanteisiin, joissa on kysymys rekisteröidyn kanssa solmittavasta sopimuksesta. Edellytyksen soveltamista koskevat esimerkit liittyvätkin usein verkkopalveluiden ja -sovellusten pyytämiin tietoihin sekä esimerkiksi markkinointilupien pyytämiseen.

3.3 Oikeutettu etu yrityskaupassa

3.3.1 Oikeutetun edun käsite

Edellisessä luvussa käsitellyn suostumuksen lisäksi tietosuoja-asetuksen 6 artiklasta löytyy myös toinen mahdollinen käsittelyperuste due diligence -tarkastukselle. Artiklan 1 kohdan f alakohdan mukaan käsittely voi olla lain mukaista silloin, jos se on tarpeen rekisterinpitäjän tai kolmannen osapuolen oikeutettujen etujen toteuttamiseksi. Oikeutetun edun määritelmä on osoittautunut jokseenkin laaja-alaiseksi niin oikeuskäytännön, asetuksen johdannon kuin oikeuskirjallisuudenkin valossa. Säännös on joustava ja siksi sitä on pidetty myös eräänlaisena ”porsaanreikänä”, jonka avulla käsittely on mahdollista useissa erilaisissa tilanteissa.[73]

Joustavuudestaan huolimatta oikeutetun edun soveltuminen edellyttää tapauskohtaista, kolmivaiheista arviointia. Ensiksi on selvitettävä, onko oikeutettua etua olemassa. Sen jälkeen on arvioitava, onko käsittely *tarpeellista* oikeutetun edun toteuttamiseksi. Kolmannessa vaiheessa oikeutettua etua punnitaan niiden rekisteröidyn etujen kanssa, jotka edellyttävät henkilötietojen suojaa.[74] Kolmatta vaihetta eli ns. tasapainotestiä käsitellään alaluvussa 3.3.3.

Oikeutettu etu voi säännöksen mukaan olla rekisterinpitäjällä tai kolmannella osapuolella. Due diligence -tarkastuksessa tämä helpottaa käsittelyperusteen soveltamista siltä osin, että vaikka

[72] WP 259, s. 9.
[73] *Kamara – de Hert* 2018, s. 4.
Ks. toisaalta myös WP 217, s. 41. Säännöstä ei tulisi käyttää porsaanreikänä vaan sen käyttö vaatii yksityiskohtaista arviointia.
[74] *Gil Gonzalez – de Hert* 2019, s. 604.

ostajaa ei välttämättä voida pitää rekisterinpitäjänä vielä due diligence -vaiheessa, voidaan ostajan mahdollisesti olemassa olevaa oikeutettua etua pitää käsittelyperusteena. Kun due diligence -tarkastuksen perimmäinen tarkoitus on varmistaa hankittavan yrityksen sopivuus ostokohteeksi, on todennäköistä, että juuri ostajalla on tarkastuksessa sellainen oikeutettu etu, jota voidaan pitää käsittelyperusteena. Oikeutetun edun on oltava konkreettinen henkilötietojen käsittelyhetkellä tai lähitulevaisuudessa.[75] Lisäksi edun on termin mukaisesti oltava *oikeutettu,* mikä tarkoittaa, ettei etu saa olla tietosuojalain tai muun lain vastainen.[76] Rekisterinpitäjän on lisäksi pystyttävä osoittamaan, että toiminta on oikeutetun edun perusteella lainmukaista (*osoitusvelvollisuus).*[77]

Vaikka oikeutetulle edulle on tietosuoja-asetuksessa ja tietosuojatyöryhmän kannanotossa asetettu tiettyjä kriteereitä ja reunaehtoja, oikeusperustetta on arvosteltu siitä, ettei oikeutetun edun määrittelemiseksi ole annettu tarpeeksi suuntaviivoja ja ohjeistusta.[78] Tietosuoja-asetuksen johdanto-osassa oikeutetusta edusta on kuitenkin annettu joitakin esimerkkejä. Henkilötietojen käsitteleminen suoramarkkinointitarkoituksissa tai siirtäminen konsernin sisällä hallinnollisista syistä voidaan katsoa oikeutetun edun toteuttamiseksi suoritettaviksi. Samoin oikeutettu etu voi johdannon mukaan olla olemassa silloin, kun rekisterinpitäjä käsittelee asiakkaan tai palveluksessaan olevan tietoja.[79]

Johdannon esimerkit eivät kuitenkaan näyttäisi soveltuvan due diligence -tarkastukseen. Kaksi ensimmäistä esimerkkiä voidaan sulkea pois suoraan ja toisaalta se, onko tarkastuksessa kysymys *rekisterinpitäjän* palveluksessa olevien tiedoista, selviää tutkielman tutkimuskysymykseen vastattaessa. Jos kohdeyhtiö katsottaisiin tarkastuksen rekisterinpitäjäksi, kyse olisi ainakin osittain rekisterinpitäjän palveluksessa olevien tiedoista.

Due diligence -tarkastuksen tavoitteena on selvittää, mitä ostettava kohdeyhtiö ”on syönyt”. Tarkastuksen tulos vaikuttaa siten kaupan ehtoihin ja muun muassa kauppahintaan, minkä vuoksi tarkastuksella voidaan katsoa olevan huomattava taloudellinen vaikutus ostajalle. Ta-

[75] WP 217, s. 24.
[76] WP 217, s. 25.
[77] Tietosuojavaltuutetun toimisto, rekisterinpitäjän oikeutettu etu.
[78] *Rauhofer* 2013, s. 11.
[79] Tietosuoja-asetuksen johdanto, kohdat 47 ja 48.

loudellista intressiä voitaisiin täten pitää sellaisena oikeutettuna etuna, jonka perusteella henkilötietojen käsittely tarkastuksessa voi olla sallittua.[80] Taloudellinen intressi on katsottu *mahdolliseksi* oikeutetuksi eduksi myös Euroopan unionin tuomioistuimen (CJEU) ratkaisukäytännössä. Esimerkiksi niin sanotussa *Google Spain* tapauksessa tuomioistuin totesi, että asiassa vastaajana olleella hakukoneella oli asiassa taloudellinen intressi ja että hakukoneen suorittama käsittely *"saattaa kuulua […] 7 artiklan f alakohdassa tarkoitetun perusteen soveltamisalaan"*. Tuomioistuin kuitenkin katsoi, että rekisteröidyn perusoikeuksiin (yksityiselämän kunnioittaminen ja henkilötietojen suoja) puuttumisen potentiaalisen vakavuuden vuoksi käsittelyä ei voitu perustella taloudellisella intressillä.[81]

Mikäli henkilötietojen käsittelyperusteena on tarkoitus käyttää oikeutettua etua, tulee etu edellä kuvatuin tavoin määritellä siten, että se on konkreettinen ja kiinteässä yhteydessä henkilötietojen käsittelyyn. Toisaalta jotkin koulukunnat ovat katsoneet, että oikeudellista etua voitaisiin pitää käsittelyperusteena silloin, kun kyseessä on tavanomainen ja harmiton liiketoimintaan liittyvä käsittely.[82] Tulipa taloudellinen intressi oikeutettuna etuna määritellä tarkoin tai ei, voitaneen sitä due diligence -tarkastuksessa kiistatta pitää sellaisena oikeutettuna etuna, jonka nojalla henkilötietojen käsittely osana tarkastusta voi olla mahdollista, jos se täyttää tarpeellisuusvaatimuksen ja tasapainotestin.

3.3.2 Käsittelyn tarpeellisuus

Kuten edellä on todettu, toinen vaihe oikeutetun edun arvioinnissa on käsittelyn tarpeellisuuden arviointi. Tarpeellisuudella tarkoitetaan, että käsittelyn ja oikeutetun edun välillä on oltava yhteys. Tarpeellisuusvaatimus liittyy myös neljään muuhun 6 artiklan käsittelyperusteeseen (alakohdat (b)-(e) oikeutetun edun lisäksi). Sen merkitys korostuu kuitenkin oikeutettua etua arvioitaessa, sillä sen avulla voidaan ehkäistä lainkohdan liian laajaa tulkintaa ja arvioida sitä, voisiko oikeutettu etu toteutua ilman henkilötietojen käsittelyä.[83]

Arvioitaessa tarpeellisuusvaatimuksen täyttymistä due diligence -tarkastuksessa on siis pohdittava, onko henkilötietojen käsittelyllä ja ostajan taloudellisella intressillä yhteyttä toisiinsa.

[80] Handbook on European data protection law, s. 78–80.
[81] Asia C-131/12, kohdat 73 ja 80–81.
[82] *Van der Sloot – Zuiderveen Borgesius,* s. 20.
[83] WP 217, s. 29.

Oman näkemykseni mukaan due diligence -tarkastusta voidaan pitää niin vakiintuneena ja tärkeänä osana yrityskauppaa, että tarkastuksen ja ostajan taloudellisen intressin välinen yhteys on kiistaton. Toisaalta tarkastus pitää sisällään myös osa-alueita, jotka eivät sisällä henkilötietoja ollenkaan (esim. yhtiön taloudellista tilaa koskevat tiedot). Sen vuoksi on relevanttia kysyä, voisiko ostajan taloudellinen intressi toteutua ilman, että tarkastuksessa käsiteltäisiin henkilötietoja?

Näkemykseni mukaan tämä riippuu pitkälti suunnitellun yrityskaupan laadusta ja muodosta. Osa taloudellisen edun takaamiseksi tarvittavista tiedoista (jotka normaalisti sisältävät henkilötietoja) on todennäköisesti mahdollista käsitellä myös anonymisoituna, jolloin tietosuoja-asetus ei soveltuisi kyseisten tietojen käsittelyyn. Toisaalta, mikäli suunnitellun yrityskaupan tarkoituksena on esimerkiksi hankkia kohdeyhtiön avainhenkilöillä oleva tietotaito, on henkilötietojen käsittelyllä suora liityntä ostajan taloudelliseen intressiin. Kyseisenlaisissa yrityskaupoissa avainhenkilöitä on kuitenkin mitä todennäköisimmin myös haastateltu due diligence -tarkastusta tehtäessä, jolloin heihin todennäköisesti sovellettaisiin suostumusperustetta, eikä oikeutettuun etuun liittyvää tarpeellisuusarviointia tarvittaisi.

Kaikissa yrityskaupoissa henkilötietojen käsittelyn yhteys taloudelliseen intressiin ei liene yhtä suora ainakaan kaikkien käsiteltävien henkilötietojen osalta. Tällaisissa tilanteissa on huomioitava, että tietosuoja-asetuksen 5 artikla, jossa on määritelty käsittelyn periaatteet, asettaa tarpeellisuusarvioinnille uloimmat rajat.[84] Erityisesti 1(c) alakohdan mukainen tietojen minimointi olisi tällöin otettava huomioon. En pidä myöskään poissuljettuna, että tietojen käsittelemiseksi henkilötiedot olisi joissakin tapauksissa poistettava käsiteltävästä materiaalista tai, että henkilötiedot olisi anonymisoitava.[85] Todennäköisesti tarpeellisuusvaatimus kuitenkin täyttyisi useimmiten ainakin joidenkin käsiteltävien henkilötietojen osalta.

[84] *Kamara – de Hert* 2018, s. 14.

[85] Anonymisoinnin tulisi tällöin tapahtua jo ennen tietojen luovuttamista tarkastuksen tekijälle. Tällöin tarkastuksen tekijällä ei olisi mahdollisuutta yhdistää käsittelemäänsä aineistoa tiettyihin henkilöihin. Anonymisointi voi toisaalta soveltua due diligence -tarkastukseen huonosti etenkin avainhenkilöiden ja johdon kohdalla, sillä usein tarvittavat ja tarkastettavat tiedot ovat sellaisia, jotka käsittelijä pystyy yhdistämään henkilöihin. Tähän vaikuttaa myös se, että due diligence -tarkastuksen tekijällä voi olla jo valmiiksi joitakin taustatietoja tarkastettavista henkilöistä.

3.3.3 Tasapainotesti

Tietosuoja-asetuksen oikeutettua etua käsittelevän 6 artiklan 1(f) alakohdan mukaan rekisterinpitäjän tai kolmannen oikeutettu etu voi olla käsittelyperuste, paitsi milloin henkilötietojen suojaa edellyttävät rekisteröidyn edut tai perusoikeudet ja -vapaudet syrjäyttävät tällaiset edut. Käsittelyperusteen sovellettavuutta arvioitaessa on siis asetettava vastakkain jo aiemmassa vaiheessa määritetty, täsmällinen ja konkreettinen oikeutettu etu sekä ne rekisteröidyn edut, jotka edellyttävät henkilötietojen suojaa. Näiden etujen vertailussa on kyse niin kutsutusta *tasapainotestistä*, joka on soveltuvuusarvioinnin kolmas vaihe.

Tasapainotesti ei ole tietosuoja-asetuksen mukanaan tuoma menetelmä, sillä testiä on käytetty oikeutetun edun arvioimiseen jo henkilötietodirektiivin aikana ja sitä on sovellettu myös EU:n tuomioistuimen ennakkoratkaisuissa. Tasapainotesti koostuu neljästä pääkohdasta: oikeutetun edun arvioinnista, rekisteröidylle käsittelystä aiheutuvien vaikutusten arvioinnista, alustavasta arviosta etujen tasapainoon liittyen ja rekisterinpitäjän keinoista suojata rekisteröidyn oikeuksia käsittelyn mahdollisilta haittavaikutuksilta.[86] Tasapainotestin alussa on siis määriteltävä yhtäältä oikeutettu etu sekä toisaalta rekisteröidyn suojattava etu tai oikeus.

Oikeutetun edun tärkeys vaihtelee tapauskohtaisesti. Etu voi olla esimerkiksi perusoikeus, kuten EU:n perusoikeuskirjan (2000/C 364/01) mukainen omistusoikeus (16 artikla) tai elinkeinovapaus (17 artikla). Toisaalta etu voi olla myös kulttuuristen tai sosiaalisten odotusten ja normien mukainen etu tai muu perusteltavissa oleva etu. Mitä vahvempi yhteys edulla on kansalliseen tai EU:n lainsäädäntöön, sitä painavammaksi oikeutettu etu voidaan tasapainotestissä katsoa.[87] Kuten edellisessä luvussa on tuotu esiin, due diligence -tarkastuksessa oikeutettu etu on mitä todennäköisimmin ostajan taloudellinen intressi. Intressin liityntä perusoikeuksiin jäänee kuitenkin hataraksi, vaikka sen yhdistäminen yllä mainittuihin omistusoikeuteen tai elinkeinonvapauteen voisi – ainakin pienemmän yhtiön osalta – joissakin tapauksissa olla perusteltavissa.[88]

[86] WP 217, s. 33.
[87] WP 217, s. 36.
[88] *Hallberg – Karapuu – Ojanen – Scheinin – Tuori – Viljanen* 2011, luku II.2. Oikeushenkilöt. Myös oikeushenkilöiden voidaan katsoa nauttivan perusoikeuksien suojaa etenkin silloin, kun suoja yltää välillisesti oikeushenkilön kautta myös luonnolliseen henkilöön.

Tasapainotestin kannalta oleellista on lisäksi se, mitä vaikutuksia käsittelystä aiheutuu tai voi aiheutua rekisteröidylle ja mitkä rekisteröidyn oikeudet tarvitsevat käsittelyssä suojaa. On huomattava, että tasapainotestiä tehtäessä on erotettava koko yrityskaupan mahdolliset seuraukset ja itse henkilötietojen käsittelyn seuraukset rekisteröidylle. Yrityskaupan seurauksena esimerkiksi työntekijän toimenkuva voi muuttua, mutta tätä ei voitane pitää henkilötietojen käsittelyn seurauksena. Itse käsittelyn seuraukset rekisteröidylle näyttäisivätkin jäävän vähäisiksi ja sillä voi yleensä olla suora vaikutus lähinnä henkilötietojen suojaan.

Kilpailevien etujen määrittelyn jälkeen olisi tehtävä alustava arvio oikeuksien tasapainosta. Tasapainon määrittely on tapauskohtaista ja riippuu konkreettisista olosuhteista.[89] Esimerkiksi edellä luvussa 3.3.1 mainitussa *Google Spain* -tapauksessa tuomioistuin katsoi, ettei taloudellista intressiä voitu pitää oikeudellisena etuna, kun käsittelyssä puututtiin rekisteröidyn yksityiselämän ja henkilötietojen suojaan niin merkittävästi.[90] Samat vastakkaiset edut tulevat punnittavaksi myös due diligence -tarkastuksessa tapahtuvassa käsittelyssä, mutta konkreettisten olosuhteiden voidaan kuitenkin katsoa olevan toisenlaiset: due diligence -tarkastuksessa henkilötietoja käsittelee rajattu joukko ihmisiä eikä rekisteröidyn henkilötietoja saateta julkisiksi. Näin ollen käsittelyn vaikutukset rekisteröidyn oikeuksiin eivät näyttäisi olevan samalla tavoin merkittäviä. Mikäli rekisteröidyn suojattavat oikeudet rajoittuvat ainoastaan henkilötietojen suojaan, taloudellisen intressin voitaisiin alustavan arvion mukaan katsoa täyttävän oikeutetun edun määritelmän due diligence -tarkastuksessa.

Tietosuojatyöryhmän mukaan neljäntenä pääkohtana tasapainotestissä on rekisterinpitäjän keinot suojata rekisteröidyn oikeuksia käsittelyn mahdollisilta haittavaikutuksilta. Tällaisia keinoja voivat olla mm. anonymisointi, läpinäkyvyyden lisääminen, kerättävien tietojen rajoittaminen ja niiden poistaminen heti käsittelyn jälkeen.[91] Tietosuoja-asetuksen myötä osa näistä velvollisuuksista on kuitenkin myös henkilötietojen käsittelijän vastuulla (ks. tarkemmin luku 5) ja näin ollen oikeuksien suojaamista koskevia keinoja on arvioitava kokonaisuutena siten, että huomioidaan myös henkilötietojen käsittelijän keinot.

[89] Asia C-13/16, kohta 31.
[90] Asia C-131/12, kohdat 86–87. Tuomioistuin korosti ratkaisussaan sitä, että hakukone helpottaa tuntuvasti rekisteröidystä hakuja tekevien mahdollisuuksia saada rekisteröityä koskevat tiedot ja sillä voi olla ratkaiseva vaikutus mainittujen tietojen levittämisessä.
[91] WP 217, s. 42.

Oikeuskirjallisuudessa on esitetty myös kritiikkiä sille, että rekisterinpitäjän keinot suojata rekisteröidyn oikeuksia on otettu osaksi tasapainotestiä. Tasapainotesti voi kallistua rekisterinpitäjän puolelle, jos rekisterinpitäjä on huolehtinut suojauskeinoista ja vastakkaisten oikeuksien ja intressien punninta voi tällöin jäädä vähemmälle. Lisäksi rekisterinpitäjän velvollisuuksiin kuuluu tietosuojasta huolehtiminen, olipa käsittelyperusteena oikeutettu etu tai jokin muu oikeusperuste.[92] Ongelmallisena voidaan mielestäni pitää myös sitä, että oikeusperusteena voi toimia *kolmannen* oikeutettu etu, mutta tasapainotestin osana on silti *rekisterinpitäjän* keinot huolehtia oikeuksien suojaamisesta.

On selvää, että tasapainotestin tekemiseen liittyy tietynlaista epävarmuutta sen suhteen, milloin rekisterinpitäjän tai kolmannen oikeutetun edun voidaan katsoa olevan vahvempi kuin rekisteröidyn yksityisyydensuojan tai muiden oikeuksien ja milloin oikeutetun edun voidaan siten katsoa toimivan käsittelyperusteena. Due diligence -tarkastuksessa voitaneen kuitenkin lähtökohtaisesti katsoa, että ostajan taloudellinen intressi oikeuttaisi henkilötietojen käsittelyn myös neljännen arviointikriteerin perusteella. Ensinnäkin käsiteltävät henkilötiedot ja tietoja käsittelevät tahot ovat rajattuja. Toiseksi, kun tarkastuksen tekee asianajotoimisto tai muu ammattimaisesti toimiva taho, on todennäköistä, että henkilötietojen suojauskeinoista on myös huolehdittu asianmukaisesti.

3.4 Käsittelyn tarkoituksena onnistunut yrityskauppa

Tietosuoja-asetuksen 6 artiklan 4 kohdassa on säädetty niistä seikoista, jotka käsittelyssä on otettava huomioon, mikäli käsittely tapahtuu muuta kuin sitä tarkoitusta varten, jonka vuoksi tiedot on kerätty. Yrityskaupassa on yleensä kyse tällaisesta tilanteesta, sillä tiedot on alun perin kerätty kohdeyhtiön määrittelemiä tarkoituksia, kuten liiketoimintaa ja työnantajan velvoitteiden täyttämistä, varten. Tietosuoja-asetuksen säännös on uusi, sillä henkilötietodirektiivissä säädettiin ainoastaan henkilötietojen myöhemmästä käsittelystä historiantutkimusta, tilastollisia tai tieteellisiä tarkoituksia varten. Tietosuojatyöryhmä WP29 on kuitenkin jo ennen tietosuoja-asetuksen säätämistä antanut ohjeistuksen[93] tietojen käytöstä eri tarkoitukseen kuin mihin ne on kerätty. Ohjeistuksen mukaan huomioitavat seikat ovat pitkälti samankaltaisia kuin asetuksessa.

