MANAGING RIGHTS TO NON-PERSONAL DATA

Pauli Engblom
507294
Faculty of Law
University of Turku

April 2019

UNIVERSITY OF TURKU
FACULTY OF LAW

Pauli Engblom: Managing Rights to Non-Personal Data

Thesis, 74 pages, attachments, XVI pages
Commercial Law
April 2019
The originality of this thesis has been checked in accordance with the University of Turku quality assurance system using the Turnitin OriginalityCheck service.

– –

The Master's thesis discusses management of non-personal data in companies within the European Union. Non-personal data is for example data produced by Internet of Things through which natural persons cannot be identified and with which company may create value. The thesis examines non-personal data as an asset, relevant legislation to management of non-personal data and different approaches with which companies can manage non-personal data, especially contract law practises. The research aims to produce knowledge on this data economy phenomenon and to systematise management of non-personal data, especially from a legal point of view.

The Master's thesis is legal dogmatic but also law and economics approach is used. Moreover, an empirical survey on contracting practises of Finnish companies is conducted from viewpoint of non-personal data. Additionally, computer science is used to understand the research object non-personal data.

It is concluded that of the approaches available to companies, contract law, combined with indirect technical, legal and business practises, is an efficient approach to the management of non-personal data. A company's position in data value chain is argued to be a factor on selecting suitable practises for management of non-personal data. The distinction between personal and non-personal data is acknowledged as advantageous for companies. Problems regarding conceptualization of data is identified as key deficiency in public and private regulation of data. Further research on the subject is recommended.

Keywords: non-personal data, data economy, data, Internet of Things, big data

TURUN YLIOPISTO
OIKEUSTIETEELLINEN TIEDEKUNTA

Pauli Engblom: Managing Rights to Non-Personal Data

Tutkielma, 74 sivua, liitteet, XIX sivua
Kauppaoikeus
Huhtikuu 2019
Turun yliopiston laatujärjestelmän mukaisesti tämän julkaisun alkuperäisyys on tarkastettu Turnitin OriginalityCheck -järjestelmällä.

_ _

Pro gradu -tutkielma käsittelee muiden kuin henkilötietojen hallinnointia yrityksissä Euroopan unionin alueella. Muut kuin henkilötiedot, esimerkiksi esineiden internetin (Internet of Things) tuottamaa data, ovat tietoja, joiden avulla ei voida identifioida luonnollisia henkilöitä ja joiden avulla yritys voi tuottaa arvoa. Tutkielmassa käydään läpi muita kuin henkilötietoja hyödykkeenä, perehdytään muiden kuin henkilötietojen hallinointiin vaikuttavaan lainsäädäntöön ja tarkastellaan, miten yritykset voivat hallinnoida muita kuin henkilötietoja erityisesti sopimusoikeudellisia keinoja hyödyntäen. Tutkimuksen tavoitteena on tuottaa ymmärrystä tästä datatalouteen sisältyvästä ilmiöstä ja systematisoida muiden kuin henkilötietojen hallinnointia erityisesti oikeudellisesta näkökulmasta.

Tutkielma on lainopillinen. Tämä lisäksi tutkielmassa hyödynnetään oikeustaloustieteellistä ajattelua ja se sisältää myös empiirisen katsauksen suomalaisten yritysten yleisiin sopimusehtoihin muiden kuin henkilötietojen käsittelyn kannalta. Tietojärjestelmätieteitä hyödynnetään tutkimuksen kohteen, muiden kuin henkilötietojen ymmärtämiseksi.

Tutkielman johtopäätöksinä todetaan yritysten kannalta sopimusoikeuden ja siihen yhdistettyjen epäsuorien teknisten, oikeudellisten ja liiketoiminnallisten käytänteiden olevan käytettävistä keinoista tehokas tapa hallinnoida muita kuin henkilötietoja. Yrityksen aseman datan arvoketjussa katsotaan vaikuttavan sopivien hallinnointikäytänteiden valintaan. Erottelun henkilötietojen ja muiden kuin henkilötietojen välillä todetaan olevan yritysten kannalta hyödyllistä. Datan käsitteellistämisen ongelmat havaitaan julkisen ja yksityisen sääntelyn avainpuutteeksi. Jatkotutkimusta aiheesta suositellaan.

Avainsanat: muut kuin henkilötiedot, tietotalous, data, Internet of Things, esineiden internet, big data

Contents

Figures

Tables

References

Ackoff, Russell L., From Data to Wisdom. Journal of Applied Systems Analysis 16 (1) 1989, pp. 3–9.

Autorité de la Concurrence and Bundeskartellamt, Competition Law and Data. 2016. <http://www.autoritedelaconcurrence.fr/doc/reportcompetitionlawanddatafinal.pdf> accessed 6 February 2019.

Barnhizer, Daniel D., Inequality of Bargaining Power. University of Colorado Law Review. 76 2005, pp. 139–242.

Barron, Anne, The Legal Properties of Film. Modern Law Review 67 (2) 2004, pp. 177–208.

Baumann F.W., Breitenbücher U., Falkenthal M., Grünert G., Hudert S., Industrial Data Sharing with Data Access Policy, pp. 215–219 in Luo Y. (eds) Cooperative Design, Visualization, and Engineering. CDVE 2017. Lecture Notes in Computer Science, vol 10451. Springer, Cham.

Binder, Guyora, Criminal Law. Oxford University Press 2016.

Brinch, Morten, Understanding the Value of Big Data in Supply Chain Management and Its Business Processes. International Journal of Operations & Production Management 38 (7) 2018, pp. 1589–1614.

Calabresi, Guido – Melamed, A. Douglas, Property Rules, Liability Rules, and Inalienability: One View of the Cathedral. Harvard Law Review 1972, pp. 1089-1128.

Calliess, Gralf-Peter, The Making of Transnational Contract Law. Indiana Journal of Global Legal Studies 14 (2) 2007, pp. 469–483.

Cevriz, Janja, Two Roads Diverged in the Woods: On Non-Personal Data as a Legal Category in the EU. CITIP Blog 2017. <https://www.law.kuleuven.be/citip/blog/two-roads-of-data-diverged-in-the-woods-and-i-shall-address-the-non-personal-one-on-non-personal-data-as-a-legal-category-in-the-eu/> accessed 12 March 2019.

Chang, Yun-Chien, Optional Law in Property: Theoretical Critiques and a New View of the Cathedral. New York University Journal of Law and Liberty 9 2015.

Charles, Dan, Should Farmers Give John Deere And Monsanto Their Data? *National Public Radio, Inc.* 2014. <https://www.npr.org/sections/thesalt/2014/01/21/264577744/should-farmers-give-john-deere-and-monsanto-their-data> accessed 7 December 2018.

Coase, Ronald Harry, The Problem of Social Cost. The Journal of Law and Economics 56 (4) 2013, pp. 837–877.

Council of Europe/European Court of Human Rights, Guide on Article 8 - Right to Respect for Private and Family Life, Home and Correspondence. 2018 <https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf > accessed 10 March 2019.

Cowan, Mark J, – Newberry, Warren Jr., Reevaluating the Intellectual Property Holding Company. Management Accounting Quarterly 14 (3) 2013, pp. 25.

Crosby, Michael – Nachiappan – Pattanayak, Pradan – Verm, Sanjeev – Kalyanaraman, Vignesh, Blockchain Technology: Beyond Bitcoin. Applied Innovation Review 2/2016, pp. 6–19.

Dallemule, Leandro – Davenport, Thomas H., What Is Your Data Strategy. Harvard Business Review : HBR 95 (3) 2017.