[92] *Kamara – de Hert* 2018, s. 17.
[93] WP 203.

Tietosuoja-asetuksen mukaan säännöstä ei sovelleta silloin, kun käsittely perustuu rekisteröidyn suostumukseen. Näin ollen voidaan siis todeta, että due diligence -tarkastuksessa lainkohta ei todennäköisesti soveltuisi johdon tai muiden avainhenkilöiden henkilötietojen käsittelyyn. Arviointi tulisi siis tehdä vain niiden henkilötietoryhmien osalta, joiden käsittelyn oikeusperuste on oikeutettu etu (eli lähinnä työntekijöiden ja osakkeenomistajien tietojen osalta.)

Rekisterinpitäjän olisi 6 artiklan 4 kohdan mukaan otettava huomioon sekä henkilötietojen keruun ja aiotun myöhemmän käsittelyn tarkoituksen väliset yhteydet että keruun asiayhteys erityisesti rekisteröityjen ja rekisterinpitäjän välisen suhteen osalta (a- ja b-alakohdat). Lainkohtia arvioitaessa asiaa on lähestyttävä myös rekisteröidyn kannalta, sillä arvioinnin osana on kysyttävä, voiko rekisteröity kohtuudella odottaa, että hänen henkilötietojaan käsitellään kyseisellä tavalla.[94] Due diligence -tarkastuksessa tuleekin puntaroitavaksi se, voidaanko olettaa, että rekisteröidyn asemassa oleva työntekijä on voinut kohtuudella olettaa tietojaan käsiteltävän yrityskaupan yhteydessä tehtävässä tarkastuksessa.[95] Vaikka henkilötietojen myöhempi käsitteleminen yrityskaupan ja due diligence -tarkastuksen yhteydessä ei todennäköisesti ole sellaista käsittelyä, jota kohdeyhtiön työntekijä keruuvaiheessa odottaisi, on käsittely yrityskaupan konkretisoituessa selvästi yhteydessä kohdeyhtiön liiketoimintaan ja sen järjestelyyn. Näin ollen voitaisiin katsoa, ettei työntekijä ainakaan kohtuudella voi olettaa, etteikö henkilötietoja voitaisi käsitellä tällaisessa tarkoituksessa.

Käsiteltäessä henkilötietoja muuta tarkoitusta varten kuin mihin tiedot on kerätty, on lisäksi huomioitava henkilötietojen luonne ja aiotun käsittelyn mahdolliset seuraukset rekisteröidylle (c- ja d-alakohdat). Erityisesti olisi huomioitava käsiteltävien tietojen mahdollinen 9 artiklan mukainen arkaluontoisuus ja 10 artiklan mukaiset rikostuomioihin ja rikkomuksiin liittyvät henkilötiedot. Kuten aiemmin luvussa 3.1 on tuotu esiin, due diligence -tarkastuksessa arkaluontoisten tietojen käsittelyn edellytykset eivät lähtökohtaisesti täyty. Myöskään rikostuomioita ja rikkomuksia koskevia tietoja ei tarkastuksessa voitaisi ainakaan työntekijän osalta käsitellä.[96] Käsittelyn mahdollisia seurauksia rekisteröidylle on käsitelty tasapainotestin yhteydessä edellisessä alaluvussa 3.3.3.

[94] Ks. esim. *Grafenstein* 2018, s. 178–191. Euroopan ihmisoikeustuomioistuin on useassa ratkaisussaan käsitellyt kohtuullisia odotuksia henkilötietojen käsittelyssä.
[95] WP 203, s. 24.
[96] Asetuksen 10 artiklan mukaan kyseisiä tietoja voidaan käsitellä vain rekisteröidyn suostumuksen perusteella tai silloin, kun se sallitaan unionin oikeudessa tai jäsenvaltion lainsäädännössä.

Viimeisenä seikkana huomioon on otettava asianmukaisten suojatoimien olemassaolo (e-ala-kohta). Tällaisia suojatoimia ovat esimerkiksi salaaminen ja pseudonymisointi[97]. Kuten edellä on todettu, on mahdollista, että osa käsiteltävistä henkilötiedoista tulisi anonymisoida ennen tietojen luovuttamista tarkastuksen tekijälle. Näin ollen myös pseudonymisointi ja salaaminen voisivat tulla kysymykseen työntekijöiden tietojen osalta.

[97] Pseudonymisointi tarkoittaa henkilötietojen käsittelyä siten, ettei tietoja voida enää yhdistää tiettyyn rekisteröityyn käyttämättä lisätietoja edellyttäen, että tällaiset lisätiedot säilytetään erillään ja niihin sovelletaan teknisiä ja organisatiorisia toimenpiteitä, joilla varmistetaan, ettei henkilötietojen yhdistämistä tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön tapahdu. (Tietosuoja-asetuksen 4 artiklan 5 kohta).

4 REKISTERINPITÄJÄ JA HENKILÖTIETOJEN KÄSITTELIJÄ

4.1 Rekisterinpitäjän määritelmä

4.1.1 Määritelmän keskeinen sisältö ja kehittyminen

Tietosuoja-asetuksen 4 artiklan 7 kohdan mukaan rekisterinpitäjällä tarkoitetaan luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot.[98] Määritelmä on pysynyt asetuksessa sanamuodoltaan muuttumattomana henkilötietodirektiiviin nähden. Käsite on siis pysynyt samana yli 20 vuotta, mikä osaltaan helpottaa sen tulkitsemista ja arvioimista, kun käsitettä tukevaa lähdemateriaalia on saatavilla pitkältä ajalta.

Suomessa rekisterinpitäjän määritelmä oli ennen asetuksen voimaantuloa erilainen. HTL:n 3 §:n 4 kohdan mukaan rekisterinpitäjällä tarkoitettiin yhtä tai useampaa henkilöä, yhteisöä, laitosta tai säätiötä, jonka käyttöä varten henkilörekisteri perustetaan ja jolla on oikeus määrätä rekisterin käytöstä tai jonka tehtäväksi rekisterinpito on lailla säädetty. Tietosuoja-asetus muutti siten rekisterinpitäjän määritelmän suomalaisessa lainsäädännössä. HTL:n mukaista määritelmää ei kuitenkaan käsitellä tässä tutkielmassa enempää, sillä tarkoituksena on tarkastella tämänhetkisen lainsäädännön mukaista määritelmää.

EU:n oikeudessa rekisterinpitäjä on käsitteenä esiintynyt jo vuonna 1981 allekirjoitetussa tietosuojasopimuksessa. Sopimus täydentää Euroopan ihmisoikeussopimusta ja sen tarkoituksena on nimensä mukaisesti henkilötietojen turvaaminen *automaattisessa* tietojenkäsittelyssä. Sopimuksen mukaan rekisterinpitäjä on sellainen luonnollinen henkilö, oikeushenkilö, julkinen viranomainen tai virasto tai muu yhteisö, joka on kansallisen lainsäädännön mukaan toimivaltainen päättämään automaattisesti käsiteltävän rekisterin tarkoituksesta sekä siitä, minkä tyyppisiä henkilötietoja talletetaan ja mitä toimintoja näihin kohdistetaan.[99]

Tietosuojasopimuksen määritelmä eroaa siis huomattavasti direktiivin ja sittemmin asetuksen mukaisesta määritelmästä. Ensinnäkin sopimus koskee ainoastaan automaattista henkilötietojen

[98] Saman säännöksen – ja aiemmin voimassa olleen henkilötietodirektiivin – mukaan, mikäli henkilötietojen käsittelyn tarkoitukset ja keinot määritellään unionin tai jäsenvaltioiden lainsäädännössä, myös rekisterinpitäjä tai kriteerit rekisterinpitäjän nimittämiselle voidaan vahvistaa unionin oikeuden tai jäsenvaltion lainsäädännön mukaisesti.
[99] Tietosuojasopimuksen 2 artiklan d kohta.

käsittelyä, kun taas asetus ja direktiivi on säädetty teknologianeutraaleiksi. Toiseksi, sopimuksen määritelmässä on kyse siitä, onko käsittelijällä *toimivalta* päättää rekisteriin liittyvistä asioista. Huomionarvoista on se, ettei rekisterinpitäjän sanamuodon mukaan välttämättä tarvitse päättää asioista, vaan riittää, että se voisi toimivaltansa perusteella päättää niistä. Kolmanneksi on syytä kiinnittää huomiota siihen, että artiklassa puhutaan *rekisteristä*, mistä myös suomenkielinen termi rekisterinpitäjä (englanniksi sopimuksessa *controller of the file*) juontanee juurensa.[100] Tietosuoja-asetuksessa tai henkilötietodirektiivissä ei kuitenkaan edellytetä, että käsiteltävät henkilötiedot olisivat jossakin tietyssä rekisterissä[101], minkä vuoksi englanninkielinen termi on asetuksessa ja direktiivissä saanut lyhyemmän muodon *controller*.

Tietosuoja-asetuksen ja henkilötietodirektiivin mukainen rekisterinpitäjän määritelmä pitää tietosuojasopimuksen tavoin sisällään kolme eri ”rakennuspalikkaa”, joiden kautta rekisterinpitäjän roolia arvioidaan. Termin jakaminen kolmeen osaan on peräisin henkilötietodirektiivin aikaisesta, 29 artiklan mukaisen tietosuojatyöryhmän kannanotosta liittyen rekisterinpitäjän ja henkilötietojen käsittelijän käsitteisiin (*Opinion 1/2010 on the concepts of ”controller and ”processor”).* Kyseinen kannanotto toimiikin pohjana tämän tutkielman määritelmiä koskevassa osuudessa.

Ensimmäinen kolmesta rakennuspalikasta on rekisterinpitäjän henkilöitymistä koskeva aspekti (onko rekisterinpitäjä luonnollinen henkilö, oikeushenkilö, viranomainen, virasto tai muu elin). Toinen palikka liittyy useamman rekisterinpitäjän mahdollisuuteen (”yksin tai yhdessä toisten kanssa”) ja kolmas osio erottaa rekisterinpitäjän muista tietosuoja-asetuksen mukaisista rooleista: mitä tarkoitetaan henkilötietojen käsittelyn tarkoituksilla ja keinoilla, jotka rekisterinpitäjä määrittelee?[102]

Tutkielman kannalta tärkeimmät kysymykset liittyvät toiseen ja kolmanteen osaan. Jotta voidaan arvioida asianajotoimiston roolia, on vastattava kysymykseen siitä, osallistuuko asianajotoimisto keinojen ja tarkoitusten määrittelyyn. Toisen osion perusteella taas arvioidaan, voiko asianajotoimisto olla toinen (tai yksi useammista) yhteisrekisterinpitäjistä.

[100] Suomenkieliselle termille ”rekisterinpitäjä” on esitetty kritiikkiä, sillä sen ei katsota kuvaavan roolia oikein. Englanninkielistä termiä ”controller” on pidetty osuvampana. (Ks. esim. *Korpisaari – Pitkänen – Warma-Lehtinen* 2018, s. 66–67.)
[101] Tietosuoja-asetuksen 2 artiklan mukaan asetusta sovelletaan henkilötietoihin, jotka muodostavat rekisterin osan tai joiden on tarkoitus muodostaa rekisterin osa, jos henkilötietoja käsitellään muussa kuin automaattisessa muodossa. Automaattisesti käsiteltyjen henkilötietojen ei siis tarvitse liittyä rekisteriin.
[102] WP 169, mm. s. 1 ja 7.

Kolmatta osiota käsitellään seuraavassa alaluvussa (4.1.2. Käsittelyn tarkoitukset ja keinot) ja toista osiota luvussa 4.2. Yhteisrekisterinpitäjät. Rekisterinpitäjän henkilöitymistä ja siihen liittyvää vastuunjakoa (eli ensimmäistä osaa) sivutaan joiltakin osin pääluvussa 5, jossa käsitellään vastuunjakoa yleisemmin.

4.1.2 Käsittelyn tarkoitukset ja keinot

Rekisterinpitäjä on siis se taho, joka määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot, ja on siksi myös ensisijaisesti vastuussa tietosuoja-asetuksen noudattamisesta.[103] Rekisterinpitäjää ei kuitenkaan pidä sekoittaa henkilötietojen ”omistajaan”[104], sillä rekisterinpitäjänä voidaan pitää myös sellaista tahoa, joka saa henkilötiedot niiden niin kutsutulta omistajalta. Henkilötietojen omistajan ja rekisterinpitäjän välille tehtävä ero vaikeuttaakin osaltaan myös rekisterinpitäjän erottamista henkilötietojen käsittelijästä. Sen vuoksi on tärkeää ymmärtää, mitä asetuksessa tarkoitetaan niillä tarkoituksilla ja keinoilla, joiden määritteleminen kuuluu rekisterinpitäjälle. Kuten tietosuojatyöryhmä WP29 kannanotossaan ilmaissut, tarkoitukset ja keinot on se osa-alue rekisterinpitäjän määritelmästä, jonka avulla rekisterinpitäjä erotetaan muista rooleista, mutta toisaalta kyseisen osion arviointi voi myös johtaa moninaisiin tulkintoihin.[105]

Ennen itse keinojen ja tarkoitusten määrittelemistä WP29 on esittänyt kolme tilannetta, joiden perusteella toimija voi osallistua keinojen ja tarkoitusten määrittelyyn. Ensimmäinen on suoraan asetuksen (ja direktiivin) määritelmästä tuleva tilanne, eli se, että keinojen ja tarkoitusten määrittely perustuu kansalliseen tai EU-tasoiseen lainsäädäntöön. Useimmiten kyse on tilanteesta, jossa lain vaatimus ei suoranaisesti velvoita käsittelijää määrittelemään tarkoituksia ja keinoja, mutta lain vaatimuksen täyttämiseksi henkilötietojen käsittely on tarpeen. Toinen tilanne on ns. implisiittisen toimivallan tilanne, mikä tarkoittaa, että osallistuminen keinojen ja tarkoitusten määrittelyyn syntyy epäsuorasti lainsäädännöstä. Se siis liittyy luonnollisesti toimijan rooliin, kuten esimerkiksi työnantajan käsitellessä työntekijän henkilötietoja. Kolmantena tilanteena ovat tosiasialliset olosuhteet, joiden perusteella toimijan voidaan katsoa osallistuvan tarkoitusten ja keinojen määrittelyyn.[106]

[103] *Houser – Voss* 2018, s. 72.
[104] *Hintze* 2018, s. 18.
[105] WP 169, s. 8 ja 12.
[106] WP 169, s. 10–11.

Asianajotoimiston suorittaessa due diligence -tarkastusta rekisterinpitäjäksi määritteleminen voisi tapahtua nähdäkseni lähinnä toisen tai kolmannen perusteen nojalla. Tarkoitusten ja keinojen määrittelyyn osallistumisen on hankala nähdä perustuvan suoraan lainmukaisen velvoitteen täyttämiseen, joskin esimerkiksi asianajajalain (496/1958) 5 §:n 1 momentissa todetaan, että asianajajan tulee rehellisesti ja *tunnollisesti* täyttää hänelle uskotut tehtävät. Voitaisiin toki arvioida, vaatiiko tehtävien täyttäminen tunnollisesti henkilötietojen käsittelyä tarkastuksessa, mutta näin pitkälle menevää johtopäätöstä ei liene tarpeellista tehdä. Toisaalta lainkohdan voitaisiin katsoa sopivan myös toiseen perusteeseen ja siten peruste keinojen ja tarkoitusten määrittelylle voisi muodostua implisiittisesti.

Kolmannen tilanteen ajatuksena on, että toimija tosiasiassa osallistuu tarkoitusten ja keinojen määrittelyyn. Mikäli asianajotoimiston katsottaisiin olevan rekisterinpitäjä, kolmas tilanne vaikuttaisi sopivan perusteeksi parhaiten. Rekisterinpitäjän roolin arvioinnissa ei kuitenkaan liene syytä antaa liian suurta painoarvoa tilanteille, joiden kautta rooli voi syntyä, sillä nähdäkseni tilanteet ovat helposti sovellettavissa kaikkiin henkilötietojen käsittelyyn osallistuviin tahoihin. Tilanteet toimivatkin lähinnä erilaisena taustatekijänä, joiden avulla voidaan hahmottaa muiden kriteereiden täyttymistä.

Itse keinoja ja tarkoituksia määritellessään tietosuojatyöryhmä on lähtenyt liikkeelle sanojen yleisistä määritelmistä. Keinolla tarkoitetaan sanakirjassa sitä ”miten päästään johonkin tulokseen tai saavutetaan lopputulos” ja tarkoitus puolestaan on ”ennalta suunniteltu lopputulos tai suunniteltua toimintaa ohjaava tekijä”. Tarkoituksen osalta tulee lisäksi huomioida sanan esiintyminen tietosuoja-asetuksen 5 artiklassa (kannanoton aikaan henkilötietodirektiivin 6 artikla), joka edellyttää, että henkilötiedot on kerättävä tiettyä, nimenomaista ja laillista tarkoitusta varten. Tarkoituksilla ja keinoilla tarkoitetaankin rekisterinpitäjän määritelmässä tietosuojatyöryhmän mukaan yksinkertaistetusti sitä, *miksi* (tarkoitus) *ja miten* (keino) *henkilötietoja käsitellään.*[107]

Asianajotoimiston tekemässä due diligence -tarkastuksessa henkilötietoja käsitellään osana kohdeyhtiön kokonaisarviointia. Henkilötietoja käsitellään siis siksi, että halutaan saada mahdollisimman tarkka kokonaiskuva siitä, mitä asianajotoimiston asiakas on ostamassa. Sitä, miksi juuri tiettyjä henkilöryhmiä koskevia henkilötietoja käsitellään, on käsitelty luvussa 2.3.

[107] WP 169, s. 13.

Rekisterinpitäjän määrittämisen kannalta kysymykseen ”miksi” riittänee kuitenkin vastaukseksi se, että tietoja käsitellään asianajotoimiston asiakkaan taloudellisten intressien turvaamiseksi.[108] Osin samaa kysymystä on pohdittu myös käsittelyn oikeusperustaa arvioitaessa.

Asianajotoimiston roolia arvioitaessa on kuitenkin itse tarkoituksen lisäksi kiinnitettävä huomiota siihen, kuka (tai ketkä) käsittelyn tarkoituksen – eli ennalta suunnitellun lopputuloksen tai suunniteltua toimintaa ohjaavan tekijän – määrittelee. Mikäli käsittelyn tarkoituksena pidetään asiakkaan taloudellisten intressien toteuttamista ja onnistunutta yrityskauppaa, voitaisiin ajatella, että tarkoitus on määritelty jo siinä vaiheessa, kun asianajotoimistolle on annettu yrityskauppaa koskeva toimeksianto. Yrityksen ostajahan ulkoistaa kauppaan liittyviä toimenpiteitä asiantuntijaorganisaatiolle varmistaakseen, että kauppa sujuu asianmukaisesti.

Toisaalta taas se, kuinka paljon ostajalla on tietämystä esimerkiksi due diligence -tarkastuksesta, lienee vaihtelevaa. Ei ole itsestään selvää, että ostajayrityksellä olisi etukäteen tietoa tarkastuksen sisällöstä tai siitä, että tarkastuksessa käsitellään henkilötietoja (tai ainakaan siitä, kuinka paljon ja millaisia tietoja käsitellään). Siksi voidaankin esittää kysymys: voiko ostaja olla henkilötietojen käsittelyn tarkoitusten määrittelijä, jos sillä ei ole tarkkaa tietoa siitä, käsitelläänkö henkilötietoja, tai mitä henkilötietoja käsitellään ja miten?

Sen lisäksi, että ostajan rooli määrittelyssä on epäselvä, tulee ottaa huomioon myös se seikka, että käsittelyn tarkoituksia voi olla useampia. Onnistunut kauppa ja itse due diligence -tarkastus ovat mitä todennäköisimmin henkilötietojen käsittelyn keskeisin tarkoitus ostajan kannalta, mutta vaikeampi kysymys lienee se, voitaisiinko tarkoitukseksi katsoa myös asianajotoimiston intressit due diligence -tarkastuksessa. Myös asianajotoimistolla on intressinsä due diligence -tarkastuksessa, sillä tarkastus on osa asianajotoimiston tavanomaista liiketoimintaa. Siksi myös asianajotoimistolla voitaisiin katsoa olevan taloudellinen intressi käsittelyssä. Vaikka intressi ei suoraan kulje käsi kädessä tarkoituksen kanssa, sopii asianajotoimiston taloudellinen intressi kuitenkin määritelmään ”suunniteltua toimintaa ohjaava tekijä”. On muistettava, että due diligence -tarkastukseen sisältyy myös runsaasti muita osa-alueita kuin henkilötietojen käsittelyä vaativia osioita. Tämä puoltaa sitä, ettei henkilötietojen käsittelyn tarkoituksena pidettäisi asianajotoimiston taloudellisen intressin toteuttamista.