Daneels, A – Salter, W, What Is SCADA?. International Conference on Accelerator and Large Experimental Physics Control Systems, 1999, pp. 339–343. <http://cds.cern.ch/record/532624/files/mc1i01.pdf> accessed 16 February 2019.

de Wolf, Ronald, The Potential Impact of Quantum Computers on Society. Ethics and Information Technology 19 (4) 2017, pp. 271–276.

den Butter, Frank AG – Groot, Stefan PT – Lazrak, Faroek, The Transaction Costs Perspective on Standards as a Source of Trade and Productivity Growth. Tinbergen Institute Discussion Paper TI 2007-090/3, 2007 <http://hdl.handle.net/1871/12633> accessed 16 February 2019.

Drexl, Josef – Hilty, Reto M. – Desaunettes, Luc – Greiner, Franziska – Kim, Daria – Richter, Heiko – Surblytė, Gintarė – Wiedemann, Klaus, Position Statement of the Max Planck Institute for Innovation and Competition of August 16, 2016 "On the Current Debate on Exclusive Rights and Access Rights to Data at the European Level", 2016.

Eigen, Zev J., Empirical Studies of Contract. Faculty Working Papers, Paper 204, 2012. <http://scholarlycommons.law.northwestern.edu/facultyworkingpapers/204> accessed 13 February 2019.

Eloranta, Ville, Servitization, Strategy and Platforms. Aalto University, Department of Industrial Engineering and Management 2016.

Ezrachi, Ariel – Stucke, Maurice E., Virtual Competition: The Promise and Perils of the Algorithm-Driven Economy. Harvard University Press 2016.

Global Piracy Increases throughout 2017, MUSO Reveals. 2018. <https://www.muso.com/magazine/global-piracy-increases-throughout-2017-muso-reveals/> accessed 22 March 2019.

GNU General Public License 3.0. 2007 Free Software Foundation. <https://www.gnu.org/licenses/gpl-3.0.html> accessed 24 February 2019.

Godt, Christine, Intellectual Property and European Fundamental Rights, pp. 210–235, in Micklitz, Hans (ed.): Constitutionalization of European Private Law, Oxford University Press 2014.

Goyal, Vipul – Pandey, Omkant – Sahai, Amit – Waters, Brent, Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data. <https://eprint.iacr.org/2006/309.pdf> accessed 25 March 2019.

Guadamuz, Andres, Artificial Intelligence and Copyright. 2017. <https://www.wipo.int/wipo_magazine/en/2017/05/article_0003.html> accessed 20 February 2019.

Hagiu, Andrei – Wright, Julian, Multi-Sided Platforms. International Journal of Industrial Organization 43 (C) 2015, pp. 162–174.

Haider, Murtaza, Getting Started with Data Science: Making Sense of Data with Analytics. IBM Press 2015.

Hoeren, Thomas, Big Data and the Legal Framework for Data Quality. International Journal of Law and Information Technology 25 (1) 2017, pp. 26–37.

Husovec, Martin, Injunctions against Intermediaries in the European Union: Accountable but Not Liable? Cambridge University Press 2017.

Ince, Darrel, Application Programming Interface, A Dictionary of the Internet Oxford University Press 2013. <http://www.oxfordreference.com/view/10.1093/acref/9780191744150.001.0001/acref-9780191744150-e-151> accessed 25 March 2019.

Kaartamo, Valtteri – Pelto, Elina, Translation Mechanisms of International Market Shaping: The Transformation of the St. Petersburg Bread Market from 1997–2007. Journal of East-West Business 23 (3) 2017, pp. 260–282.

Karo, Marko, Tekijänoikeudesta ja tietokantojen suojasta informaatioyhteiskunnassa, pp. 127–182 in Mylly, Tuomas (ed), Immateriaalioikeudet kansainvälisessä kaupassa, Kauppakaari -

Lakimiesliiton Kustannus 2001.

Kastrenakes, Jacob, Why Carmakers Want to Keep Apple and Google at Arm's Length. *The Verge*. 2017. <https://www.theverge.com/2017/1/13/14268252/apple-carplay-google-android-auto-vs-carmakers> accessed 7 December 2018.

Ken, Moon – Carter, Laura, New Zealand: Digital Files Constitute "Property", Says Supreme Court. Managing Intellectual Property 2015 pp. 3–5.

König, Michael, The 'Emerging Issue' of Data Ownership. 2016. <http://www.grur.org/uploads/tx_meeting/03-Vortrag_König_GRUR.pdf> accessed 24 February 2019.

Krönke, Christoph, Data Regulation in the Internet of Things. Frontiers of Law in China 13 (3) 2018, pp. 367–379.

Law, Jonathan, Standard of Proof, A Dictionary of Law. Oxford University Press 2018. <http://www.oxfordreference.com/view/10.1093/acref/9780198802525.001.0001/acref-9780198802525-e-3757> accessed 5 March 2019.

Osborne Clarke LLP, Legal Study on Ownership and Access to Data. Final Report – A study prepared for the European Commission DG Communications Networks, Content & Technology, 2016.

Lim, Chiehyeon – Kim, Ki-Hun – Kim, Min-Jun – Heo, Jun-Yeon – Kim, Kwang-Jae – Maglio, Paul P., From Data to Value: A Nine-Factor Framework for Data-Based Value Creation in Information-Intensive Services. International Journal of Information Management 39 2018, pp. 121–135.

Maine, Henry Sumner, Ancient Law: Its Connection with the Early History of Society and its Relation to Modern Ideas, John Murray, 1861.

Marr, Bernard, Internet Of Things And Machine Learning: Ever Wondered What Machines Are Saying To Each Other? *Forbes*. 2017. <https://www.forbes.com/sites/bernardmarr/2017/02/21/how-ai-and-real-time-machine-data-helps-kone-move-millions-of-people-a-day/#6526dd555f97> accessed 7 December 2018.

Nordic Market Data AB, Suurimmat Yritykset Liikevaihdon Mukaan - Suomi. <http://www.largestcompanies.fi/toplistat/suomi/suurimmat-yritykset-liikevaihdon-mukaan-ilman-tytaryhtioita> accessed 11 February 2019.

YouGov, Number of Britons Illegally Downloading Music Falls, 2018.

<https://yougov.co.uk/topics/arts/articles-reports/2018/08/02/number-britons-illegally-downloading-music-falls> accessed 22 March 2019.

O'Leary, Daniel E., Artificial Intelligence and Big Data. IEEE Intelligent Systems 28 (2) 2013, pp. 96–99.

OECD, The Internet of Things: Seizing the Benefits and Addressing the Challenges. 2016. <https://doi.org/10.1787/5jlwvzz8td0n-en> accessed 22 February 2019.

OECD, Data-Driven Innovation: Big Data for Growth and Well-Being. 2015. <https://doi.org/10.1787/9789264229358-en> accessed 22 February 2019.

Oppliger, Rolf, Internet Security: Firewalls and Beyond. Communications of the ACM 40 (5) 1997, pp. 92–102.

Pan, Xinyu – Ma, Jingzhong – Wu, Chengxia, Decision Game of Data Sharing in Supply Chain Enterprises Considering Data Value over Time. The Journal of Supercomputing 2018.

Porter, Michael E., Competitive Advantage : Creating and Sustaining Superior Performance. Free Press 1985.

Rapaczynski, Andrzej, The Roles of the State and the Market in Establishing Property Rights. Journal of Economic Perspectives 10 1996, pp. 87–103.

Rawls, John, A Theory of Justice. Rev ed. Oxford University Press 1999.

Reinsel, David – Gantz, John – Rydning, John, Data Age 2025: The Evolution of Data to Life-Critical Don't Focus on Big Data; Focus on the Data That's Big. IDC White Paper 2017 pp. 1–25. <www.idc.com> accessed 14 November 2018.