[108] Olisi toki myös mahdollista tarkastella asianajotoimiston roolia jokaisen due diligence -tarkastuksessa käsiteltävän henkilötietoryhmän osalta erikseen, mutta koska perimmäinen tarkoitus kaikkien käsiteltävien tietojen osalta on sama, en pidä tällaista lähestymistapaa tarpeellisena. Oletus on siis, että asianajotoimiston rooli henkilötietoja käsiteltäessä on sama ja koskee koko due diligence -tarkastusta.

Tarkoituksen lisäksi on rekisterinpitäjän asemaa arvioitaessa kiinnitettävä huomiota käsittelyn keinoihin eli siihen, miten tietoja käsitellään. Tietosuojatyöryhmä korostaa, ettei käsittelyn keinoilla tarkoiteta ainoastaan teknisiä keinoja, vaan keinoihin liittyvät myös mm. kysymykset siitä, mitä henkilötietoja käsitellään, kenellä on pääsy henkilötietoihin ja milloin henkilötiedot poistetaan.[109] Asianajotoimiston hoitaessa toimeksiantoaan on selvää, että se osallistuu henkilötietojen käsittelyn keinojen määrittelyyn, joskin se voi määritellä keinot yhdessä asiakkaansa kanssa. Yleensä asianajotoimisto on kuitenkin asiantuntijaorganisaationa se taho, jolla on vastaukset yllä mainittuihin kysymyksiin (mitä henkilötietoja tarkastuksessa käsitellään, miten ja kuinka kauan niitä säilytetään). Asianajotoimisto voi osallistua kohdeyhtiön/myyjän tai sen edustajan kanssa myös esimerkiksi sen määrittelyyn, miten käsittelyn tekninen puoli on järjestetty; nykyisin tiedot ladataan useimmiten virtuaalisiin datahuoneisiin, mutta periaatteessa on mahdollista, että due diligence -tarkastuksen materiaali (ja siten henkilötiedot) luovutettaisiin asianajotoimistolle paperisena.

Vaikka määritelmän mukaan rekisterinpitäjänä pidetään sitä, joka määrittelee henkilötietojen käsittelyn keinot, tietosuojatyöryhmän kannanotossa on todettu, että keinojen määrittely voi toisaalta joissakin tapauksissa kuulua henkilötietojen käsittelijälle. Rajanvetotapauksissa olisi kuitenkin kiinnitettävä huomiota käsittelyn tarkoitusten ja keinojen väliseen suhteeseen siten, että määriteltävien keinojen rooli olisi lähinnä toimia tarkoitusten saavuttamisen välineenä. Jos keinot määrittelee henkilötietojen käsittelijä, tulee rekisterinpitäjälle antaa tieto määritellyistä keinoista kokonaisuudessaan. Lisäksi olisi kiinnitettävä huomiota siihen, kuinka tarkat ohjeet keinojen määrittelyyn on rekisterinpitäjän taholta annettu.[110]

Näin ollen voidaan siis todeta, että mikäli asianajotoimiston ei katsota osallistuvan due diligence -tarkastuksessa käsiteltävien henkilötietojen käsittelyn tarkoitusten määrittelyyn, se ei tietosuojatyöryhmän kannanoton perusteella välttämättä ole rekisterinpitäjä, vaikka se osallistuisi keinojen määrittelyyn. Asianajotoimiston osallistuessa keinojen määrittelyyn tulee toisaalta huomioida se, antaako se keinoista tiedon rekisterinpitäjälle. Kysymyksestä monimutkaisen tekee kuitenkin se, että sen arvioimiseksi tulisi ensin hahmottaa, mikä taho toimii rekisterinpitäjänä, mikäli due diligence -tarkastusta tekevä asianajotoimisto katsottaisiin henkilötietojen käsittelijäksi.

[109] WP 169, s. 14.
[110] WP 169, s. 14.

4.1.3 Rekisterinpitäjän tosiasiallinen rooli

Vaikka tarkoitusten ja keinojen määrittely on rekisterinpitäjän roolin tunnistamisen eräänlainen ydin, on roolin varmistamisessa otettava huomioon myös muita siihen vaikuttavia tekijöitä. Tietosuojatyöryhmän kannanotossa todetaankin, että kysymys on henkilötietojen käsittelyyn osallistuvan *tosiasiallisesta roolista*, minkä arvioimiseksi pelkkien muodollisten kriteerien tarkastelu ei ole riittävää vaan saattaa johtaa tilanteisiin, jossa rekisterinpitäjän nimeäminen ei vastaa todellisuutta tai on puutteellinen.[111]

Rekisterinpitäjän roolia on arvioitu myös useissa EU:n tuomioistuimen (CJEU) tapauksissa, joita käsitellään tarkemmin yhteisrekisterinpitäjiä koskevassa luvussa 4.2. Tuomioistuimen ratkaisuissa korostuu vahvasti tietosuoja-asetuksen (ja henkilötietodirektiivin, jonka ajalta tapaukset ovat) 1 artiklan mukainen tavoite suojella luonnollisia henkilöitä ja heidän perusoikeuksiaan ja vapauksiaan, sekä erityisesti oikeutta henkilötietojen suojaan. CJEU onkin toimijoiden roolia arvioidessaan kiinnittänyt huomiota luonnollisten henkilöiden oikeuksien kokonaisvaltaisen ja kattavan suojelun toteutumiseen ja todennut, että rekisterinpitäjän määritelmää olisi sen vuoksi tulkittava laajasti.[112] Näin ollen on siis arvioitava sitä, muodostaisiko toimijan määritteleminen muuksi kuin rekisterinpitäjäksi aukkoja oikeuksien suojeluun.[113]

Oikeuksien kattavan suojaamisen lisäksi CJEU on arvioinut toimijan roolia myös henkilötietojen käsittelyn kokonaisuuden kannalta. Ratkaisussaan *Google Spain* tuomioistuin kiinnitti huomiota hakukoneen rooliin tietojen kokonaisvaltaisessa jakelussa. Vaikka Googlella ei olisi määräysvaltaa toiselta internetsivustolta löytyviin henkilötietoihin, sen rooli henkilötietojen jakelussa on niin merkittävä, että sitä on pidettävä rekisterinpitäjänä, kun tiedot löytyvät hakukoneen kautta.[114] Myös tietosuojatyöryhmä on kiinnittänyt huomiota henkilötietojen käsittelijän rooliin kokonaisuutena. Esimerkiksi SWIFT:n[115] henkilötietojen käsittelyä koskevassa kannanotossaan työryhmä on määritellyt SWIFT:n rekisterinpitäjäksi ja todennut muun muassa, että faktojen perusteella SWIFT:llä on itsenäisempi rooli kuin toimia ainoastaan asiakkaidensa lukuun [henkilötietojen käsittelyssä].[116] On kuitenkin huomattava, että niin oikeuskäytännössä

[111] WP 169, s. 8.
[112] Asia C-210/16, kohdat 28 ja 42 ja Asia C-131/12, kohta 34.
[113] *Lindroos-Hovinheimo* 2019, s. 232.
[114] Asia C-131/12, kohdat 36–38.
[115] SWIFT eli *Society for Worldwide Interbank Telecommunication* on kansainvälinen palvelu, jonka kautta pankit voivat lähettää ja vastaanottaa viestejä rahan liikkumiseen (transaktioihin) liittyen suojatussa ympäristössä. Viestit sisältävät henkilötietoja muun muassa maksajista ja maksun saajista ja SWIFT vastaa viestien säilyttämisestä.
[116] WP 128, s. 11.

kuin tietosuojatyöryhmän kannanotossakin arvioinnin ydin on siinä, kuka määrittelee käsittelyn keinot ja tarkoitukset. Henkilötietojen käsittelyn kokonaisuutta ei siis arvioida itsenäisenä, irrallisena kriteerinä, vaan siitä voidaan saada tukea rekisterinpitäjän määrittelyyn.

Kun arvioidaan asianajotoimiston roolia due diligence -tarkastuksessa, on selvää, että sen rooli on tarkastuksen tekijänä kokonaisvaltainen. Se hoitaa tarkastuksen ja päättää siitä, miten tarkastus käytännössä ja teknisiltä osin toteutetaan, minkä vuoksi sillä on myös paremmat edellytykset vastata henkilötietojen kokonaisvaltaisesta suojaamisesta kuin ostajalla, joka ei tarkastuksessa osallistu käsittelyyn. Toisaalta on tarpeellista huomioida myös asianajotoimiston ja tietoja luovuttavan myyjän (tai sen edustajan) välinen suhde, sillä henkilötietojen laajan määritelmän vuoksi myös myyjäpuolen voidaan tietojen luovuttamisen osalta katsoa käsittelevän henkilötietoja tarkastuksessa ja sillä on prosessin alusta lähtien tarkat tiedot siitä, kenestä (ja mitä) henkilötietoja on annettu. Myyjällä on myös pääsy datahuoneeseen, jossa tietoja säilytetään, mutta toisaalta sillä ei välttämättä ole varmuutta siitä, onko asianajotoimisto ladannut tietoja datahuoneesta ja miten käsittely tarkalleen ottaen tapahtuu.

Kuten edellä on todettu, asianajotoimisto suorittaa due diligence -tarkastusta ostajan lukuun ja vaikuttaisi siten, ilman tarkempaa analyysia, henkilötietojen käsittelijältä. Samankaltainen tilanne on nähtävissä myös tietosuojatyöryhmän kannanotossa, jossa SWIFT toimii henkilötietoja käsitellessään pankkien lukuun ja siksi sen katsottiin lähtöolettamana toimivan henkilötietojen käsittelijänä. WP29 määritteli kuitenkin organisaation rekisterinpitäjäksi ja katsoi, että SWIFT:n roolia on pidettävä itsenäisenä muun muassa siksi, että se päättää mitä henkilötietoja palvelussa käsitellään ja miten paljon tietoa jaetaan pankeille. Lisäksi WP29 on arvioinut, että SWIFT määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot muun muassa kehittämällä, markkinoimalla ja muuttamalla palveluitaan ja henkilötietojen käsittelyä ilman pankkien suostumusta.[117]

Vaikka SWIFT:n toimiala ja tehtävät poikkeavat asianajotoimiston roolista due diligence -tarkastuksessa, on WP29:n kannanotto mielestäni analogisesti sovellettavissa myös asianajotoimistoon. Tietyllä tavalla myös asianajotoimisto on tarkastuksessa se taho, joka päättää, mitä tietoja käsitellään[118] ja mitkä tiedot ovat siltä osin relevantteja, että ne on syytä tuoda ostajan

[117] WP 128, s. 11.
[118] Asianajotoimisto voi luonnollisesti päättää käsiteltävistä henkilötiedoista sen puitteissa, mitä tietoja myyjäpuoli due diligence -tarkastusta varten luovuttaa toimistolle. Luovutettavat tiedot riippuvat muun muassa siitä, onko

tietoon tarkastuksen lopputulosta esiteltäessä. Käsittelyn keinojen ja tarkoitusten osalta asianajotoimisto osallistuu selkeästi ainakin keinojen määrittelyyn, mutta tarkoitusten määrittelyyn osallistumisen arviointi on haasteellisempaa ja riippuu mm. siitä, pidetäänkö asianajotoimiston taloudellista intressiä henkilötietojen käsittelyn tarkoituksena.

Rekisterinpitäjän määrittelyyn liittyy käytännön näkökulmasta myös kysymys siitä, miten yksityiskohtaisesti toimijan tulee osallistua tarkoitusten ja keinojen määrittelyyn ollakseen rekisterinpitäjä. Useampien toimijoiden rooleja arvioitaessa onkin kiinnitettävä huomiota siihen, millainen harkintavalta ja liikkumavara toimijalla on päätöksenteossa ja tarkoitusten määrittelyssä. Tällöin roolien arvioimiseksi voidaan esittää kysymys: käsittelisikö toimija henkilötietoja ilman, että toinen taho (rekisterinpitäjä) olisi pyytänyt sitä?[119] WP29 tarkoittaa kannanotossaan erityisesti ulkoistamistilanteita, jollaisesta voidaan nähdä olevan kyse myös asianajotoimiston suorittaessa due diligence -tarkastusta. Toimisto tekee tarkastuksen toimeksiannon perusteella, eli asiakas on ulkoistanut tarkastuksen tekemisen asianajotoimistolle.

Vastaus WP29:n kannanotossa esitettyyn kysymykseen olisikin asianajotoimiston osalta yksiselitteisesti kieltävä. Asianajotoimistolla ei olisi syytä käsitellä henkilötietoja ilman ostajan pyyntöä, sillä tällöin se ei tekisi tarkastusta. Toisaalta ostaja ei todennäköisesti esitä toimeksiantoa tehdessään asianajotoimistolle pyyntöä nimenomaan henkilötietojen käsittelystä, vaan koko tarkastuksesta. Tämä näkökulma ei kuitenkaan liene relevantti, sillä joka tapauksessa voidaan todeta, ettei henkilötietojen käsittelyä tapahtuisi ilman ostajan toimeksiantoa.

Asianajotoimiston toimiminen rekisterinpitäjänä näyttäytyy edellä esitetyn valossa epäselvältä. Sekä määritelmän puolesta että sitä vastaan puhuvia seikkoja on löydettävissä ja rajanveto näyttäisi pitkälti riippuvan näkökulmasta. WP29 on kuitenkin katsonut asianajajien lukeutuvan yleensä ottaen rekisterinpitäjiksi. Sen antamassa esimerkissä kysymys on oikeudenkäynnistä, jossa henkilötietojen käsittelyperusteena on asiakkaan oikeutettu etu, mutta asianajajan toiminta olisi katsottava ammatinharjoittamiseen yleisesti liittyväksi (”*for which activity such professions have traditionally their own legal basis”),* minkä vuoksi asianajajaa olisi pidettävä rekisterinpitäjänä.

kyseessä huutokauppa, jossa mahdollisesti liikesalaisuudenkin piiriin kuuluvia tietoja pitäisi antaa usealle ostajakandidaatille, vai kahden osapuolen kauppa, josta on jo tehty osapuolia sitova aiesopimus.
[119] WP 128, s. 13.

Tietosuojatyöryhmän kannanotto jättää kuitenkin avoimeksi sen, mikä asiakkaan rooli olisi tällöin henkilötietojen käsittelyssä. Esimerkissä ei myöskään ole suoraan arvioitu tarkoitusten ja keinojen määrittelyä, vaan lähestytty asiaa muun muassa asianajajalla olevan ammattitaidon ja perinteisen roolin näkökulmasta, minkä vuoksi esimerkkiä on mielestäni syytä tarkastella kriittisesti. Tutkielman kysymyksen kannalta on myös oleellista ottaa huomioon asiakkaalla mahdollisesti oleva ammattitaito – ostajalla voi olla laaja kokemus yrityskaupasta ja henkilötietojen käsittelystä sen yhteydessä, minkä vuoksi due diligence -tarkastus poikkeaa luonteeltaan oikeudenkäynnistä. Lisäksi roolin uudelleenarviointi voi olla relevanttia johtuen tietosuoja-asetuksen tuomista uusista velvoitteista niin rekisterinpitäjille kuin henkilötietojen käsittelijöillekin, sillä direktiivin aikaisessa kannanotossa henkilötietojen aukoton suoja on saattanut vaatia erilaista arviointia. Vastuukysymyksiin ja henkilötietojen kattavan suojan turvaamiseen palataan pääluvussa 5.

4.2 Yhteisrekisterinpitäjät

Rekisterinpitäjä määrittelee tietosuoja-asetuksen mukaan henkilötietojen käsittelyn tarkoitukset ja keinot joko yksin *tai yhdessä toisten kanssa* (tietosuoja-asetuksen 4 artiklan kohta 7). Asetuksen 26 artiklan mukaan, jos käsittelyn tarkoitukset ja keinot määrittää vähintään kaksi rekisterinpitäjää, ne ovat *yhteisrekisterinpitäjiä (joint controllers).* Yhteisrekisterinpitäjiä koskeva artikla on tietosuoja-asetuksessa uusi, sillä käsitettä ei löydy asetusta edeltävästä henkilötietodirektiivistä (95/46/EY). Rekisterinpitäjä on kuitenkin määritelty direktiivissä samoin kuin asetuksessa, eli myös direktiivin mukaan käsittelyn tarkoitukset ja keinot voidaan määrittää yhdessä. Lisäksi yhteisrekisterinpitäjät (*joint controllers*) on terminä esiintynyt oikeuskirjallisuudessa ja virallislähteissä jo henkilötietodirektiivin aikana, vaikkei siitä aiemmin ole säädetty erikseen.

Mikäli asianajotoimiston katsottaisiin täyttävän rekisterinpitäjän määritelmän, tulisi todennäköisesti arvioitavaksi myös se, toimisiko se rekisterinpitäjänä itsenäisesti vai yhteisrekisterinpitäjänä toisen tahon kanssa. Sitä, minkä tahon (tai tahojen) kanssa asianajotoimiston olisi mahdollista toimia yhteisrekisterinpitäjänä, voidaan hahmottaa tarkastelemalla suunnitellun yrityskaupan sopimussuhteita. Luonnollisesti yksi vaihtoehto on, että asianajotoimisto olisi yhteisrekisterinpitäjä asiakkaansa, eli ostajan kanssa. Toinen vaihtoehto olisi, että yhteisrekisterinpitäjyys syntyisi myyjän tai sitä edustavan tahon kanssa, sillä kuten edellä on todettu, myös myy-

jäpuoli osallistuu due diligence -tarkastuksessa käsiteltävien henkilötietojen käsittelyyn. Yhteisrekisterinpitäjien määrittelemiseksi on kuitenkin jälleen palattava rekisterinpitäjän roolin keskeisimpään kriteeriin, eli tarkoitusten ja keinojen määrittelyyn.

Yhteisrekisterinpitäjiksi voidaan katsoa myös sellaisia tahoja, jotka eivät ole määritelleet keskinäisiä vastuualueitaan. Jos katsotaan, että molemmat käsittelyyn osallistuvat tahot ovat osallistuneet myös käsittelyn keinojen ja tarkoitusten määrittelyyn, niitä voidaan pitää yhteisrekisterinpitäjinä, vaikka he eivät olisi määritelleet keskinäisiä järjestelyitään.[120] Tällainen tilanne syntyy yleensä siten, että yhteisrekisterinpitäjät ovat määritelleet roolinsa toisin[121] tai eivät ole määritelleet roolejaan ollenkaan. Jos roolit on määritelty erilaisiksi ja todellisuudessa kysymys on yhteisrekisterinpitäjistä, on mahdollista, että toiminnassa rikottu tietosuoja-asetuksen 26 artiklaa.[122]

Yhteisrekisterinpitäjät määrittävät siis henkilötietojen käsittelyn tarkoitukset ja keinot yhdessä. Tietosuoja-asetuksesta ei kuitenkaan käy ilmi se, tuleeko yhteisrekisterinpitäjillä olla sama tarkoitus (tai tarkoitukset) henkilötietojen käsittelylle.[123] EU:n tietosuojatyöryhmän mukaan tarkoitusten tulee olla yhteneviä ainakin osittain. Vaikka tarkoitukset näyttäytyisivät mikrotasolla erilaisina, tulisi henkilötietojen käsittelyn vaiheiden ja tarkoitusten yhteyttä tarkastella myös makrotasolla, jolla yhteinen tarkoitus voi löytyä.[124] Mikäli (edes osittaista) yhteistä tarkoitusta ei löydy, on kysymyksessä kaksi erillistä rekisterinpitäjää. Tällöin muun muassa rekisterinpitäjien välinen vastuunjako määräytyy toisin.

Due diligence -tarkastuksen tarkoitus on varmistua siitä, että kaupan kohde vastaa sovittua. Tämä on ennen kaikkea nähtävä ostajan intressinä, vaikka on myös myyjän edun mukaista tietää, mitä kohdeyhtiö pitää sisällään. Halutessaan myyjä teettää tai tekee kuitenkin itse oman due diligence -tarkastuksensa, joten ostajan teettämässä tarkastuksessa ei ole kysymys myyjän edusta. Myyjä luovuttaa kohdeyhtiöstä tiedot tarkastusta varten, jotta yrityskauppa toteutuisi. WP29 on kuitenkin lausunnossaan (WP 169) korostanut, että henkilötietojen siirtäminen toisen

[120] *Meyer* 2018, s. 22.
[121] Ks. esim. *Hintze* 2018, s. 19. Koska henkilötietoja käsittelevät tahot voivat olla niin käsittelijöitä, rekisterinpitäjiä kuin yhteisrekisterinpitäjiäkin, toimijoiden keskinäiset suhteet toisiinsa eivät aina ole selvät ja erilaisia variaatioita, joihin laintulkinta voi johtaa, on useita.
[122] *Meyer* 2018, s. 22.
[123] *Korpisaari – Pitkänen – Warma-Lehtinen* 2018 s. 283.
[124] WP 169, s. 20.

tahon käsiteltäväksi ei itsessään luo yhteisrekisterinpitäjyyttä luovuttajan ja vastaanottajan välille. Vaikka molemmat tahot käsittelisivät samoja tietoja, niiden tarkoitukset ja keinot voivat olla erilliset, jolloin tahot katsotaan kahdeksi erilliseksi rekisterinpitäjäksi.[125]

Makrotasolla tarkoituksia voidaan ostajan ja myyjän kesken sinänsä pitää samana, mutta koska ostaja yleensä pyrkii käyttämään tarkastuksen lopputulosta neuvotteluvalttina, ovat intressit myös vastakkaiset. Tilanne on nähdäkseni sama myös silloin, kun ostajaehdokkaita ja siten tarkastuksen tekijöitä on useampia kuin yksi. Ostajan ja asianajotoimiston välisessä suhteessa tarkastuksen tarkoitus voidaankin nähdä yhteisenä helpommin. Niiden tavoitteena on tarkastuksen avulla saavuttaa ostajan näkökulmasta onnistunut yrityskauppa, vaikkakin asianajotoimistolla voidaan nähdä olevan myös oma, erillinen intressinsä ammatinharjoittajana. Näin ollen asianajotoimistolla ja ostajalla on ainakin osittainen yhteinen tarkoitus henkilötietoja käsiteltäessä ja niiden välillä yhteisrekisterinpitäjyys näyttää todennäköisemmältä kuin myyjän ja asianajotoimiston välillä.