Riva, Monica, Trade Secret's Protection and Big Data an Italian View. *Talking Tech*. 2018. <https://talkingtech.cliffordchance.com/en/ip/other/trade-secret-s-protection-and-big-data-an-italian-view.html> accessed 24 February 2019.

Rock, Ron – Moran, Michael, A 21st Century Framework for Data Ownership. 2018. <https://www.microshare.io/wp-content/uploads/2018/06/21stCenturyFramework-June2018-ML-R3.pdf> accessed 23 February 2019.

Savelyev, Alexander: Contract Law 2.0: Smart Contracts as the Beginning of the End of Classic Contract Law. Higher School of Economics Paper No. WP BRP 71/LAW/2016, 2016.

Schroedert, Jeanne L, Three's a Crowd: A Feminist Critique of Calabresiand Melamed's One View of the Cathedral. Cornell Law Review 84 (2) 1999, pp. 394–503.

Seppälä, Timo – Juhanko, Jari – Mattila, Juri, Data Ownership and Governance. ETLA Brief No 71, 2018.

Tammi-Salminen, Eva, Esinevakuusoikeuden Perusteet. Talentum Pro 2015.

Tarkela, Pekka, Digitaalinen talous, data ja varallisuusoikeuden muutostarpeet. Liikejuridiikka (2) 2016.

Tollen, David W., The Big Data Licensing Issue-Spotter. The Licensing Journal 36 (3) 2016, pp. 1–8.

Toosi, Adel Nadjaran – Calheiros, Rodrigo N. – Buyya, Rajkumar, Interconnected Cloud Computing Environments. ACM Computing Surveys 47 (1) 2014, pp. 1–47.

Trivedi, Priti, Writing the Wrong: What the E-Book Industry Can Learn from Digital Music's Mistakes with DRM Notes and Comments. pp. 925–966.

Tusikov, Natasha, Chokepoints : Global Private Regulation on the Internet. 1st ed. University of California Press 2016.

Unicode/UTF-8-Character Table. <https://www.utf8-chartable.de/unicode-utf8-table.pl?utf8=bin> accessed 22 February 2019.

Wang, Shangping – Zhang, Yinglong – Zhang, Yaling, A Blockchain-Based Framework for Data Sharing With Fine-Grained Access Control in Decentralized Storage Systems. IEEE Access 6 2018, pp. 38437–38450. <https://ieeexplore.ieee.org/document/8400511/> accessed 18 February 2019.

Wendell Holmes Jr., Oliver, The Path of the Law. Harvard Law Review 10 (457) 1897, pp. 1–36.

Wolff, Richard D. – Resnick, Stephen A., Contending Economic Theories : Neoclassical, Keynesian, and Marxian. MIT Press 2012.

Yu, Zhenxin – Yan, Hong –Cheng, T. C. Edwing, Benefits of Information Sharing with Supply Chain Partnerships. Industrial Management & Data Systems 101 (3) 2001, pp. 114–121.

Zamir, Shmuel – Solan, Eilon – Maschler, Michael, Game Theory. Cambridge eText 2013.

European Commission Documents

Decisions

Case 94/19/EC. Commission Decision of 21 December 1993 relating to a proceeding pursuant to Article 86 of the EC Treaty (IV/34.689 - Sea Containers v. Stena Sealink - Interim measures). OJ 18.1.1994 L 15.

Non-regulatory documents

COM(2017) 9 Final. Communication from the Commission – Building a European Data Economy.

COM(2017) 495 Final. Proposal for a regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union.

COM(2018) 232 Final. Communication from the Commission – Towards a common European data space.

IP/18/4227. 2018. European Commission Press Relase: *Digital Single Market: EU negotiators reach a political agreement on free flow of non-personal data*.

IP/19/525. 2019. European Commission Press Relase: *Digital Single Market: EU negotiators agree on new rules for sharing of public sector data*.

SWD(2017) 2 Final. Commission Staff Working Document on Free Flow of Data and Emerging Issues of the European Data Economy.

SWD(2018) 125 Final. Commission Staff Working Document – Guidance on sharing private sector data in the European data economy.

SWD(2018) 146 Final. Commission Staff Working Document – Evaluation of Directive 96/9/EC on the legal protection of databases.

Case Law

Court of Justice of the European Union

Brayer

Judgment of the Court (Second Chamber), 19 October 2016, *Patrick Breyer v Bundesrepublik Deutschland*, C-582/14, EU:C:2016:779.

British Horseracing Board v William Hill

Judgment of the Court (Grand Chamber), 9 November 2004, *The British Horseracing Board Ltd and Others v William Hill Organization Ltd*, C-203/02, EU:C:2004:695.

Fixtures Marketing v OPAP

Judgment of the Court (Grand Chamber), 9 November 2004, *Fixtures Marketing Ltd v Organismos prognostikon agonon podosfairou AE (OPAP)*, C-444/02, EU:C:2004:697.

Fixtures Marketing v Svenska Spel

Judgment of the Court (Grand Chamber), 9 November 2004, *Fixtures Marketing Ltd v Svenska Spel AB*, C-338/02, EU:C:2004:696.

Fixtures Marketing v Veikkaus

Judgment of the Court (Grand Chamber), 9 November 2004, *Fixtures Marketing Ltd v Oy Veikkaus Ab*, C-46/02, EU:C:2004:694.

Football DataCo v Yahoo

Judgment of the Court (Third Chamber), 1 March 2012, *Football Dataco Ltd and Others v Yahoo! UK Ltd and Others*, C-604/10, EU:C:2012:115.

Ryanair v PR Aviation

Judgment of the Court (Second Chamber), 15 January 2015. *Ryanair Ltd v PR Aviation BV*, C-30/14, EU:C:2015:10.

SAS Institute. v World Programming

Judgment of the Court (Grand Chamber), 2 May 2012, *SAS Institute Inc. v World Programming Ltd*, C-406/10, EU:C:2012:259.

France:

Cour de cassation, criminal chamber, published 20 May 2015, N°: 14-81336, FR:CCASS:2015:CR01566.

United Kingdom

Oxford v Moss, (1979) 68 Cr App Rep 183, [1979] Crim LR 119.

Your Response Ltd v Datateam Business Media Ltd, [2014] EWCA Civ 281.

United States of America

Oracle America, Inc., v. Google LLC, No. 17-1118, (Fed. Cir. Mar. 27, 2018).

List of Abbreviations

API	Application programming interface
Art.	Article
B2B	Business-to-business
B2G	Business-to-government
DG	Directorate General
DRM	Digital Rights Management
EUCJ	the Court of Justice of the European Union
EU	European Union
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
GTC	General Terms and Conditions
OAD Report	Legal study on Ownership and Access to Data – Final Report. A study prepared for the European Commission DG Communications Networks, Content & Technology by: Osborne Clarke LLP
OEM	Original equipment manufacturer
TRIPS	Agreement on Trade-Related Aspects of Intellectual Property Rights
UK	United Kingdom

1. INTRODUCTION

Should Farmers Give John Deere and Monsanto Their Data?[1] *Internet of Things and Machine Learning: Ever Wondered What Machines Are Saying To Each Other?*[2] *Why carmakers want to keep Apple and Google at arm's length*?[3]

News headlines like these show that, as the global economy is becoming data-driven, questions are emerging, and not only regarding the protection of personal data.[4] Even though data privacy and issues considering personal data have been highlighted in the European Union lately due to the introduction of the General Data Protection Regulation (GDPR)[5], there are important issues concerning non-personal data as well. Problems, such as who non-personal data belongs to and how non-personal data can be licensed, have become important. For companies, their ability to utilise digital data has become a key competitive factor following advancements in information technology, such as faster connectivity and increased processing capacity.[6]