Vaikka yhteisrekisterinpitäjiä koskevaa sääntelyä ei ollut henkilötietodirektiivissä, on CJEU antanut kesällä 2018 kaksi ratkaisua, joissa se on katsonut henkilötietojen käsittelijät yhteisesti vastuullisiksi rekisterinpitäjiksi. Koska tapauksiin on sovellettu henkilötietodirektiiviä, niissä ei ole arvioitu tietosuoja-asetuksen 26 artiklan toteutumista. Artiklassa on säädetty yhteisrekisterinpitäjien vastuusta, jota käsitellään jäljempänä luvussa 5.6. CJEU:n ennakkoratkaisuja voidaan kuitenkin käyttää apuna yhteisrekisterinpitäjiä määriteltäessä.

Ensimmäisessä asiassa (C-210/16) yksi ratkaistava kysymys oli se, tulisiko Facebookissa fanisivua hallinnoivaa Wirtschaftsakademiea pitää rekisterinpitäjänä niiden henkilötietojen osalta, jotka Facebook keräsi fanisivulla kävijöistä ja joita Facebook käsitteli. Koska fanisivun hallinnoija osallistui käsittelyyn muun muassa valitsemalla parametrit, joiden perusteella fanisivulla vierailevien henkilötietoja kerättiin, ja lisäksi vastaanotti Facebookilta kohdeyleisöään koskevia tilastoja, tuomioistuin katsoi ratkaisussaan, että hallinnoija osallistui käsittelyn keinojen ja tarkoitusten määrittelyyn ja sitä oli siksi pidettävä rekisterinpitäjänä Facebookin kanssa.[126] Osittain samanlainen asetelma on nähtävissä myös due diligence -tarkastuksessa asianajotoimiston ja ostajan välillä. Asianajotoimisto käsittelee tietoja, mutta ostajan ja yrityskaupan tar-

[125] WP 169, s. 20. Erityisesti esimerkki 9.
[126] Asia C-210/16, kohta 39.

koitukset määrittelevät sitä, mitä henkilötietoja yrityskaupassa on tarpeen käsitellä (vrt. parametrien valitseminen). Ostaja myös vastaanottaa asianajotoimiston käsittelemät tiedot due diligence -raportin muodossa.

Toisaalta CJEU on tapauksessa katsonut, että Wirtschaftsakademien vastuuta korosti tietojen kerääminen myös muista kuin Facebook-käyttäjistä. Henkilötietojen käsittelyn kohteeksi joutuivat kaikki ne, jotka päätyivät Wirtschaftsakademien hallinnoimalle sivulle.[127] Due diligence -tarkastuksessa kerättävät henkilöt ovat tarkoin rajattuja, minkä vuoksi ostajan vastuuta ei tarkastuksessa voida ainakaan samalla perusteella (tai analogisesti) korostaa.

Toisessa asiassa (C-25/17) oli kysymys Jehovan todistajien uskonnollisen yhdyskunnan ovelta ovelle -saarnaamistyöstä ja sen yhteydessä manuaalisesti muistivihkoon kerättävistä henkilötiedoista. Tuomioistuin katsoi, että tapauksessa rekisterinpitäjinä voitiin pitää sekä yhdyskunnan jäseniä, jotka keräsivät henkilötietoja, että itse yhdyskuntaa, jonka tavoitteen toteutumista varten henkilötietoja käsiteltiin.[128] Vaikka yhdyskunta ei tapauksessa kerännyt (kieltorekisteriä lukuun ottamatta) tietoja itselleen, katsottiin, että merkitystä oli yhdyskunnan tosiasiallisella määräysvallalla sekä tietoja keräävien jäsenten käsityksellä siitä, toimiiko yhdyskunta rekisterinpitäjänä.[129]

Ostajan ja asianajotoimiston välisessä suhteessa ostajalla voidaan sinänsä nähdä olevan määräysvaltaa, että asianajotoimisto toimii sen lukuun. Käytännössä on kuitenkin epätodennäköistä, että ostaja käyttäisi määräysvaltaansa ohjeistamalla asianajotoimistoa. Lähtökohtaisesti ei myöskään voitane katsoa, että osapuolten välillä olisi tapauksen kaltaista epäselvyyttä siitä, toimiiko ostaja rekisterinpitäjänä. Asianajotoimistolla voidaan näet katsoa olevan sellainen asiantuntemus, että henkilötietojen käsittelystä aiheutuvat vastuut ja roolit on määritelty tarkoin jo ennen tarkastuksen aloittamista.

Tuorein yhteisrekisterinpitäjyyttä koskeva CJEU:n ratkaisu (C-40/17) on annettu heinäkuussa 2019. Niin kutsutussa *Fashion ID* -tapauksessa oli kysymys internetsivuston ylläpitäjän vastuusta, kun sen sivuille asetetun Facebookin tykkäyspainikkeen vuoksi sivustolla vierailevien henkilötietoja päätyi automaattisesti Facebookille. Fashion ID ja Facebook katsottiin ratkaisussa yhteisrekisterinpitäjiksi. CJEU:n mukaan yhteisrekisterinpitäjyys ei kuitenkaan tarkoita

[127] Asia C-210/16, kohta 41.
[128] Asia C-25/17, kohdat 68–75.
[129] Asia C-25/17, kohdat 21–23.

sitä, että vastuu jakautuisi tasan tai olisi samanlaista yhteisrekisterinpitäjien välillä. Toimijat voivat näet osallistua käsittelyyn eriasteisesti.[130] Eritasoinen rekisterinpitäjien välinen vastuu voisi realisoitua myös due diligence -tarkastuksessa, mikäli ostajan (tai myyjän) ja asianajotoimiston katsottaisiin olevan yhteisrekisterinpitäjiä. On selvää, että osapuolten osallistuminen käsittelyyn on erilaista. Mahdollista on myös, ettei ostaja käytännössä osallistu käsittelyyn vaan sen rooli muodostuisi lähinnä tekemänsä toimeksiannon perusteella ja siksi, että se voi mahdollisesti vastaanottaa tietoja asianajotoimistolta. CJEU:n mukaan yhteisrekisterinpitäjyys ei näet edellytä, että kaikilla rekisterinpitäjillä olisi pääsyä käsiteltäviin henkilötietoihin.[131]

Tuomioistuinkäytännöstä löytyy siis useita yhteisrekisterinpitäjyyttä käsitteleviä tapauksia. Vaikka tapauksissa käsitellyt tilanteet ovat erilaisista tilanteista verrattuna tutkielman tilanteeseen, voidaan niiden perusteluita käyttää myös käsillä olevan tilanteen arviointiin. Tapausten valossa ei näyttäisi olevan mahdotonta, että yhteisrekisterinpitäjyys syntyisi asianajotoimiston ja ostajan välille. Toisaalta edellä käsitellyt tapaukset ovat kaikki henkilötietodirektiivin ajalta, jolloin tietosuoja-asetuksen 26 artiklaa vastaavaa sääntelyä vastuunjakautumisesta ei ollut. Lisäksi, kuten jäljempänä pääluvussa 5 havaitaan, vastuuasetelmat ovat henkilötietodirektiivin ajalta muuttuneet siten, ettei toimijoiden määritteleminen yhteisrekisterinpitäjiksi enää välttämättä ole yhtä tärkeässä roolissa rekisteröidyn oikeuksien turvaamisen näkökulmasta.

4.3 Henkilötietojen käsittelijän määritelmä

Henkilötietojen käsittelijä käsittelee tietosuoja-asetuksen mukaan henkilötietoja rekisterinpitäjän lukuun (4 artiklan 8 kohta). Käsitteen määritelmä on pysynyt muuttumattomana henkilötietodirektiiviin nähden, mutta direktiiviä edeltäneessä tietosuojasopimuksessa henkilötietojen käsittelijän määritelmää ei vielä ollut. Tietosuojatyöryhmän kannanoton mukaan tietojen käsittely jonkun toisen *lukuun* tarkoittaa, että käsittely tapahtuu toisen tahon tarkoituksen palvelemiseksi. Sen voidaan siten katsoa muistuttavan valtuuttamista.[132] On kuitenkin huomattava, että tosiasiallisesti roolin määritteleminen henkilötietojen käsittelijäksi tai rekisterinpitäjäksi tapahtuu samassa prosessissa ja näiden määritelmien arvioinnin erottaminen omiksi tarkasteltaviksi kokonaisuuksiksi on sinänsä keinotekoista ja toimii lähinnä akateemisen tekstin jäsentämiseksi.

[130] Asia C-40/17, kohta 70. Vastaavasti asia C-25/17, kohta 66.
[131] Asia C-40/17, kohta 69.
[132] WP 169, s. 25.

Arvioitaessa asianajotoimiston asemaa due diligence -tarkastuksessa, henkilötietojen käsittelijän määritelmän voitaisiin sanamuotonsa perusteella katsoa sopivan siihen: asianajotoimisto käsittelee tietoja ostajan tekemästä toimeksiannosta, ostajan tarkoituksen (onnistunut yrityskauppa) palvelemiseksi, eli ostajan lukuun. Kuten edellä on hahmotettu, rekisterinpitäjän ja henkilötietojen käsittelijän välisen eron määrittelemiseen liittyy kuitenkin useita haasteita. Näin ollen on syytä tarkastella myös henkilötietojen käsittelijän määritelmää ja roolia tarkemmin.

Henkilötietojen käsittelijän olemassaolo riippuu siitä, miten rekisterinpitäjä on päättänyt järjestää henkilötietojen käsittelyn: se voi käsitellä tietoja itse tai valtuuttaa kolmannen osapuolen käsittelemään tietoja.[133] Due diligence -tarkastuksessa ostaja on valtuuttanut asianajotoimiston tekemään tarkastuksen ja käsittelemään henkilötietoja siinä yhteydessä. Ostaja voisi tehdä tarkastuksen myös itse, jolloin henkilötietojen käsittelijän roolia ei erikseen tarvitsisi arvioida. Ostajan ei nimittäin voitane katsoa tekevän tarkastusta ja siten käsittelevän henkilötietoja esimerkiksi myyjän tai sen edustajan lukuun. Kyseinen päätelmäketju varmistaa toisaalta myös sen, ettei myöskään tarkastusta tekevän asianajotoimiston voida katsoa toimivan henkilötietojen käsittelijänä suhteessa myyjään tai sen edustajaan. Näin ollen, mikäli asianajotoimisto katsotaan tarkastuksessa henkilötietojen käsittelijäksi, näyttäisi olevan selvää, että ostaja toimii tällöin rekisterinpitäjänä.

Henkilötietojen käsittelijän ja rekisterinpitäjän määritelmän välinen rajanveto riippuu niistä tosiasiallisista toimista, joita tietoja käsiteltäessä tehdään. Tällä tarkoitetaan ensinnäkin sitä, että käsittelijä voi toimia eri roolissa erilaisten henkilötietojen osalta ja roolia on arvioitava henkilötietoryhmittäin.[134] Vaikka due diligence -tarkastuksessa käsitellään useita eri henkilötietoryhmiä (mm. työntekijät, osakkeenomistajat, johdon jäsenet), käsittely tapahtuu kaikkien ryhmien osalta samaa tarkoitusta varten ja asianajotoimiston roolin voidaan siten katsoa olevan sama kaikkien tarkastuksessa käsiteltävien henkilötietoryhmien osalta.

Tosiasiallisten toimien osalta on arvioitava toisaalta, onko henkilötietoja käsittelevällä taholla merkityksellistä roolia käsittelyn tarkoitusten ja keinojen määrittelyssä. Kuten aiemmin luvussa 4.1 on tuotu esiin, lähtökohtaisesti käsittelyn tarkoitukset ja keinot määrittelee rekisterinpitäjä. Henkilötietojen käsittelijällä voi WP29:n mukaan olla kuitenkin tiettyä harkintaa sen suhteen,

[133] WP 169, s. 25.
[134] WP 169, s. 25.

miten se katsoo parhaiten toteuttavansa rekisterinpitäjän toimeksiannon. Henkilötietojen käsittelijä voi siis osallistua ainakin käsittelyn *keinojen* määrittelyyn.[135] Myös oikeuskirjallisuudessa on yleisesti päädytty tähän tulkintaan, vaikka on löydettävissä myös näkökulmia, joiden mukaan henkilötietojen käsittelijä osallistuu jossain määrin myös käsittelyn tarkoitusten määrittelyyn.[136] Euroopan unionin tuomioistuimen ratkaisukäytännön valossa lienee kuitenkin todennäköistä, että tarkoitusten määrittelyyn osallistuessaan henkilötietojen käsittelijä katsottaisiin herkästi pikemminkin yhteisrekisterinpitäjäksi.

Oikeuskirjallisuudessa vallitsevan näkemyksen mukaan keinot, joiden määrittelyyn henkilötietojen käsittelijä voisi osallistua, olisivat kuitenkin yleensä ottaen puhtaasti teknisiä.[137] Myös tietosuojatyöryhmä on tuonut kannanotoissaan esiin, että keinojen määrittely liittyy lähinnä teknisiin ja organisatorisiin keinoihin, jotka henkilötietojen käsittelijä voi määritellä itsenäisestikin.[138] Henkilötietojen käsittelijän määrittelemiseksi on arvioitava, mitä keinoja pidetään teknisinä ja organisatorisina. Jotkin toimenpiteet, kuten esimerkiksi tietojärjestelmän valitseminen ja henkilötietojen säilyttämismuoto, ovat selvästi määriteltävissä teknisiksi keinoiksi. Toisaalta esimerkiksi tietojen poistamiseen liittyvien keinojen on katsottu kuuluvan rekisterinpitäjälle siltä osin, kuin päätetään, *milloin* tiedot poistetaan[139], mutta henkilötietojen käsittelijä voisi määritellä sen, *miten* tiedot poistetaan.[140]

Kuten olen edellä luvussa 4.1.2 tuonut esiin, näyttää varsin selvältä, että asianajotoimisto osallistuu due diligence -tarkastuksessa ainakin keinojen määrittelyyn. Etenkin teknisten keinojen osalta on selvää, että asianajotoimisto on se taho, joka vastaa määrittelystä (asianajotoimisto voi myös ulkoistaa tietojen säilytyksen datahuonetta ylläpitävälle pilvipalvelulle). Muiden kuin teknisten keinojen osalta rajanveto asianajotoimiston ja asiakkaan välillä voi olla haastavampaa, mutta esimerkiksi yllä mainitun tietojen poistamisen osalta on todennäköistä, että vastuu niin tietojen poistamisen ajankohdasta kuin poistotavasta on asianajotoimistolla.[141] Asianajotoimisto on lähtökohtaisesti myös se taho, joka määrittelee, mitä tietoja käsitellään.

[135] WP 169, s. 25.
[136] *Hintze* 2018, s. 18. Kirjoittaja ei kuitenkaan artikkelissaan käsittele sitä, missä määrin ja miten henkilötietojen käsittelijä voisi osallistua tarkoitusten määrittelyyn.
[137] Ks. esim. *Blume* 2013, s. 142.
[138] WP 169, s. 14 ja 25 ja WP196, s. 8.
[139] WP 169, s. 14.
[140] *IT Governance* 2017, s. 240.
[141] Asianajotoimistolla voi olla myös vastuuasemaansa liittyvä tarve säilyttää tietoja kauemmin kuin ostajalla olisi.

Henkilötietojen käsittelijän rooliin liittyy lisäksi velvollisuus toimia rekisterinpitäjän antamien ohjeiden mukaan (vaikka henkilötietojen käsittelijä määrittelisi tekniset keinot täysin itsenäisesti) ja velvollisuus antaa rekisterinpitäjälle tieto määritellyistä keinoista. Asianajotoimiston rooli tarkastuksen toteuttamisessa on kuitenkin sinänsä itsenäinen. Tarkastukset kuuluvat asianajotoimiston tavanomaiseen liiketoimintaan ja vaikka ostaja voi antaa ohjeita tarkastukseen liittyen, on asianajotoimistolla yleensä runsaasti liikkumavaraa toteuttaa tarkastus parhaaksi katsomallaan tavalla. Tiedonvaihdon laajuutta ja ostajan kontrollia määrittää myös asianajotoimiston ja ostajan välillä tehty toimeksiantosopimus, jossa voidaan sopia myös henkilötietojen käsittelystä. Sopimuksessa ei kuitenkaan voida sitovasti määrätä osapuolten rooleista henkilötietojen käsittelijänä tai rekisterinpitäjinä, sillä roolit määräytyvät tosiasiallisten toimien perusteella. Henkilötietojen käsittelijän ja rekisterinpitäjän väliseen sopimukseen palataan luvussa 5.3.

5 VASTUUN JAKAUTUMINEN HENKILÖTIETOJEN KÄSITTELYSSÄ

5.1 Vastuunjaosta yleisesti

Henkilötietojen käsittelyn jatkuva lisääntyminen digitaalisessa yhteiskunnassa loi (ja luo edelleen) tarpeita selkiyttää henkilötietojen käsittelyyn liittyvää vastuuta. Vastauksena tähän tarpeeseen tietosuoja-asetuksessa on säädetty henkilötietodirektiiviä tarkemmin käsittelijöiden vastuualueista ja niiden jakautumisesta rekisterinpitäjän ja henkilötietojen käsittelijän välillä. Asetuksessa on useita uusia, molempien vastuuta lisääviä säännöksiä.

Henkilötietodirektiivissä vastuu henkilötietojen käsittelystä oli lähes yksinomaisesti rekisterinpitäjällä, eikä henkilötietojen käsittelijälle asetettuja suoria velvollisuuksia ollut direktiivissä lainkaan.[142] Käsittelijän velvollisuudet liittyivät lähinnä tietoturvaedellytyksiin ja sopimusvelvoitteisiin.[143] Tietosuoja-asetus on kuitenkin muuttanut asetelmaa huomattavasti, sillä myös henkilötietojen käsittelijälle on asetettu useita suoria vastuita ja velvollisuuksia. Monien asetuksessa säädettyjen velvollisuuksien osalta vastuu voi olla myös jakautunut henkilötietojen käsittelijän ja rekisterinpitäjän välillä. Vaikka kehitys on ollut tarpeen esimerkiksi monimutkaistuneiden käsittelijäketjujen vuoksi, on esitetty myös näkemyksiä, joiden mukaan uuden sääntelyn mukainen vastuunjakautuminen voi luoda epävarmuutta ja jopa riskejä tietosuojasääntelyn vakaudelle.[144]

Tämän luvun tarkoituksena on luoda katsaus vastuun jakautumiseen keskeisimpien tietosuojavelvoitteiden osalta rekisterinpitäjän ja henkilötietojen käsittelijän välillä sekä tarkastella tietosuoja-asetuksen tuomia muutoksia vastuunjakoon. Vastuualueiden tarkastelu on oleellinen osa tutkimuskysymykseen vastaamista, sillä esimerkiksi yhteisrekisterinpitäjien asemaa on CJEU:n ratkaisukäytännössä perusteltu usein tarpeella varmistaa rekisteröidylle aukoton henkilötietojen suoja. Koska henkilötietojen käsittelijällä ei ole ollut suoraa vastuuasemaa direktiivissä, kattava suoja on ollut mahdollista turvata ainoastaan määrittelemällä useampia toimijoita (yhteis)rekisterinpitäjiksi. Onkin tarpeen arvioida, voisiko henkilötietojen käsittelijän laajentunut vastuu vaikuttaa siihen, ketä on pidettävä rekisterinpitäjänä ja voitaisiinko henkilötietojen käsittelijäksi lukea useampia käsittelijöitä kuin direktiivin aikana ilman, että vaarannetaan rekisteröidyn oikeuksien toteutumista.

---

[142] *Treacy* 2012, s. 1. Henkilötietodirektiiviä kansallisesti implementoitaessa on kuitenkin voitu säätää myös henkilötietojen käsittelijän vastuusta, kuten esim. Irlannissa on tehty.
[143] *Hanninen – Laine – Rantala – Rusi – Varhela* 2017, s. 27.
[144] *Blume* 2013, s. 140.