The growing impact data has on commerce is having businesses ask how data-related rights and obligations should be managed between companies. The theme is interesting because, while in the past data had to be collected and stored by humans, data collection can now be done automatically by machines. The amount of machine-generated data is currently increasing fast as more sensor will be connected to the so-called Internet of Things, a technology enabling machine to machine communication in different industries.[7] The data, collected by these sensors, could be for instance data about production processes, processing steps of machinery or environmental parameters such as humidity, light irradiation, and temperature.[8] The market research company IDC predicts that not only will the amount of data generated annually increase tenfold from 16 zettabytes in 2016 to 163 in 2025 (zettabyte being one trillion gigabytes), but a significant proportion of that data will also be crucial to the daily lives of

[1] Charles 2014.
[2] Marr 2017.
[3] Kastrenakes 2017.
[4] On data economy, see COM(2017) 9 Final. 2017.
[5] OJ 4.5.2016 L 119, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC
[6] See for example a report by the French and German competition authorities, Autorité de la Concurrence and Bundeskartellamt 2016 8, 11.
[7] OECD 2016 7.
[8] Baumann et al. 2017 216.

people.[9] In addition, development of phenomena, such as platform economics and artificial intelligence, are fuelled by the growing amounts of data.[10]

In this thesis, I aim to shed light on the issues mentioned above. More precisely, the research question of the thesis is *how private market actors can get access to non-personal data and to restrict others from using non-personal data.* I call the process of getting access to and restricting others from using non-personal data the management of non-personal data.

I will start this thesis with an introduction. The introduction will contain a basic overview of applicable law and a look at literature considering the use of non-personal data. After this, I will lay out specifications and limitations on how the research question is addressed. Lastly, I will present the structure of the thesis.

1.1. Overview of the Relevant Legislation

In the European Union, the two key legal concepts of data are personal and non-personal data. In Art. 4(1) of the GDPR, personal data is defined as any information relating to an identified or identifiable natural person. Symmetrically, in Art. 3(1) of the GDRP's counterpart, the Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union[11], non-personal data is defined as data other than personal data as defined in Art. 4(1) of the GDPR. The two regulations are thus mutually exclusive. As indicated in recital 1 of the GDPR, the separation of personal and non-personal data reflects the fact that personal data has strong ties to the protection of privacy which is secured as fundamental freedom by *inter alia* Art. 8 of the Charter of Fundamental Rights of the European Union.[12] However, especially after *Breyer* case the distinction between personal and non-personal data is not as straightforward as it might seem. In *Breyer*, the Court of Justice of the European Union, interpreting the GDPR's predecessor, Directive 95/46[13], held that data can be considered personal data even when the data subject can only be identified using additional information from third-parties.[14]

---

[9] Reinsel – Gantz – Rydning 2017.
[10] Ezrachi – Stucke 2016 16–17; O'Leary 2013.
[11] OJ 28.11.2018 L 303.
[12] For example, under the European Convention of Human Rights, privacy is protected under Art. 8, right to respect for private and family life. See for example, Guide on Article 8 - Right to Respect for Private and Family Life, Home and Correspondence. 2018.
[13] OJ, 23.11.1995 L 281, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
[14] C-582/14, *Patrick Breyer v Bundesrepublik Deutschland*, EU:C:2016:779, paragraph 49.

In addition to the two regulations, data or rather 'computer data' is, in EU legislation, also defined in Art. 2 of the Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA[15] as a representation of facts, information or concepts in a form suitable for processing in an information system, including a programme suitable for causing an information system to perform a function.

There is not too much literature on the legal framework of non-personal data specifically, perhaps due to the wider introduction of the term itself as recently as in 2018 with the introduction of the Free Flow of Non-Personal Data Regulation.[16] However, there are a few studies conducted for research or public agencies that focus on data generally and paint a picture of the legal framework relevant to non-personal data. Also more specific academic literature exists. The three studies presented next give a general grasp on the issues regarding management of non-personal data, based on which the structure the thesis can be laid out.