5.2 Rekisterinpitäjän vastuu tietosuoja-asetuksen noudattamisesta

5.2.1 Osoitusvelvollisuus

Vaikka henkilötietojen käsittelijän vastuu ja merkitys ovat tietosuoja-asetuksessa kasvaneet, on rekisterinpitäjä viimesijaisesti vastuussa henkilötietojen käsittelyn lainmukaisuudesta. Rekisterinpitäjä näet vastaa siitä, että käsittelyssä noudatetaan tietosuoja-asetuksen mukaisia käsittelyperiaatteita ja sen on lisäksi pystyttävä osoittamaan periaatteiden noudattaminen (tietosuoja-asetuksen 5 artiklan 2 kohta). Jälkimmäistä velvollisuutta kutsutaan *osoitusvelvollisuudeksi* ja noudatettavat periaatteet on lueteltu saman artiklan 1 kohdassa.[145] Osoitusvelvollisuus on erityisen tärkeä siksi, että sillä on tarkoitus varmistaa tietosuojasäännösten tehokas toimeenpaneminen Euroopassa ja varmistua siitä, että sääntelyä noudatetaan käsittelyn joka vaiheessa eikä vasta silloin, kun havaitaan tietoturvaloukkauksia tai ongelmia.[146]

Säädöksessä osoitusvelvollisuudella viitataan vain käsittelyn periaatteiden noudattamiseen, mutta tosiasiallisesti säädös asettaa rekisterinpitäjälle osoitusvelvollisuuden koko tietosuoja-asetuksen noudattamisesta.[147] Rekisterinpitäjän on siis yhtäältä noudatettava asetusta ja toisaalta pystyttävä osoittamaan, että se (ja henkilötietojen käsittelijä) on tehnyt niin. Osoitusvelvollisuutta ei siten ole katsottu sisältöä luovaksi, vaan funktionaaliseksi normiksi ja se, *miten* tietoja käsitellään, ratkeaa muiden säännösten perusteella.[148] Osoitusvelvollisuuden täyttämiseksi rekisterinpitäjän tulee muun muassa dokumentoida käsittelyyn liittyviä seikkoja, ja siitä *miten ja mitä* on dokumentoitava, on säädetty asetuksen muissa artikloissa.

Osoitusvelvollisuus on tietosuoja-asetuksessa ensimmäistä kertaa oikeudellisesti sitova sääntö, sillä siitä ei säädetty henkilötietodirektiivissä, jossa rekisterinpitäjän oli sanamuodon mukaan ainoastaan huolehdittava periaatteiden noudattamisesta.[149] Asetuksessa osoitusvelvollisuuden merkitys korostuukin muun muassa sen vuoksi, että myös henkilötietojen käsittelijälle on asetettu suoria velvoitteita. Osoitusvelvollisuudella asetetaan siis rekisterinpitäjälle viimesijainen

[145] Periaatteita ovat käsittelyn lainmukaisuus, kohtuullisuus ja läpinäkyvyys, käyttötarkoitussidonnaisuus, tietojen minimointi, täsmällisyys, säilytyksen rajoittaminen sekä eheys ja luottamuksellisuus.
[146] Handbook on European data protection law, s. 174.
[147] Tietosuojavaltuutetun toimisto: Osoita noudattavasi tietosuojasäännöksiä. https://tietosuoja.fi/osoitusvelvollisuus
[148] *Vainio* 2017, s. 52.
[149] Osoitusvelvollisuus on kuitenkin sinänsä tunnistettu jo henkilötietodirektiivin aikana ja muun muassa tietosuojatyöryhmä on direktiivin aikaisissa kannanotoissaan (WP 168 ja WP 173) tuonut esiin tarpeen säätää osoitusvelvollisuudesta oikeudellisesti sitovasti tietosuojalainsäädännön tehokkaaksi toimeenpanemiseksi.

vastuu ja velvollisuus varmistua käsittelyn lainmukaisuudesta, vaikka se käyttäisikin käsittelyssä henkilötietojen käsittelijää.

Rekisterinpitäjän osoitusvelvollisuudesta on tietosuoja-asetuksen 5 artiklan lisäksi säädetty myös 24 artiklassa. Sen mukaan rekisterinpitäjän on toteutettava tarvittavat tekniset ja organisatoriset toimenpiteet, joilla voidaan varmistaa ja *osoittaa*, että käsittelyssä noudatetaan tietosuoja-asetusta (1 kohta).[150] Teknisillä toimenpiteillä tarkoitetaan tietojärjestelmiin ja laitteisiin liittyviä toimenpiteitä, kuten esimerkiksi erilaisten suojausjärjestelmien käyttöä, pseudonymisointia tai tietoja käsittelevän henkilöjoukon rajaamista teknisillä keinoilla. Organisatoriset toimenpiteet voivat puolestaan olla esimerkiksi yhtiön sisäisiä tietosuojakäytäntöjä, riskiarviointeja, henkilöstön kouluttamista sekä auditointeja, joilla varmistetaan toimenpiteiden toimivuus.[151]

Tarvittavien toimenpiteiden määrittäminen riippuu artiklan mukaan käsittelyn luonteesta, laajuudesta, asiayhteydestä sekä käsittelyyn liittyvistä, luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvista riskeistä. Riskit voivat olla fyysisiä, aineellisia tai aineettomia.[152] Due diligence -tarkastuksessa käsiteltävien henkilötietojen joukko ja käsittelyn asiayhteys ovat tarkoin rajattuja, eikä tarkastuksessa käsitellä esimerkiksi tietosuoja-asetuksen mukaisia arkaluontoisia tietoja, joiden kohdalla erilaisten riskien määrä ja vakavuus voivat olla huomattavampia. Tarkastuksessa käsiteltävien tietojen osalta riskit liittynevät ennen kaikkea tietoturvaloukkaustilanteisiin, joissa henkilötietoihin voidaan päästä luvattomasti käsiksi ja jotka voivat johtaa esimerkiksi identiteettivarkauksiin tai salassapitovelvollisuuden alaisten henkilötietojen luottamuksellisuuden menetykseen.

Osoitusvelvollisuuden nostamista oikeudellisesti sitovaksi säännökseksi perusteltiin aiemmin muun muassa sillä, että tietosuojan tulisi olla osa yhtiöiden vakiintuneita käytäntöjä ja sisäisiä menetelmiä, joiden avulla sääntelyn noudattamisen osoittaminen myös ulkoisille tahoille – kuten valvoville viranomaisille – olisi pakollista.[153] Mikäli rekisterinpitäjäksi katsottaisiin due diligence -tarkastuksessa ostaja, tulisi sen huolehtia asetuksen noudattamisesta ja osoitusvelvol-

[150] Teknisten ja organisatoristen toimien käyttö on myös osa henkilötietojen käsittelyä koskevia periaatteita ja niistä on säädetty asetuksen 5 artiklan 1 kohdan f alakohdassa (käsittelyn eheys ja luottamuksellisuus).
[151] Know Your Compliance, 2018.
[152] Tietosuoja-asetuksen johdanto, kohta 75.
[153] WP 168, s. 19–20.

lisuuden täyttämisestä. Todennäköisesti nämä velvoitteet koskettavat ostajaa jo muiden henkilötietoryhmien – kuten sen työntekijöiden – osalta, joihin nähden se on rekisterinpitäjä. Tarkastuksen osalta sen olisi kuitenkin arvioitava edellä mainittuja riskejä ja muita tekijöitä erikseen, jotta se voisi määritellä tarvittavat tekniset ja organisatoriset toimenpiteet tarkastukseen liittyen. Koska due diligence -tarkastusten voidaan katsoa olevan osa asianajotoimiston tavanomaista liiketoimintaa, olisi asianajotoimiston todennäköisesti helpompi täyttää osoitusvelvollisuus ja määritellä toimenpiteet, joilla sääntelyn noudattaminen henkilötietojen käsittelyssä varmistetaan. Esimerkiksi tietosuojakäytäntöjen määritteleminen ja henkilötietoja käsittelevän henkilöstön kouluttaminen voivat tosiasiassa osoittautua jopa mahdottomiksi toimenpiteiksi ostajalle, joka ei tosiasiassa käsittele tietoja.

Arvioitaessa ostajan ja asianajotoimiston mahdollisuuksia täyttää tietosuoja-asetuksen mukaiset velvoitteet on muistettava, etteivät osapuolten roolit määräydy sen mukaan, kenen olisi helpointa täyttää tietosuoja-asetuksen mukaiset velvoitteet, vaan toisin päin: velvoitteet määräytyvät sen mukaan, katsotaanko yrityksen toimivan rekisterinpitäjänä vai henkilötietojen käsittelijänä (eli määritteleekö yritys käsittelyn tarkoitukset ja keinot). Painoarvoa voidaan kuitenkin antaa sille, että CJEU:n ratkaisukäytännössä asiaa on lähestytty myös käänteisesti ja keskitytty siihen, miten turvataan rekisteröidyn henkilötietojen aukoton suoja. Turvaamisen kannalta oleellista on se, että rekisterinpitäjällä on myös tosiasiallinen mahdollisuus huolehtia sitä koskevien velvollisuuksien täyttymisestä.

Toisaalta CJEU on muun muassa *Fashion ID* -ennakkoratkaisussa todennut, että rekisterinpitäjäksi voidaan katsoa myös taho, joka ei voi mitenkään vaikuttaa siihen, miten toiselle taholle [kyseisessä tapauksessa Facebookille] välitettyjä tietoja käsitellään.[154] Tällöin kyseisen rekisterinpitäjän on mahdotonta täyttää osoitusvelvollisuuttaan kyseisen tietojen käsittelyn osalta, minkä vuoksi toimijat on ennakkoratkaisussa katsottu yhteisrekisterinpitäjiksi. Mikäli siis due diligence -tarkastuksessa ostajan katsottaisiin olevan rekisterinpitäjä, olisi todennäköistä, että se toimisi yhteisrekisterinpitäjänä asianajotoimiston kanssa, jotta tietosuoja-asetuksen noudattamisesta ja rekisteröidyn oikeuksista voitaisiin varmistua.

[154] Asia C-40/17, kohdat 64–65.

5.2.2 Rekisteröidyn läpinäkyvä informointi yrityskauppatilanteissa

Tietosuoja-asetus on lisännyt paitsi käsittelyyn liittyviä velvoitteita, myös rekisteröidyn oikeuksia. Vaikka useimmista rekisteröidyn oikeuksista säädettiin jo henkilötietodirektiivissä, tietosuoja-asetus on sekä tarkentanut että laajentanut oikeuksia. Rekisteröidyllä on asetuksen mukaan muun muassa oikeus saada pääsy tietoihinsa, oikaista ja poistaa tietoja, oikeus rajoittaa käsittelyä ja siirtää tiedot järjestelmästä toiseen. Lisäksi sillä on oikeus vastustaa henkilötietojen käsittelyä ja olla joutumatta puhtaasti automaattiseen käsittelyyn perustuvan päätöksen kohteeksi. (15–22 artiklat). Oikeuksien toteutumiseen ja toteuttamiseen liittyy asetuksessa erilaisia edellytyksiä, joita ei kuitenkaan käsitellä tässä tutkielmassa tarkemmin.

Jotta rekisterinpitäjä voi turvata rekisteröidyn oikeuksien toteutumisen, asetuksessa on säädetty myös rekisterinpitäjän velvollisuuksista antaa rekisteröidylle tietoja ja helpottaa rekisteröidyn mahdollisuuksia käyttää oikeuksiaan. Kyseiset velvollisuudet eivät koske henkilötietojen käsittelijää ja rekisteröidyn oikeuksien toteutuminen on siten kokonaisuudessaan rekisterinpitäjän vastuulla.[155] Rekisterinpitäjän on 12 artiklan mukaan toteutettava asianmukaiset toimenpiteet toimittaakseen rekisteröidylle kaikki käsittelyä koskevat tiedot[156] tiiviisti esitettävässä, läpinäkyvässä, helposti ymmärrettävässä ja saatavilla olevassa muodossa. Lisäksi rekisterinpitäjän on artiklan 2 kohdan mukaan helpotettava rekisteröidyn oikeuksien käyttämistä. Kyseinen 12 artikla on ennen kaikkea menettelyä koskeva säädös, jossa hahmotellaan sitä, *miten* tiedot tulee antaa. Se, *mitä* tietoja rekisterinpitäjän on annettava, määräytyy asetuksen 13–22 ja 34 artikloiden perusteella.[157]

Kun rekisterinpitäjä aloittaa käsittelyn, sen on annettava rekisteröidylle käsittelyä koskevat tiedot. Asetuksessa on säädetty kahdesta erilaisesta tilanteesta: tietojen antamisesta silloin, kun tiedot kerätään rekisteröidyltä (13 artikla) ja silloin, kun ne on kerätty muulla tavoin (14 artikla). Due diligence -tarkastuksessa käsiteltävät tiedot antaa tarkastuksen tekijälle lähtökohtaisesti aiotun yrityskaupan myyjäosapuoli ja rekisteröidylle annettaviin tietoihin sovelletaan siten todennäköisesti 14 artiklaa (mikäli ostaja tai sitä edustava asianajotoimisto katsotaan rekisterinpitäjäksi). Toisaalta tilanteessa, jossa tarkastuksen tekijä esimerkiksi haastattelee kohdeyhtiön johtoa tai avainhenkilöitä, sovellettavaksi voi tulla myös 13 artikla.

[155] Ks. kuitenkin luku 5.3 henkilötietojen käsittelystä tehtävästä sopimuksesta.
[156] Käsittelyä koskevilla tiedoilla tarkoitetaan tietosuoja-asetuksen 13–22 artikloissa ja 34 artiklassa säädettyjä tietoja.
[157] *Korpisaari – Pitkänen – Warma-Lehtinen* 2018, s. 174.

Asetuksen mukainen tiedonantovelvollisuus on laaja, ja siinä on säädetty melko yksityiskohtaisesti siitä, mitä tietoja rekisteröidylle on toimitettava. Sekä 13 että 14 artiklassa luetellut tiedot ovat monilta osin samoja tai samantapaisia, kuin mitä rekisterinpitäjän on kirjattava käsittelytoimia koskevaan selosteeseensa. Tiedonantovelvollisuuden toteuttamiseen liittyy kuitenkin due diligence -tarkastuksessa tietynlaisia erityiskysymyksiä, sillä usein jo yrityskauppa-aikeet ja kaupan vireilläolo ovat liikesalaisuuksia, joiden salassapidosta sovitaan osapuolten kesken,[158] eikä tietoja anneta ulkopuolisille tahoille, joihin myös kohdeyhtiön työntekijät yleensä kuuluvat.[159]

Rekisterinpitäjän velvollisuus antaa rekisteröidylle (jonka tietoja käsiteltäisiin oikeutetun edun perusteella) tiedot käsittelystä näyttäytyy siksi ongelmallisena. Rekisterinpitäjän olisi annettava muun muassa tieto käsittelyn tarkoituksesta sekä tieto siitä, mistä henkilötiedot on saatu. On mahdollista ja jopa väistämätöntä, että kyseiset tiedot paljastaisivat rekisteröidylle liikesalaisuutena pidettävän yrityskaupan vireilläolon.[160] Tämän vuoksi due diligence -tarkastusta aloitettaessa olisi tarpeen selvittää, voiko rekisterinpitäjä välttyä tiedonantovelvollisuuden täyttämiseltä.

Kun rekisterinpitäjä on saanut tiedot muualta kuin rekisteröidyltä, sovellettavaksi tulevassa 14 artiklassa on säädetty poikkeuksista, joiden nojalla rekisterinpitäjä voi jättää tiedot antamatta. Yksi poikkeus on tilanne, jossa tiedot on unionin oikeuteen tai jäsenvaltion lainsäädäntöön perustuvan vaitiolovelvollisuuden vuoksi pidettävä luottamuksellisina (TSA 14 artiklan 5 kohdan d alakohta). Poikkeuksen osalta on kuitenkin huomattava, että se koskee ainoastaan *lakisääteistä* vaitiolovelvollisuutta. Yrityskaupassa vaitiolovelvollisuus perustuu lähtökohtaisesti osapuolten tekemään sopimukseen, eikä laissa säädettyyn velvollisuuteen.

Vuonna 2018 voimaan tullut liikesalaisuuslaki (595/2018) on kuitenkin tuonut myös salassapitosopimuksiin uutta sääntelyä, sillä se tulee sovellettavaksi, jos on solmittu liikesalaisuuden käyttämistä tai ilmaisemista rajoittava sopimus.[161] Lisäksi on mahdollista, että yrityskauppa-

[158] *Vapaavuori* 2019, s. 635.
[159] Kuten edellä suostumusta käsittelevässä luvussa 3.2.1 on tuotu esiin, due diligence -tarkastusta tehtäessä kohdeyhtiön työntekijöillä ei yleensä ole tietoa suunnitellusta yrityskaupasta, mikä on myös yksi syy siihen, ettei työntekijöiden tietoja voida käsitellä suostumusperusteella.
[160] Erityisesti julkisten osakeyhtiöiden osalta TSA:n mukainen tiedonantovelvollisuus on ongelmallinen, sillä yrityskauppahanke on usein sisäpiiritietoa. (*Vapaavuori* 2019, s. 635).
[161] *Vapaavuori* 2019, s. 462.

neuvottelut muodostavat sellaisen luottamuksellisen liikesuhteen, jonka perusteella tiedon vastaanottajalle – eli ostajalle ja/tai asianajotoimistolle – muodostuu automaattisesti liikesalaisuuksia koskeva käyttö- ja ilmaisukielto (LSL 4 § 2 mom. 3 k.).[162] Tällöin olisi mahdollista, että myös tietosuoja-asetuksen 14 artiklan poikkeus tulisi sovellettavaksi, eikä rekisterinpitäjällä olisi velvollisuutta antaa rekisteröidylle tietoa käsittelystä.

Lakisääteisen vaitiolovelvollisuuden lisäksi tietosuoja-asetuksen johdannossa on todettu, ettei rekisteröidyn oikeus saada pääsy tietoihinsa saisi vaikuttaa epäedullisesti muiden oikeuksiin ja vapauksiin, kuten liikesalaisuuksiin. Tämä ei kuitenkaan saisi johtaa siihen, ettei rekisteröidylle anneta tietoja ollenkaan.[163] Toisaalta taas liikesalaisuusdirektiivin[164] johdannossa on todettu, ettei direktiivi saisi vaikuttaa henkilötietodirektiivissä (joka oli voimassa liikesalaisuusdirektiivistä säädettäessä) säädettyihin oikeuksiin ja velvollisuuksiin, etenkään tiettyihin rekisteröidyn oikeuksiin, kuten oikeuteen saada pääsy tietoihinsa. Tietosuoja-asetuksen ja liikesalaisuusdirektiivin välistä suhdetta henkilötietojen käsittelyn osalta olisi siten punnittava tarkemmin, mikäli rekisterinpitäjälle ei tarkastuksessa ja yrityskauppahankkeessa muodostuisi LSL:n mukaista ilmaisu- ja käyttökieltoa. Mikäli kiellon edellytykset eivät tarkastuksessa täyttyisi ja työntekijöiden tietoja haluttaisiin käsitellä ilmoittamatta siitä työntekijöille, olisi tiedot nähdäkseni anonymisoitava, jotta tietosuoja-asetusta ei sovellettaisi.

Liikesalaisuuden ja informointivelvollisuuden välinen suhde on nähtävissä jokseenkin monimutkaisena etenkin kun otetaan huomioon säädösten johdanto-osien ristiriitaiset ilmaisut. Koska informointivelvollisuus ja rekisteröidyn oikeuksista huolehtiminen ovat keskeisiä rekisterinpitäjälle kuuluvia velvoitteita, näkökulma on tarpeellista tuoda esiin, vaikka sitä ei tarkemmin käsitellä tässä tutkielmassa. Pidän näet erittäin epätodennäköisenä, että rekisterinpitäjä – olipa se ostaja tai asianajotoimisto – ilmoittaisi käsittelystä työntekijöille tarkastuksen aikana. Jos sillä ei ole oikeusperustetta jättää tietoja antamatta, se ei voi käsitellä työntekijän tietoja siinä muodossa, että työntekijät olisivat tunnistettavissa.

[162] *Vapaavuori* 2019, s. 636.
[163] Tietosuoja-asetuksen johdanto, kohta 63.
[164] Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/943 julkistamattoman taitotiedon ja liiketoimintatiedon (liikesalaisuuksien) suojaamisesta laittomalta hankinnalta, käytöltä ja ilmaisemiselta.

5.3 Sopimus henkilötietojen käsittelystä

Jos henkilötietoja käsitellään rekisterinpitäjän lukuun, on rekisterinpitäjän ja henkilötietojen käsittelijän välillä oltava sopimus tai muu oikeudellisesti sitova, kirjallinen asiakirja. Sopimuksessa on vahvistettava käsittelyn kohde ja kesto, luonne ja tarkoitus, henkilötietojen tyyppi ja rekisteröityjen ryhmät sekä rekisterinpitäjän velvollisuudet ja oikeudet. (TSA 28 artiklan 3 kohta). Rekisterinpitäjän ja henkilötietojen käsittelijän välisestä sopimuksesta säädettiin jo henkilötietodirektiivissä, mutta huomattavasti asetusta suppeammin. Direktiivissä sopimuksen tuli erityisesti sisältää sitoumus noudattaa rekisterinpitäjän ohjeita ja toteuttaa tekniset ja organisatoriset toimenpiteet jäsenvaltion lainsäädännön mukaisesti. Asetuksessa on edellä lueteltujen seikkojen lisäksi säädetty myös useista henkilötietojen käsittelijän vastuista, jotka sopimukseen on erityisesti sisällytettävä.

Ensinnäkin sopimuksessa on säädettävä siitä, että tietoja käsitellään ainoastaan rekisterinpitäjän antamien, dokumentoitujen ohjeiden mukaisesti, jollei lainsäädäntö velvoita käsittelemään tietoja ilman ohjeistusta (TSA 28 artiklan 3 kohdan a alakohta). Rekisterinpitäjän on siis annettava ohjeistus ja henkilötietojen käsittelijän on noudatettava sitä. Mikäli jompikumpi (tai molemmat) osapuolista ei noudata velvoitetta, henkilötietojen käsittelijästä voi tulla (yhteis)rekisterinpitäjä.[165] Jos asianajotoimisto katsottaisiin due diligence -tarkastuksessa henkilötietojen käsittelijäksi, saisi se siis käsitellä tietoja ainoastaan ostajan antamien ohjeiden mukaisesti. Kun otetaan huomioon, että asianajotoimisto on saanut toimeksiannon yrityskaupan hoitamiseen ja tarkastukseen asiantuntemuksensa vuoksi, on epätodennäköistä, että se tosiasiassa noudattaisi tarkastuksessa ostajan antamia, tarkkoja ohjeita edes siltä osin, kuin kyse on henkilötietojen käsittelystä.

Sopimuksessa on lisäksi säädettävä siitä, että henkilötietojen käsittelijä auttaa mahdollisuuksien mukaan rekisterinpitäjää täyttämään III luvun mukaiset velvollisuudet vastata rekisteröidyn oikeuksien käyttämistä koskeviin pyyntöihin. Auttamisen tulisi tapahtua teknisin ja organisatorisin toimenpitein (28 artiklan 3 kohdan e alakohta). Kyseisen luvun mukaiset rekisteröidyn oikeudet on lueteltu edellä alaluvussa 5.2.2, jossa on lisäksi todettu, että luku asettaa velvollisuuksia ainoastaan rekisterinpitäjälle. Sen vuoksi henkilötietojen käsittelijällä – jolla voi olla jopa rekisterinpitäjää paremmat mahdollisuudet vastata rekisteröidyn pyyntöihin – on oltava

[165] *Treacy* 2012, s. 2. Lisäksi TSA 28 artiklan 10 kohta, jonka mukaan henkilötietojen käsittelijän määritellessä käsittelyn tarkoitukset ja keinot, sitä on pidettävä rekisterinpitäjänä.

velvollisuus avustaa rekisterinpitäjää. Joissakin tapauksissa henkilötietojen käsittelijä voi jopa tosiasiallisesti olla se taho, joka vastaa rekisteröidyn pääsystä tietoihin.[166] Näin olisi todennäköisesti myös due diligence -tarkastuksessa, jos ostaja toimisi rekisterinpitäjänä. Todennäköisesti ostajalla ei olisi tosiasiallista mahdollisuutta vastata rekisteröityjen tietopyyntöihin ainakaan ilman asianajotoimiston apua.

Koska asianajotoimistolla on pääsy kaikkiin tarkastuksessa käsiteltäviin henkilötietoihin eikä ostajalla välttämättä ole pääsyä tietoihin tai se ei ainakaan käsittele kaikkia tietoja, olisi asianajotoimiston toimiessa henkilötietojen käsittelijänä myös tärkeää määritellä, mitä henkilötiedoille tehdään tarkastuksen jälkeen. Sopimuksessa onkin säädettävä myös siitä, tuleeko henkilötietojen käsittelijän poistaa vai palauttaa henkilötiedot rekisterinpitäjälle palveluiden tarjoamisen päätettyä. Lisäksi jäljennökset olisi poistettava, jollei niiden säilyttämiselle ole lainmukaista perustetta (28 artiklan 3 kohdan g alakohta). Kuten aiemmin on tuotu esiin, asianajotoimistolla voi vastuukysymysten takia olla velvollisuus tai ainakin tarve säilyttää tietoja pidempään, kuin ainoastaan käsittelyn ajan. Säilyttämiselle ei kuitenkaan nähdäkseni ole suoraan laista tulevaa velvoitetta, minkä vuoksi tietojen poistamisvelvoite näyttäytyy ongelmallisena. Luonnollisesti tietojen palauttaminen ei tarkastuksessa tule kysymykseen, kun tietoja ei ole saatu ostajalta.

Henkilötietojen käsittelijän on myös varmistettava, että tietoja käsittelevät henkilöt ovat sitoutuneet noudattamaan salassapitovelvollisuutta tai että heitä sitoo lakisääteinen salassapitovelvollisuus (TSA 28 artiklan 3 kohdan b alakohta). Useimmiten – kuten myös due diligence -tarkastuksessa – nämä henkilöt ovat henkilötietojen käsittelijänä toimivan yrityksen työntekijöitä. Lisäksi tulee sopia siitä, että henkilötietojen käsittelijä noudattaa toisen henkilötietojen käsittelijän käytön edellytyksiä, joista on säädetty saman artiklan 2 ja 4 kohdissa (TSA 28 artiklan 3 kohdan d alakohta). Luonnollisesti vaatimus koskee vain niitä tilanteita, joissa henkilötietojen käsittelijä käyttää toista käsittelijää. Asianajotoimiston ja ostajan välisessä suhteessa kyseinen vaatimus ei liene relevantti, sillä jos asianajotoimisto on henkilötietojen käsittelijä, se ei todennäköisesti käytä toista käsittelijää tarkastuksen tekemiseen.

Henkilötietojen käsittelijällä on asetuksen mukaan myös velvollisuus huolehtia käsittelyn turvallisuudesta ja auttaa rekisterinpitäjää varmistamaan, että turvallisuutta ja tietoturvaloukkauksia koskevia velvoitteita noudatetaan (28 artiklan 3 kohdan c ja f alakohdat). Turvallisuutta ja

[166] Ks. esim. *Blume* 2013, s. 142.

velvoitteiden jakautumista henkilötietojen käsittelijän ja rekisterinpitäjän välillä käsitellään tarkemmin seuraavassa alaluvussa. Viimeisenä kohtana (h alakohta) sopimuksessa on säädettävä henkilötietojen käsittelijän velvoitteesta antaa rekisterinpitäjälle kaikki ne tiedot, jotka ovat tarpeen sen osoittamiseksi, että kyseisen artiklan mukaisia velvollisuuksia noudatetaan. Rekisterinpitäjälle on lisäksi annettava mahdollisuus suorittaa auditointeja ja henkilötietojen käsittelijän on osallistuttava niihin.

Vaikka henkilötietojen käsittelijää koskevassa artikla on kirjoitettu muotoon, jossa korostuu erityisesti käsittelystä tehtävän sopimuksen sisältö, on artiklan tosiasiallinen merkitys myös siinä, että se nimeää henkilötietojen käsittelijän vastuualueet ainakin tärkeimmiltä osin. Useiden vastuualueiden sisältö on kuitenkin määritelty tarkemmin muissa, kuten käsittelyn turvallisuutta koskevissa artikloissa. Se, että sopimus on tehtävä kirjallisesti, auttaa myös rekisterinpitäjän osoitusvelvollisuuden toteuttamista. Erityisesti viimeinen, h alakohta on osoitusvelvollisuuden kannalta tärkeä, sillä kun viimesijainen vastuu asetuksen noudattamisen osoittamisesta on rekisterinpitäjällä, tulee sillä olla laajat mahdollisuudet valvoa henkilötietojen käsittelijää.

Henkilötietojen käsittelijän johtaminen ja hallinnointi on kuitenkin käytännössä vaativaa ja usein voidaankin kyseenalaistaa, toteutuuko se käytännössä tyydyttävällä ja asetuksen vaatimalla tavalla.[167] Jos asianajotoimistoa pidettäisiin tarkastuksessa henkilötietojen käsittelijänä suhteessa ostajaan, olisi todennäköistä, että ostajan mahdollisuudet tosiasiassa hallinnoida henkilötietojen käsittelijää ja asianajotoimistoa sen liiketoimintaan kuuluvassa käsittelyssä olisivat heikot.

5.4 Seloste käsittelytoimista ja muut dokumentointivelvoitteet

Rekisterinpitäjä vastaa siis siitä, että tietosuoja-asetusta noudatetaan ja siitä, että se voi osoittaa asetusta noudatetun. Jotta osoitusvelvollisuus voidaan täyttää, on rekisterinpitäjän pidettävä käsittelystä kirjaa. Se, mitä rekisterinpitäjän on dokumentoitava, määräytyy osin suoraan tietosuoja-asetuksen säännösten perusteella, minkä lisäksi rekisterinpitäjän on suositeltavaa kirjata tietoja myös sellaisista käsittelyyn liittyvistä toimista, joita asetus ei nimenomaisesti edellytä.

Yksi asetuksen mukainen dokumentointivelvollisuus on käsittelytoimia kuvaavan selosteen ylläpitäminen. Vaikka henkilötietojen käsittelijällä ei ole osoitusvelvollisuutta, velvollisuus pitää

[167] *Blume* 2013, s. 142.

yllä kyseistä selostetta koskee myös käsittelijää. Rekisterinpitäjän tai tarvittaessa sen edustajan[168] on pidettävä yllä selostetta sen vastuulla olevista käsittelytoimista (TSA 30 artiklan 1 kohta) ja henkilötietojen käsittelijän tai sen edustajan puolestaan niistä toimista, joita se suorittaa rekisterinpitäjän lukuun (2 kohta). Dokumentointivelvoite on asetuksessa uusi ja se koskee yritystä, jolla on vähintään 250 työntekijää. Lisäksi selostetta on työntekijöiden lukumäärästä riippumatta ylläpidettävä, jos käsittely ei ole satunnaista, se kohdistuu arkaluontoisiin tietoihin[169] tai aiheuttaa riskin rekisteröidyn oikeuksille ja vapauksille. (TSA 30 artiklan 5 kohta). Koska työntekijöiden lukumäärä on yksiselitteisesti laskettavissa, velvollisuutta ylläpitää selostetta arvioidaan due diligence -tarkastuksessa ennen kaikkea käsittelyn satunnaisuuden ja riskien näkökulmasta silloin, kun työntekijöitä on alle 250. Arkaluontoisia tietoja tarkastuksessa ei käsitellä.

Rekisteröidyn oikeuksille ja vapauksille aiheutuvan riskin arviointi on jälleen arvioinnin kohteena. Selostetta koskeva artikla tai asetuksen johdanto eivät kuitenkaan määrittele, millaisia riskejä artiklassa tarkoitetaan. Riskejä lienee siten syytä arvioida samoin kuin esimerkiksi tarvittavien teknisten ja organisatoristen toimenpiteiden osalta yllä luvussa 5.2.1. Käsittelystä voi siten aiheutua riskejä tarkastuksessa esimerkiksi tietoturvaloukkauksen yhteydessä, mutta samankaltaiset riskit liittyvät valtaosaan käsittelyprosesseista riippumatta siitä, mitä tarkoitusta varten henkilötietoja käsitellään. Oikeuksien ja vapauksien loukkaamisen riski ei siten välttämättä yksin laukaisisi velvollisuutta ylläpitää selostetta tarkastuksesta, toimipa rekisterinpitäjänä asianajotoimisto tai ostaja.

Käsittelyn satunnaisuuden osalta asianajotoimiston ja ostajan välillä voidaan nähdäkseni tehdä selvä ero: mikäli yrityskaupat ja sen myötä due diligence -tarkastukset eivät kuulu ostajan tavanomaiseen liiketoimintaan, on tarkastuksessa suoritettava henkilötietojen käsittely sille satunnaista. Näin ollen ostajan, jolla on alle 250 työntekijää, ei ainakaan ”ei-satunnaisuuden” perusteella olisi välttämätöntä ylläpitää selostetta due diligence -tarkastuksesta. Asianajotoimiston osalta voidaan kääntyä vastakkaiseen tulkintaan: tarkastus kuuluu sen tavanomaiseen liiketoimintaan, joten vaikka kyseessä olisi alle 250 työntekijän yritys, sen olisi ylläpidettävä selostetta, koska käsittely ei ole satunnaista.

[168] Edustajalla tarkoitetaan unionin ulkopuolelle sijoittautuneen rekisterinpitäjän kirjallisesti nimeämää, unioniin sijoittautunutta luonnollista henkilöä tai oikeushenkilöä.
[169] Tietosuoja-asetuksen 9 artiklan 1 kohdassa ja 10 artiklassa tarkoitetut tiedot.

Rekisterinpitäjän ylläpitämän selosteen tulee pitää sisällään rekisterinpitäjän tai -pitäjien, niiden edustajien ja tietosuojavastaavan[170] tiedot, käsittelyn tarkoitukset, kuvaus henkilötietoryhmistä ja rekisteröityjen ryhmistä, henkilötietojen mahdollisista vastaanottajista sekä *mahdollisuuksien mukaan* tieto tietojen poistamisen määräajoista ja kuvaus teknisistä ja organisatorisista toimenpiteistä. Lisäksi selosteessa on oltava tiedot henkilötietojen siirtämisestä kolmansiin maihin tai kansainvälisiin järjestöihin. Henkilötietojen käsittelijän seloste on puolestaan hieman suppeampi, eikä siinä selosteta esimerkiksi tietojen poistamiseen tai luovuttamiseen liittyviä seikkoja.

Etenkin rekisterinpitäjän selosteessa on siten tuotu esiin laajasti käsittelyyn liittyviä seikkoja ja se osaltaan toteuttaa myös osoitusvelvollisuutta. Selosteen osalta on lisäksi hyvä huomata, että se on yrityksen sisäinen asiakirja, joka on pyydettäessä esitettävä valvontaviranomaiselle. Se eroaa siten henkilötietodirektiivin mukaisesta tietosuojaselosteesta, joka toimi ennen kaikkea rekisteröidyn informoinnin välineenä. Tietosuojaseloste voi tosin olla myös asetuksen tiedonantovelvollisuuden täyttämiseksi hyödyllinen ja yritys voi tehdä selosteen, vaikkei sitä asetuksessa vaadita.

Osoitusvelvollisuuden täyttäminen edellyttää, että rekisterinpitäjä voi osoittaa käsittelyn olevan asetuksen mukaista kokonaisuudessaan, joten pelkkä 32 artiklan mukainen seloste käsittelytoimista ei yksin kata koko osoitusvelvollisuutta. Rekisterinpitäjälle asetettuja erilaisia dokumentointivelvollisuuksia on tietosuoja-asetuksessa useita. Rekisterinpitäjän on esimerkiksi pystyttävä osoittamaan, että se on saanut rekisteröidyltä suostumuksen henkilötietojen käsittelyyn (TSA 7 artiklan 1 kohta) ja sen on dokumentoitava kaikki tietoturvaloukkaukset, niiden vaikutukset ja korjaavat toimet (33 artiklan 5 kohta). Molemmat velvoitteet koskevat rekisterinpitäjää myös due diligence -tarkastuksessa, jossa osa tiedoista on voitu kerätä suostumusperusteella ja tietoturvaloukkausten osalta velvollisuus ei ole riippuvainen käsittelyn luonteesta, vaan kuuluu kaikille rekisterinpitäjille. Lisäksi rekisterinpitäjän on ennen tietyntyyppisen käsittelyn suunniteltua aloittamista tehtävä tietosuojaa koskeva vaikutustenarviointi (35 artikla). Arviointi on osa sekä dokumentointivelvoitetta että käsittelyn turvallisuuden varmistamista, mutta sitä ei tässä tutkielmassa käsitellä tarkemmin, sillä due diligence -tarkastuksessa ei ole kysymys artiklan mukaisista käsittelytoimista.

[170] Tietosuoja-asetuksen 4 jaksossa säädetään tietosuojavastaavan nimittämisestä, asemasta ja tehtävistä. Tässä tutkielmassa velvollisuutta nimetä tietosuojavastaava ei ole käsitelty, sillä nimeämisvelvoitteet ovat rekisterinpitäjälle ja henkilötietojen käsittelijälle samat, eivätkä nimeämisen edellytykset siten riipu siitä, käsitteleekö asianajotoimisto henkilötietoja due diligence -tarkastuksessa rekisterinpitäjänä vai henkilötietojen käsittelijänä.

Asetuksen mukaisten dokumentointivelvollisuuksien lisäksi rekisterinpitäjän on suositeltavaa dokumentoida kaikki ne keinot ja toimenpiteet, joilla se on pyrkinyt varmistamaan henkilötietojen turvallisen käsittelyn niiden keräämisestä niiden käsittelyyn ja tuhoamiseen saakka. Dokumentointiin tulisi sisällyttää muun muassa riskiarvioita, rekisteriselosteita, työntekijöille annettu koulutus henkilötietojen käsittelyyn liittyen ja kaikki sellainen tietosuoja-asetuksen noudattamiseen liittyvä materiaali, joka tukee käsittelyn lainmukaisuuden osoittamista tilanteessa, jossa rekisterinpitäjän on osoitusvelvollisuutensa mukaisesti esitettävä käsittelyyn liittyvät tiedot valvovalle viranomaiselle.[171]

Jos asianajotoimisto katsottaisiin henkilötietojen käsittelijäksi, tulisi sekä ostajan että asianajotoimiston laatia seloste käsittelytoimista. Muut dokumentointivelvoitteet olisivat kuitenkin tällöin ostajan vastuulla, vaikka lähtökohtaisesti asianajotoimistolla lienee paremmat edellytykset dokumentoida esimerkiksi mahdolliset tietoturvaloukkaukset ja suostumus henkilötietojen käsittelyyn.

5.5 Käsittelyn turvallisuus

Tietosuoja-asetuksen artikloista suuri osa on keskittynyt säätämään käsittelyn turvallisuuden varmistamisesta rekisteröidyn oikeuksien lisäksi. Rekisterinpitäjä on osoitusvelvollisuutensa nojalla vastuussa sen toteen näyttämisestä, että asetuksen mukaiset turvallisuusvaatimukset on täytetty. Kuten edellä luvussa 5.2.1 on tuotu esiin, velvollisuuteen kuuluu myös 24 artiklan mukainen velvollisuus toteuttaa tarvittavat tekniset ja organisatoriset toimenpiteet, joilla asetuksen noudattaminen voidaan sekä osoittaa että varmistaa. Tekniset ja organisatoriset toimenpiteet ovat keskiössä myös muissa asetuksen turvallisuutta koskevissa säädöksissä ja niiden toteuttaminen kuuluu sekä rekisterinpitäjälle että henkilötietojen käsittelijälle. Vastuunjako toimijoiden välillä ei kuitenkaan ilmene suoraan asetuksesta.

Jotta rekisterinpitäjä voi täyttää osoitusvelvollisuutensa, on tärkeää, että se varmistuu myös käyttämänsä henkilötietojen käsittelijän riittävistä valmiuksista noudattaa asetusta. Rekisterinpitäjällä onkin tietosuoja-asetuksessa nimenomainen velvollisuus varmistua henkilötietojen käsittelijän valmiuksista, sillä se saa 28 artiklan 1 kohdan mukaan käyttää vain sellaista henkilötietojen käsittelijää, joka toteuttaa riittävät suojatoimet asianmukaisten teknisten ja organisatoristen toimien täytäntöön panemiseksi niin, että käsittely täyttää asetuksen vaatimukset ja sillä

[171] Ks. mm. *Calder* 2016, s. 69 ja *IT Governance* 2019, s. 34–35.

varmistetaan rekisteröidyn oikeuksien suojelu. Säädöksen sanamuoto on sinänsä erikoinen, ettei se suoraan näyttäisi asettavan henkilötietojen käsittelijälle vastuuta itse teknisistä ja organisatorisista toimista, vaan ainoastaan *riittävistä suojatoimista.*

EU-sääntelyn, ja siten myös tietosuoja-asetuksen, erityispiirre on se, että jokainen unionin virallinen kieli on yhtä todistusvoimainen. Sen vuoksi säädösten tulkinnassa ei ole riittävää nojautua ainoastaan sanamuodon mukaiseen tulkintaan, mikäli eri kieliversioissa on eroja.[172] Suomenkielisestä versiosta ”riittävät suojatoimet” on englanninkielisessä versiossa käytetty sanamuotoa ”*sufficient guarantees”* ja ruotsinkielinen käännös käyttää samankaltaista ilmaisua ”*tillräckliga garantier*”. Kyseisten kieliversioiden perusteella näyttäisikin siltä, että henkilötietojen käsittelijän tulisi antaa rekisterinpitäjälle *riittävät takeet* siitä, että tekniset ja organisatoriset toimenpiteet toteutetaan. Tulkintaa tukee ensinnäkin se, että ennen sopimuksen tekemistä ja käsittelytoimia rekisterinpitäjä ei ainakaan helposti voi varmistua käsittelijän teknisistä ja organisatorisista toimista, mutta se voi vaatia käsittelijältä takeita niistä. Toiseksi, muualla asetuksessa on asetettu vastuu teknisistä ja organisatorisista toimenpiteistä myös henkilötietojen käsittelijälle eikä ”riittäviä suojatoimia” ole määritelty asetuksessa – sen vuoksi suomenkielisen version mukainen tulkinta jättää avoimeksi sen, mistä rekisterinpitäjän tulisi oikeastaan varmistua ennen sopimuksen tekoa.

Henkilötietojen käsittelyn turvallisuudesta on säädetty asetuksen 32 artiklassa, joka sanamuotonsa perusteella asettaa identtisen vastuun rekisterinpitäjälle ja henkilötietojen käsittelijälle. Artiklan mukaan rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava asianmukaiset tekniset ja organisatoriset toimenpiteet, joista artiklassa on myös annettu esimerkkejä. Se, miten *asianmukaiset* toimenpiteet määritellään, perustuu riskiarvioon: toimenpiteet on suhteutettava rekisteröidyn oikeuksille ja vapauksille aiheutuviin riskeihin.[173] Lisäksi käsittelyn turvallisuutta koskien on luotu erilaisia kansallisia ja kansainvälisiä standardeja, joita voidaan käyttää apuna toimenpiteiden määrittelyssä ja toteuttamisessa.[174]

[172] *Talus – Penttinen* 2015, s. 238.
[173] Ks. WP 218. Riskiperusteisuutta ei kuitenkaan tule nähdä vaihtoehtona täysimääräiselle tietosuojaperiaatteiden ja sääntöjen noudattamiselle.
[174] Ks. Handbook on European data protection law, s. 165–166. Erilaisia tietosuojastandardeja on EU:ssa useita.

Artiklan soveltuminen suoraan sekä henkilötietojen käsittelijään että rekisterinpitäjään on todettu yksiselitteisesti myös oikeuskirjallisuudessa.[175] Se, että henkilötietojen käsittelijä toteuttaa kaikki 32 artiklan mukaiset toimenpiteet, on todettava myös käsittelyä koskevassa sopimuksessa. Kyseisessä sopimuksessa on lisäksi säädettävä siitä, että käsittelijä *auttaa* rekisterinpitäjää varmistamaan, että 32–36 artiklan vaatimukset ja velvoitteet täytetään (28 artiklan 3 kohdan f alakohta). Käsittelijän on siis yhtäältä toteutettava toimenpiteet ja toisaalta autettava rekisterinpitäjää varmistamaan turvallisuutta koskevien artiklojen noudattaminen. Sinänsä 28 artiklan alakohtien välillä voidaan nähdä jopa ristiriita, mutta toisaalta f alakohtaa voidaan lukea siten, että henkilötietojen käsittelijällä on velvollisuus avustaa rekisterinpitäjää osoitusvelvollisuuden täyttämisessä niiltä osin, kuin kyseiset artiklat eivät suoraan velvoita käsittelijää.

Edellä käsiteltyjen säännösten lisäksi tekniset ja organisatoriset toimenpiteet asettavat velvollisuuksia rekisterinpitäjälle myös 25 artiklassa, jossa säädetään sisäänrakennetusta ja oletusarvoisesta tietosuojasta (*privacy by design and default),* joista rekisterinpitäjän on huolehdittava teknisin ja organisatorisin keinoin. Sisäänrakennetulla tietosuojalla tarkoitetaan asetuksessa sitä, että tietosuojaperiaatteet sisällytetään käsittelyn osaksi käsittelytapojen määrittämisen ja käsittelyn yhteydessä (25 artiklan 1 kohta). Yleisemmin ajatuksena on, että tietoturva tulisi huomioida alusta alkaen järjestelmiä suunniteltaessa.[176] Oletusarvoinen tietosuoja taas tarkoittaa, ettei henkilötietoja oletusarvoisesti saateta rajoittamattoman henkilömäärän saataville ilman luonnollisen henkilön myötävaikutusta ja, että käsitellään vain tarkoitusta varten tarpeellisia tietoja (25 artiklan 2 kohta). Nämä velvollisuudet ovat siis rekisterinpitäjälle asetettuja, eikä henkilötietojen käsittelijällä ole asetuksen mukaan vastuuta toteuttamisesta.

Se, miten ja missä laajuudessa rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava teknisiä ja organisatorisia toimenpiteitä, on edellä esitetyn perusteella jossain määrin epäselvää. Henkilötietojen käsittelijän vastuu on mainittu ainoastaan 32 artiklassa, mutta toisaalta esimerkiksi oletusarvoinen ja sisäänrakennettu tietosuoja liittyvät kiinteästi käsittelyn turvallisuuteen ja artiklat on nähtävissä osin myös päällekkäisinä. Lisäksi, kun (yhteis)rekisterinpitäjällä ei tarvitse olla pääsyä käsiteltäviin tietoihin ja henkilötietojen käsittelijä voi osallistua teknisten keinojen määrittelyyn, olisi loogista, että henkilötietojen käsittelijä voisi tapauskohtaisesti vastata myös sisäänrakennetusta ja oletusarvoisesta tietosuojasta.

[175] *Hintze* 2018, s. 24.
[176] *Veale – Binns – Ausloos* 2018, s. 105.

Rekisterinpitäjän vastuu toimenpiteistä näyttää siten jokseenkin laajemmalle kuin henkilötietojen käsittelijän. Lisäksi on huomioitava, että rekisterinpitäjälle kuuluu myös muita turvallisuuteen liittyviä vastuualueita, joiden osalta henkilötietojen käsittelijän rooli on ainoastaan auttaa reksiterinpitäjää. Esimerkiksi tietosuojaa koskeva vaikutustenarviointi ja siihen eräissä tapauksissa liittyvä ennakkokuuleminen ovat rekisterinpitäjän vastuulla, samoin kuin tietoturvaloukkauksesta ilmoittaminen niin rekisteröidylle kuin valvontaviranomaiselle (henkilötietojen käsittelijä on kuitenkin loukkauksen havaitessaan velvollinen ilmoittamaan rekisterinpitäjälle loukkauksesta). Onkin esitetty, että etenkin tietoturvaloukkauksia koskevat velvollisuudet olisi ollut perusteltua ohjata asetuksessa myös henkilötietojen käsittelijän vastuulle.[177]

Due diligence -tarkastuksessa turvallisuusvelvoitteita koskeva vastuunjako näyttäytyy merkityksellisenä. Mikäli asianajotoimisto katsottaisiin henkilötietojen käsittelijäksi eikä sen vastuu siten ulottuisi esimerkiksi tietoturvaloukkauksista ilmoittamiseen (muutoin kuin rekisterinpitäjää avustavassa roolissa), olisi kiinnitettävä huomiota siihen, pystyisikö rekisterinpitäjä huolehtimaan kyseisistä velvoitteista. Myös sisäänrakennetun ja oletusarvoisen tietosuojan edellyttämät toimenpiteet olisivat todennäköisesti vaikeita toteuttaa muun kuin tarkastusta tekevän asianajotoimiston (ja datahuonetta tarjoavan pilvipalvelun) toimesta.

5.6 Yhteisrekisterinpitäjien vastuunjako

Edellä luvussa 4.2 on käsitelty yhteisrekisterinpitäjän määritelmää. Yhteisrekisterinpitäjyys on tunnistettu jo henkilötietodirektiivissä, mutta tietosuoja-asetuksessa säädetään ensimmäistä kertaa käsitteestä ja yhteisrekisterinpitäjien välisestä vastuunjaosta. Sinänsä yhteisrekisterinpitäjien vastuut ovat sisällöllisesti samoja kuin jos rekisterinpitäjiä olisi vain yksi. Yhteisrekisterinpitäjien (jotka siis määrittelevät ainakin osittain yhdessä käsittelyn tarkoitukset ja keinot) välillä vastuu asetuksen mukaisten velvoitteiden täyttämisestä voi kuitenkin jakautua eri tavoin. Vastuunjaon kannalta onkin tärkeää erottaa tilanteet, joissa kysymys on kahdesta eri rekisterinpitäjästä yhteisrekisterinpitäjien sijaan.

Tietosuoja-asetuksen mukaan yhteisrekisterinpitäjät määrittelevät keskinäisellä järjestelyllä vastuualueet tietosuoja-asetuksessa vahvistettujen velvoitteiden noudattamiseksi silloin, kun vastuualueita ei ole määritelty unionin tai jäsenvaltion lainsäädännössä (TSA 26 artiklan 1 kohta). Järjestelyitä koskeva määrittely voi olla vapaamuotoinen kuvaus velvoitteista, eikä sen

[177] *Blume* 2013, s. 144.

tarvitse esimerkiksi sisältyä osapuolten väliseen sopimukseen.[178] Määrittelyn tulee kuitenkin asetuksen mukaan olla läpinäkyvää. Läpinäkyvä tapa voi olla esimerkiksi vastuualueiden määrittely tietosuojaselosteissa.[179]

Asetuksen 26 artiklan 2 kohdan mukaan yhteisrekisterinpitäjien keskinäisestä järjestelystä on käytävä ilmi osapuolten todelliset roolit ja suhteet rekisteröityihin nähden. Lisäksi järjestelyn keskeisten osien on oltava rekisteröidyn saatavilla. Saatavuus voidaankin mahdollistaa esimerkiksi juuri ottamalla järjestely osaksi tietosuojaselostetta, jolloin keskeiset tiedot voidaan myös helposti luovuttaa rekisteröidylle. Sitä, mitä osapuolten todellisilla rooleilla tarkoitetaan, ei ole avattu asetuksessa tarkemmin, mutta järjestelyn määrittelystä lienee syytä käydä ilmi esimerkiksi se, miltä osin kumpikin rekisterinpitäjistä käsittelee tietoja (tai onko toisen rekisterinpitäjän rooli esimerkiksi vain ohjata käsittelyä tai hyötyä tietojen käsittelystä, jota toinen rekisterinpitäjä suorittaa).

Mikäli asianajotoimisto ja ostaja toimisivat due diligence -tarkastuksessa yhteisrekisterinpitäjinä, järjestelyitä koskeva määrittely olisi todennäköisesti otettu osaksi toimeksiantosopimusta. Jos yhteisrekisterinpitäjyys olisi vakituinen käytäntö tarkastuksissa, asianajotoimistolla olisi todennäköisesti valmis malli määrittelyn tekemiseksi. Järjestelyn läpinäkyvyyden osalta esiin nousee kuitenkin sama kysymys, kuin rekisterinpitäjän tiedonantovelvollisuuksien osalta: voidaanko järjestelyä saattaa rekisteröidyn saataville edes keskeisiltä osin ilman, että paljastetaan yrityskaupan vireilläolo? Nähdäkseni myös järjestelyitä koskevan määrittelyn osalta pätevät samat, luvussa 5.2.3 käsitellyt periaatteet: mikäli tarkastuksessa ei ole kysymys lakisääteisestä vaitiolovelvollisuudesta eikä tietoja haluta antaa, työntekijöiden henkilötietoja ei voida käsitellä. Sinänsä tämä ei kuitenkaan vaikuta velvollisuuteen toteuttaa järjestely läpinäkyvällä tavalla, sillä myös esimerkiksi kohdeyhtiön johtoon kuuluvilla henkilöillä on rekisteröityinä oikeus saada tieto järjestelystä.

Tietosuoja-asetuksesta ei käy tarkemmin ilmi se, miten vastuualueet tulisi määrittää ja voidaanko vastuu jakaa yhteisrekisterinpitäjien välillä ns. mielivaltaisesti esimerkiksi siten, että vastuu määritellään keskinäisellä järjestelyllä vain toiselle yhteisrekisterinpitäjälle. Asetuksen johdannossa on todettu ainoastaan, että vastuualueet tulee jakaa selkeästi.[180] CJEU on ratkaisu-

[178] *Korpisaari – Pitkänen – Warma-Lehtinen* 2018, s. 284.
[179] *Hanninen – Laine – Rantala – Rusi – Varhela* 2017, s. 28.
[180] Tietosuoja-asetuksen johdanto, kohta 79.

käytännössään todennut, ettei yhteisrekisterinpitäjien välinen vastuu välttämättä tarkoita rekisterinpitäjien samanlaista vastuuta, vaan vastuu riippuu muun muassa käsittelyn asteesta ja vaiheista.[181] Lisäksi EU:n julkisasiamies on ratkaisuehdotuksessaan esittänyt, että vastuun tulisi määrittyä sen mukaan, minkä toimintojen osalta (yhteis)rekisterinpitäjä on määritellyt (yhdessä tai itse) käsittelytoimen tarkoituksen ja keinot.[182] Tämä tarkoittaa siis sitä, että mikäli toinen yhteisrekisterinpitäjistä suorittaisi sellaisia käsittelytoimia, joiden tarkoitukset ja keinot se on määritellyt yksin, toimii se myös rekisterinpitäjänä tällaisten toimien osalta itsenäisesti eikä vastuu kuulu molemmille yhteisrekisterinpitäjille. Vastuunjakoon voi lisäksi vaikuttaa esimerkiksi se, mitä henkilötietoja käsitellään[183] ja onko rekisterinpitäjällä pääsy käsiteltäviin tietoihin[184]. Vaikka CJEU on ratkaisukäytännössä katsonut, ettei yhteisrekisterinpitäjällä tarvitse olla pääsyä tietoihin, pääsy voi vaikuttaa vastuun jakautumiseen yhteisrekisterinpitäjien välillä.

Mikäli ostaja ja asianajotoimisto katsottaisiin due diligence -tarkastuksessa yhteisrekisterinpitäjiksi, vastuu jakautuisi todennäköisesti monilta osin eri tavoin niiden välillä. Ensinnäkin, vaikka tarkoitukset ja keinot katsottaisiin makrotasolla (ks. luku 4.2) samoiksi, asianajotoimistolla voidaan katsoa olevan oma taloudellinen intressinsä ammatinharjoittajana. Lisäksi asianajotoimiston on todennäköisesti säilytettävä tarkastuksessa käsiteltyjä tietoja vielä tarkastusprosessin jälkeen erilaisten vastuukysymysten (kuten mahdollisen vahingonkorvausvastuun) vuoksi. Ostajalla ei myöskään välttämättä ole pääsyä tarkastusta varten saatuihin tietoihin. Näyttäisikin siltä, että asianajotoimiston vastuu muodostuisi tarkastuksessa ostajan vastuuta laajemmaksi, mikäli yhteisrekisterinpitäjyys syntyisi.

Yhteisrekisterinpitäjiä koskevan 26 artiklan 3 kohdan mukaan keskinäisen järjestelyn ehdoista riippumatta rekisteröity voi kuitenkin käyttää asetuksen mukaisia oikeuksiaan suhteessa kuhunkin rekisterinpitäjään ja kutakin rekisterinpitäjää vastaan. Vaikka yhteisrekisterinpitäjien vastuulle kuuluvat sinänsä kaikki asetuksen mukaan rekisterinpitäjälle kuuluvat velvoitteet, artikla korostaa nimenomaisesti rekisteröidyn oikeuksien käyttöön sekä 13 ja 14 artiklan mukaisiin

[181] Asia C-210/16, kohta 43.
[182] Ratkaisuehdotus asiassa C40/17, kohta 101.
[183] *Blume* 2013, s. 141.
[184] Handbook on European data protection law, s. 24.

rekisterinpitäjän tehtäviin liittyviä velvoitteita. Säännöksessä viitatuista rekisteröidyn oikeuksista tärkein lienee TSA 82 artiklan mukainen vahingonkorvausoikeus.[185] Lisäksi rekisteröidyllä on käytössään 15–22 artikloiden mukaiset oikeudet, joita nähdäkseni voidaan niin ikään osoittaa kummalle tahansa yhteisrekisterinpitäjistä.

Rekisteröityyn päin vastuu on siis tietosuoja-asetuksessa yhteistä, mutta asetuksessa määriteltyjen hallinnollisten sakkojen osalta vastuu rajautuu sen mukaan, koskeeko rikkomus yhteisrekisterinpitäjien keskinäisen järjestelyn mukaan yksittäisen rekisterinpitäjän vastuualuetta.[186] Rekisteröityä kohtaan muodostuvan yhteisvastuun vuoksi on kuitenkin tärkeää, että jokainen yhteisrekisterinpitäjä huolehtii valmiuksistaan toteuttaa rekisteröidyn oikeuksia.[187] Yhteisvastuun vuoksi yhteisrekisterinpitäjän kannattaakin varmistua myös toisten yhteisrekisterinpitäjien valmiuksista noudattaa tietosuoja-asetusta jo ennen kuin yhteisrekisterinpitäjyydestä ja henkilötietojen käsittelystä sovitaan.

Vaikka rekisteröity voi osoittaa vaatimuksensa kenelle tahansa yhteisrekisterinpitäjistä, voidaan järjestelyn yhteydessä nimetä rekisteröidyille yhteyspiste (TSA 26 artiklan 1 kohta), jonka kautta rekisteröity voi vaatimuksensa esittää. Yhteyspisteen nimeäminen voikin olla yhteisrekisterinpitäjille keino saada rekisteröityjen pyynnöt keskitettyä mahdollisimman pitkälti samalle taholle ja siten voidaan jossain määrin kontrolloida myös sitä, kuka yhteisrekisterinpitäjistä huolehtii kustakin rekisteröidyn oikeuden toteutumisesta. Due diligence -tarkastuksessa oletettavasti asianajotoimiston on helpointa vastata muun muassa rekisteröidyn 15–22 artikloiden mukaisiin vaatimuksiin ja yhteyspisteen avulla pyynnöt voitaisiin kohdistaa suoraan sille, mikäli asianajotoimisto ja ostaja katsottaisiin yhteisrekisterinpitäjiksi. Rekisteröidyn kannalta ei näet liene olennaista, mikä taho tiedot antaa.

[185] *Feiler – Forgó – Weigl* 2018, s. 147.
[186] *Feiler – Forgó – Weigl* 2018, s. 147.
[187] *Hanninen – Laine – Rantala – Rusi – Varhela* 2017, s. 28.

6 JOHTOPÄÄTÖKSET

Tämän tutkielman tavoitteena on ollut selvittää, mikä on asianajotoimiston vastuuasema due diligence -tarkastuksessa, jota se suorittaa asiakkaansa toimeksiannon perusteella ja jossa käsitellään erilaisia henkilötietoryhmiä. Asianajotoimiston vastuuasemaa, eli toisin sanoen sitä, toimiiko asianajotoimisto henkilötietojen käsittelijänä vai rekisterinpitäjänä, on yhtäältä tarkasteltu käsitteiden määritelmien näkökulmasta ja toisaalta arvioimalla, miten osapuolet tosiasiassa voisivat täyttää asetuksen mukaiset velvoitteet. Ennen kyseistä arviointia on osakysymyksenä tutkittu, onko käsittelylle olemassa tietosuoja-asetuksen mukainen käsittelyperuste ja jos on, mikä tai mitkä perusteet tarkastukseen voisivat soveltua.

Oikeusperusteen määrittämisessä lähtökohtana oli, että henkilötietoja voitaisiin tarkastuksessa käsitellä lähinnä suostumuksen tai oikeutetun edun perusteella ja muut perusteet pystytään melko yksiselitteisesti rajaamaan pois. Suostumuksen osalta haasteena on se, ettei sen nojalla voida käsitellä työntekijän tietoja ensinnäkään siksi, ettei työntekijältä todennäköisesti haluta pyytää suostumusta, koska yrityskaupat ovat yleensä liikesalaisuuksia. Toiseksi, työntekijöiden on katsottu olevan sillä tavoin alemmassa asemassa työnantajaan nähden, ettei suostumusta työnantajaa koskevassa asiassa voida pitää vapaaehtoisena. Sen sijaan esimerkiksi yrityksen johdon ja mahdollisten avaintyöntekijöiden osalta suostumusta voidaan tarkastuksessa käyttää käsittelyperusteena.

Koska suostumus ei käsittelyperusteena sovellu kaikkiin tarkastuksessa käsiteltäviin henkilötietoihin, on arvioitava, voidaanko tietoja käsitellä oikeutetun edun perusteella. Ensinnäkin käsittelyperusteen soveltamiseksi on tarkasteltava, voidaanko ostajayhtiön taloudellista intressiä pitää oikeutettuna etuna. Vaikka oikeutettua etua ei tule nähdä porsaanreikänä, jonka avulla kaikki henkilötietojen käsittely voitaisiin viimesijaisesti perustella, on huomioitava, että jo normaalin liiketoiminnan kannalta on tärkeää, että oikeusperustetta voidaan käyttää erilaisissa tilanteissa. Kuten edellä on todettu, myös CJEU on ratkaisukäytännössään katsonut, että taloudellinen intressi voi sinänsä muodostaa oikeudellisen edun. Oikeutetun edun soveltamiseksi on lisäksi arvioitava käsittelyn tarpeellisuutta eli sitä, onko käsittelyn ja oikeutetun edun välillä yhteys. Kuten olen tutkielmassa tuonut esiin, tarpeellisuusvaatimuksen täyttyminen voi riippua myös yrityskaupan luonteesta, mutta todennäköisesti tarpeellisuusvaatimus useimmiten täyttyy.

Yrityskaupat ja due diligence -tarkastus ovat esimerkkejä, jotka on nimenomaisesti tuotu esiin oikeutetun edun tilanteina.[188] Tästä huolimatta tasapainotesti on kuitenkin tehtävä tapauskohtaisesti. Rekisteröidylle tarkastuksesta mahdollisesti aiheutuvat seuraukset liittyvät lähinnä henkilötietojen suojaan esimerkiksi tietoturvaloukkausten tilanteessa. Mikäli henkilötietojen suojalle aiheutuvan riskin katsottaisiin kaikenlaisessa käsittelyssä estävän oikeutetun edun käytön, oikeusperusteen käyttö tilanteessa kuin tilanteessa muodostuisi lähes mahdottomaksi. Pidänkin lähtökohtana, että due diligence -tarkastuksessa oikeutettu etu mahdollistaa henkilötietojen käsittelyn, koska riski rekisteröidyn oikeuksien loukkaamiselle on verrattain pieni.

Oikeusperuste on siis löydettävissä lähtökohtaisesti kaikkien esitettyjen henkilötietoryhmien käsittelyyn tarkastuksessa. Luvussa 5.2.2 on kuitenkin tuotu esiin rekisteröidyn informoinnin ja yrityskaupan liikesalaisuusluonteen välinen konflikti. Tiedonantovelvollisuus voi muodostua ongelmalliseksi niiden rekisteröityjen (esim. työntekijöiden) osalta, joille tietoa aiotusta yrityskaupasta ei voida tai haluta antaa. Tiedonantovelvollisuudesta poikkeuksen muodostavat tilanteet, joissa tiedot on lain nojalla pidettävä luottamuksellisena. Tällöin due diligence -tarkastuksessa on arvioitava, täyttääkö yrityskauppa LSL:n mukaisen käyttö- ja ilmaisukiellon vai perustuuko salassapito ainoastaan osapuolten väliseen sopimukseen.

Kysymykseen vastaaminen vaatii perusteellista ja yrityskauppakohtaista arviota. Arvion lopputuloksesta riippuen voitaisiin päätyä kahteen lopputulokseen: jos käyttö- ja ilmaisukieltoa koskeva säännös ei yrityskaupassa ja due diligence -tarkastuksessa sovellu, myyjän on anonymisoitava tiedot ennen niiden luovuttamista ostajalle ja asianajotoimistolle. Jos kielto realisoituu, henkilötietoja voidaan käsitellä ilman, että siitä ilmoitetaan rekisteröidyille. Huomattavaa on myös, että arvion tekeminen ei kuulu ainoastaan asianajotoimistolle tai ostajalle, vaan myös – ja ennen kaikkea – myyjälle, joka tiedot luovuttaa ja jonka on ennen luovutusta tehtävä arvio siitä, onko sen anonymisoitava tiedot ennen niiden luovuttamista.

Vaikka lainsäädäntöä tulkittaisiin siten, ettei työntekijöiden tietoja voitaisi tarkastuksessa käsitellä (anonymisoimatta), on asianajotoimiston rooli rekisterinpitäjänä tai henkilötietojen käsittelijänä määriteltävä muiden henkilötietoryhmien käsittelyä varten. Tämä määrittely perustuu usean elementin arviointiin, joista tärkein on kysymys siitä, osallistuuko asianajotoimisto käsittelyn tarkoitusten ja keinojen määrittämiseen. Tarkoitusten määrittämisen osalta voidaan to-

[188] Data Protection Network 2018, s. 13–14.

deta, että due diligence -tarkastuksen osalta ydintarkoitus, eli yrityskaupan tekeminen, on määritelty jo ennen henkilötietojen käsittelyn aloittamista ja mahdollisesti jo ennen toimeksiannon tekemistä, jolloin tarkoituksen on siltä osin määrittänyt ostaja. Tällöin on kuitenkin relevanttia arvioida, olisiko onnistunut yrityskauppa katsottava nimenomaisesti henkilötietojen *käsittelyn* tarkoitukseksi, sillä due diligence -tarkastus pitää sisällään huomattavan paljon myös muuta informaatiota, jonka tarkastamisella tavoitteeseen voitaisiin mahdollisesti päästä.

Nimenomaisesti henkilötietojen käsittelyn tarkoituksen osalta on huomattava, ettei ostajalla välttämättä ole tietoa siitä, mitä ja miten henkilötietoja on tarpeen käsitellä tarkastuksessa. Tällöin voitaisiin katsoa, että henkilötietojen käsittelyn tarkoituksen määrittää asianajotoimisto, joka ammatillisen toimintansa puolesta kykenee perustelemaan sen, miksi erilaisia tietoja käsitellään tarkastuksessa, eli mikä on henkilötietojen käsittelyn tarkoitus. Lisäksi on mahdollista, että asianajotoimiston taloudellinen intressi ammatinharjoittajana katsotaan käsittelyn erilliseksi tarkoitukseksi, sillä tarkoitus voidaan määritellä *suunniteltua toimintaa ohjaavaksi tekijäksi.* Olisi kuitenkin mahdollista argumentoida myös sen puolesta, ettei taloudellista intressiä pidettäisi itse henkilötietojen käsittelyn vaan pikemminkin koko yrityskauppaprosessissa avustamisen tarkoituksena.

Tarkoitusten lisäksi on arvioitava myös keinojen määrittelyyn osallistumista. Vaikka sinänsä olisi mahdollista, että keinot määrittäisi ostaja, tosiasiallisesti asianajotoimisto lienee kuitenkin se taho, joka määrittämisestä vastaa. Teknisten keinojen määrittely on luonnollinen osa asianajotoimiston roolia, sillä tarkastukset kuuluvat sen tavanomaiseen liiketoimintaan ja siksi sillä on oletettavasti vakiomuotoiset prosessit tarkastuksen tekniseen toteuttamiseen. Lisäksi on tarkasteltava esimerkiksi käsiteltävien tietojen, tietoihin pääsyn ja tietojen poistamiseen liittyvien seikkojen määrittämistä. Tällöin on huomioitava, että asianajotoimistolla voi olla vastuuasemaansa liittyviä syitä säilyttää tietoja pidempään kuin ostajan kannalta on tarpeellista. Lisäksi, kun asianajotoimisto on valtuutettu tekemään tarkastus ammattitaitonsa vuoksi, on perusteltua katsoa, että se päättää myös siitä, mitä tietoja tarkastuksessa käsitellään ja kenellä on pääsy tietoihin.

Tietosuojatyöryhmä WP29 on kuitenkin kannanotossaan korostanut, että yksin muodollisten seikkojen tarkastelu ei ole riittävää, vaan rekisterinpitäjän ja henkilötietojen käsittelijän määrittelyssä olisi kiinnitettävä huomiota tosiasialliseen rooliin. On selvää, että asianajotoimisto ei käsittelisi henkilötietoja ilman toisen tahon – eli ostajan – pyyntöä, mikä puoltaisi sen roolia

henkilötietojen käsittelijänä. Toisaalta asianajotoimiston rooli on tarkastuksessa kokonaisvaltainen, sillä se edustaa ostajaa ja tekee tarkastuksen itsenäisesti eikä ostaja lähtökohtaisesti anna ohjeita tarkastuksen tekemiseen ja siten henkilötietojen käsittelyyn. Tämä näkökulma tukee roolia rekisterinpitäjänä.

Koska erityisesti CJEU:n ennakkoratkaisuissa on korostettu tarvetta turvata rekisteröidyn oikeudet ja vapaudet aukottomasti, tutkielmassa tarkasteltiin myös, voitaisiinko turvaamisesta varmistua tietosuoja-asetuksen nojalla myös silloin, jos asianajotoimisto toimisi henkilötietojen käsittelijänä. Henkilötietodirektiivin aikana tuo turvaaminen näet edellytti useiden tahojen määrittelemistä rekisterinpitäjäksi, kun henkilötietojen käsittelijällä ei ollut nimenomaisia velvoitteita. Tätä arviota tehdessä on syytä huomata, että jos asianajotoimisto toimisi henkilötietojen käsittelijänä, rekisterinpitäjän roolissa toimisi väistämättä ostaja, jonka toimeksiannosta asianajotoimisto tekee tarkastusta. Vaikka myös myyjä ja sen edustaja käsittelevät tarkastuksessa henkilötietoja ainakin siltä osin, kuin ne luovuttavat tietoja tarkastusta varten, ei asianajotoimisto käsittele henkilötietoja niiden lukuun.

Rekisterinpitäjän ja henkilötietojen käsittelijän välisen sopimuksen sisältövaatimukset kuvastavat käsittelijän laajentunutta vastuuta. Käsittelijällä on muun muassa velvollisuuksia avustaa rekisterinpitäjää niiden asetuksen mukaisten vastuiden osalta, jotka eivät suoraan kuulu käsittelijälle. Auttamisvelvoitteet mahdollistavat näkökulman, jonka mukaan rekisterinpitäjänä toiminen ei enää olisi oikeuksien turvaamisen kannalta yhtä kriittistä kuin aiemmin. Lisäksi käsittelijälle suoraan osoitetut velvollisuudet turvaavat aiempaa paremmin rekisteröidyn oikeuksia. On silti huomionarvoista, että vaikka rekisterinpitäjä ja henkilötietojen käsittelijä vastaavat 32 artiklan mukaisesta turvallisuudesta tasapuolisesti, rekisterinpitäjän vastuu on kuitenkin siltä osin nähtävä laajempana, että se huolehtii yleisellä tasolla 5 artiklan mukaisten periaatteiden noudattamisesta ja sisäänrakennetun ja oletusarvoisen tietoturvan olemassaolosta. Lisäksi muun muassa tietoturvaloukkauksista ilmoittaminen ja rekisteröidyn 15–22 artikloiden mukaisista oikeuksista huolehtiminen on yksinomaan rekisterinpitäjän vastuulla. Rekisterinpitäjän vastuu näyttääkin myös tietosuoja-asetuksessa olevan huomattavasti laajempi kuin henkilötietojen käsittelijällä, vaikka kiistatta myös käsittelijän vastuut ovat lisääntyneet.

Mikäli asianajotoimisto toimisi henkilötietojen käsittelijänä, ostaja tarvitsisi rekisterinpitäjänä velvoitteidensa täyttämiseen huomattavan määrän apua asianajotoimistolta. Ostajalla ei näet olisi tosiasiallisia mahdollisuuksia esimerkiksi rekisteröidyn oikeuksien täyttämiseen tai tieto-

turvaloukkauksesta ilmoittamiseen ilman asianajotoimistoa. Myös oletusarvoisesta ja sisäänrakennetusta tietoturvasta vastaaminen olisi todennäköisesti jopa mahdotonta, kun ostajalla ei välttämättä ole mahdollisuuksia tai edes intressiä vaikuttaa käsittelyn tekniseen puoleen. Lisäksi varsin laajan osoitusvelvollisuuden täyttäminen voi osoittautua ostajalle käytännössä haastavaksi: sillä ei välttämättä ole käsittelystä ja sen vaiheista sellaisia kattavia tietoja, joilla se voi asianmukaisesti täyttää osoitusvelvollisuuden. Todennäköisesti moniin, samankaltaisiin vaikeuksiin törmätään myös useissa muissa tilanteissa, joissa rekisterinpitäjäksi katsottu taho on ulkoistanut henkilötietojen käsittelyn. Rekisterinpitäjä voi tällöin yrittää varmistua henkilötietojen käsittelijän luotettavuudesta erilaisten sertifiointimenettelyjen kautta, mutta sekään ei sinänsä tarjoa ratkaisua rekisterinpitäjän laajoihin velvoitteisiin. Tietosuojasääntelyä onkin kritisoitu siitä, että rekisterinpitäjän voi olla vaikeaa täyttää velvollisuutensa etenkin, kun se usein käsittelyn kannalta riippuvainen henkilötietojen käsittelijästä.[189]

Rekisteröidyn oikeuksien turvaamisen näkökulmasta tietosuoja-asetus voisi sinänsä mahdollistaa myös asianajotoimiston toimimisen henkilötietojen käsittelijänä vastuun laajennuttua, kun asianajotoimistolla olisi velvollisuus auttaa ostajaa oikeuksien toteuttamisessa. Oikeuksien turvaaminen näyttää toisaalta myös jokseenkin teoreettiselta velvollisuudelta due diligence -tarkastuksessa. Mikäli työntekijöiden tiedot olisi tarkastuksessa anonymisoitava, asetus soveltuisi ainoastaan yrityskaupasta tietävien rekisteröityjen henkilötietojen käsittelyyn. Pidän jokseenkin epätodennäköisenä, että nämä rekisteröidyt käyttäisivät oikeuksiaan kesken tarkastuksen – toki mahdollisuutta ei täydellisesti voida poissulkea. Lisäksi, mikäli yrityskaupan katsottaisiin muodostavan LSL:n mukaisen käyttö- ja ilmaisukiellon, työntekijöille ei annettaisi tietoa tehtävästä käsittelystä asetuksen 14 artiklan mukaisesti, jolloin ne eivät myöskään voisi käyttää 15–22 artikloiden mukaisia oikeuksiaan.

Vaikka rekisteröidyillä ei olisi tosiasiallista mahdollisuutta käyttää asetuksen mukaisia oikeuksia, se ei kuitenkaan poista niiden oikeutta henkilötietojen suojaan. Sen vuoksi pidän jokseenkin ongelmallisena, että ostajan ollessa rekisterinpitäjä, sen vastuu käsittelyn turvallisuudesta olisi tosiasiassa laajempi, vaikka 32 artikla asettaisi velvoitteet tasapuolisesti myös asianajotoimistolle. Lisäksi merkityksellistä on se, että henkilötietojen käsittelijänä asianajotoimiston olisi

[189] *Blume* 2013, s. 142.

käsiteltävä henkilötietoja ainoastaan ostajan dokumentoitujen ohjeiden mukaisesti (TSA 28 artiklan 3 kohdan a alakohta). Ostaja käyttää tarkastuksessa asianajotoimistoa sen ammattitaidon vuoksi ja siksi on epätodennäköistä, että ostaja edes kykenisi antamaan tällaista ohjeistusta.

Asianajotoimistolla on tarkastuksen toteuttamisessa ja henkilötietojen käsittelyssä runsaasti liikkumavaraa ja harkintavaltaa, ja ostajan rooli jää käsittelyn osalta siihen nähden marginaaliseksi, jollei jopa olemattomaksi.[190] Kun lisäksi otetaan huomioon, että asianajotoimiston voidaan perustellusti katsoa määrittävän käsittelyn tarkoituksia vähintään ostajan kanssa yhdessä, ja käsittelyn keinoja jopa itsenäisesti. Asianajotoimisto ei päätä ainoastaan käsittelyn teknisistä keinoista, eikä se todennäköisesti myöskään raportoi ostajalle käyttämistään keinoista. Asianajotoimiston määrittelemiselle henkilötietojen käsittelijäksi on siten vaikea löytää puoltavia seikkoja ja siksi sitä on mielestäni pidettävä rekisterinpitäjänä due diligence -tarkastuksessa. Ratkaistavaksi jää kuitenkin se, katsotaanko asianajotoimisto yhteisrekisterinpitäjäksi jonkin muun tahon – eli lähinnä ostajan tai mahdollisesti myyjän – kanssa.

Yhteisrekisterinpitäjäksi voidaan katsoa taho, jonka kanssa asianajotoimisto määrittää käsittelyn keinot ja tarkoitukset. Henkilötietojen käsittelyyn osallistuu tarkastuksessa myös myyjä ja sen edustaja, mutta koska niiden intressejä voidaan pitää vastakkaisina ostajan ja asianajotoimiston kanssa, pidän epätodennäköisenä, että asianajotoimiston ja myyjäpuolen välille syntyisi yhteisrekisterinpitäjien suhde. Henkilötietojen siirtäminen ei näet itsessään luo tällaista suhdetta ja todennäköisesti myyjällä ei muilta osin ole tarvetta käsitellä tietoja tarkastuksessa. Lähtökohtaisesti myyjä on kyseisiä henkilötietoja kohtaan rekisterinpitäjä esimerkiksi työnantajana ja tältä osin sitä pidetään erillisenä rekisterinpitäjänä.

Ostajan kanssa asianajotoimistolla on selvästi yhteinen tarkoitus, eli yrityskaupan onnistunut toteutuminen. Kuten olen edellä todennut, on mahdollista, ettei yrityskauppaa kuitenkaan pidettäisi nimenomaisesti *henkilötietojen käsittelyn* tarkoituksena (vaan due diligence -tarkastuksen tarkoituksena laajemmin). Osapuolet voivat myös määrittää käsittelyn keinoja yhdessä, vaikka tosiasiassa asianajotoimistolla on edellä mainituin tavoin suurempi rooli keinojen määrittämisessä. Yhteisrekisterinpitäjyys tulee kuitenkin punnita tarkkaan myös ostajan ja asianajotoimiston välillä, sillä on mahdollista, ettei ostaja osallistu henkilötietojen käsittelyyn tarkastuksessa ollenkaan. Vaikka CJEU:n ratkaisukäytännössä on todettu, ettei molemmilla rekis-

[190] Jossain määrin ostajan osallistuminen käsittelyyn riippuu kuitenkin toimeksiantosopimuksesta.

terinpitäjillä tarvitse olla pääsyä henkilötietoihin, ratkaisuille yhteistä on se, että yhteisrekisterinpitäjien välillä on luovutettu henkilötietoja tai toinen rekisterinpitäjistä vähintään kontrolloi ja ohjeistaa tiedonkeruuta. Lisäksi yhteisrekisterinpitäjyys on voinut ratkaisuissa syntyä sillä perusteella, että toinen osapuoli valitsee käsittelyn parametreja tai vastaanottaa tietoja.

Se, täyttyvätkö yllä olevat kriteerit ostajan ja asianajotoimiston välillä, riippuu ainakin osin siitä, mitä osapuolten välillä on toimeksiantosopimuksessa sovittu. Jos ostajalla on pääsy tietoihin (eli käytännössä datahuoneeseen) tai sillä on muuten mahdollisuus kontrolloida tietojen käsittelyä, se voitaisiin määritellä yhteisrekisterinpitäjäksi. Lisäksi, vaikka ostajalla ei olisi pääsyä tietoihin, se voi saada henkilötietoja due diligence -raportissa, jonka asianajotoimisto sille luovuttaa. Jos yhteisrekisterinpitäjyys katsottaisiin syntyväksi vain jälkimmäisen tilanteen nojalla, olisi mahdollista, että asianajotoimisto anonymisoisi raportissa mahdollisesti esitettävät henkilötiedot ja ostajaa ei siten katsottaisi yhteisrekisterinpitäjäksi.

Ostajan ja asianajotoimiston toimiminen yhteisrekisterinpitäjinä näyttäisi siten olevan niiden sopimuksen ja käytännön toteutuksen perusteella tapauskohtaisesti arvioitava tilanne. Mikäli toimijat katsottaisiin yhteisrekisterinpitäjiksi, muodostuisi asianajotoimiston vastuu kuitenkin myös tällaisissa tilanteissa laajemmaksi kuin ostajan vastuu ensinnäkin siksi, ettei ostajalla todennäköisesti ole aktiivista roolia käsittelyssä ja sillä ei välttämättä myöskään ole pääsyä tietoihin. Toiseksi, koska asianajotoimiston on säilytettävä tietoja myös tarkastuksen jälkeen, eikä ostaja määrittele tällaisen käsittelyn osalta tarkoituksia tai keinoja, asianajotoimiston katsottaisiin olevan tarkastuksen jälkeisestä käsittelystä vastuussa yksin, sillä yhteisrekisterinpitäjän vastuulle ei katsota sellaisia käsittelyketjun osia, joihin se ei osallistu lainkaan.[191]

Tutkielman johtopäätös on siis, että asianajotoimisto on tietosuoja-asetuksen nojalla katsottava rekisterinpitäjäksi. Sen voidaan katsoa täyttävän rekisterinpitäjän määritelmän ja lisäksi sen tosiasiallinen rooli käsittelyssä on kokonaisvaltainen. Se, määritelläänkö asianajotoimisto yhteisrekisterinpitäjäksi ostajan kanssa, riippuu osin ostajan asiantuntijuudesta ja samalla osapuolten välisestä sopimuksesta sekä siitä, osallistuuko ostaja tosiasiassa käsittelyyn.

Henkilötietojen käsittelyyn ja roolien määrittelyyn due diligence -tarkastuksessa liittyy myös lukuisia muita arvioitavia kysymyksiä. Erityisesti datahuonetta tarjoavien pilvipalveluiden asema käsittelyssä ja palvelun suhde sekä ostajan että myyjän puolella toimiviin tahoihin olisi

[191] Ks. Asia C-40/17, kohta 74.

jatkokysymyksenä mielenkiintoinen. Tietosuoja-asetuksen vaikutuksia pilvipalveluihin on myös oikeuskirjallisuudessa käsitelty runsaasti ja sinänsä niiden voidaan katsoa olevan keskiössä, kun asetuksella pyritään vastaamaan teknologiakehitykseen. Lisäksi EU:n ulkopuolelle osin sijoittuvat yrityskaupat ja tällaisesta rajan yli toiminnasta aiheutuvat velvoitteet sekä niiden mahdollinen vaikutus yrityskauppoihin yleisesti ovat kiinnostavia kysymyksiä.