Firstly, in Finland, Seppälä, Juhanko and Mattila conducted a short report for ETLA, Research Institute of the Finnish Economy, where they concluded that under Finnish law, data cannot be legally owned.[17] However, as they point out, practically data can belong to certain actors. This is because usually the owner of the device or service in question has the inherent ability to prevent others from accessing the data that is stored in the device or service. In addition to factual management of data, Seppälä, Juhanko and Mattila conclude that there are different legal regimes suitable for management of data, such as intellectual property law including database protection, data protection legislation and contract law.[18]

Secondly, at the EU level, the European Commission's Directorate-General of Communications Networks, Content & Technology ordered a study from the law firm Osborne Clarke LLP on Ownership and Access to Data (OAD Report).[19] The report explores the EU *acquis communautaire* and the national legislation of England and Wales, France, Germany and Spain in relation to non-personal data. For example the relationship between their criminal law systems and data are explored and differences between national systems found.[20] Considering the EU *acquis*, the study suggests that the relatively new Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed

[15] OJ 14.8.2013 L 218.
[16] Regarding the introduction of the consept of non-personal data, see Cevriz 2017.
[17] Seppälä – Juhanko – Mattila 2018.
[18] Seppälä – Juhanko – Mattila 2018 3–4.
[19] Osborne Clarke LLP 2016.
[20] Osborne Clarke LLP 2016 6.

know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure[21] (Trade Secrets Directive) could be used in protecting data, if the data meets certain criteria.[22] Regarding copyright and database protection, the study concludes that they offer only limited scope of protection for data.[23] The study also explores sector specific legislation and the impact of competition law.[24] It is also pointed out that, in practise, contract law is the field of law relied by companies managing their data.[25]

Finally, in literature, Tarkela has argued that the legislation surrounding data is fragmented. He claims that the existing property law or intellectual property law rules do not provide a functioning point of reference for digital data as they cannot grasp the special attributes of data, such as its formability. Tarkela also views the protection of personal data regime as too sector-specific to provide a coherent legal system around data. Instead of looking at one regime at a time, he calls for legal scholars to study broader connections between different branches of law in order to systematise the law for digital economy.[26]

As a conclusion from these three studies it can be said, that while data has a net asset value, the legal aspects surrounding data are somewhat ambiguous not less so because there is no well-established property right regime (*erga omnes* rights, rights with effects towards everybody) for data. A metaphor for the fragmented regulation surrounding data could be a flower with several petals, each of the petals covering some area at the centre of the flower, while none of them covers the whole centre (Figure 1). Similarly, there are multiple areas of law or different legislative regimes that surround or cover data but none of them covers the whole field of data related issues.

For actors within the data economy, this scattered legislation presents significant challenges. This is especially true regarding non-personal data, since the GDPR provides *lex generalis* for personal data while the Free-Flow of Non-Personal Data Regulation only regulates specific issues. Some issues are regulated whilst some are not. Somehow the market actors must try to cover whole of the whole area, even when no legislation covers it all.

---

[21] OJ 15.6.2016 L 157.
[22] Osborne Clarke LLP 2016 9–12.
[23] Osborne Clarke LLP 2016 12–15.
[24] Osborne Clarke LLP 2016 15–26.
[25] Osborne Clarke LLP 2016 28.
[26] Tarkela 2016 5.1.

Figure 1 Legislation surrounding data can be viewed as a flower the petals of which are fields of law, each covering partly the legal issues regarding non personal data while non cover the whole of the middle area.

The main tool to emerge for managing non-personal data and rights to it seems to be contract law. Therefore as this thesis will explore management of rights to non-personal data from various angles, contract law will act as the common thread, binding the aspects together. For example, the tension between the flexibility of contract law and its inability to inflict obligations on third-parties will be central.

1.2. Methods, Scope and Structure of the Research

The information interest associated with the research question *how private actors can get access to non-personal data and to restrict others from using non-personal data* is quite pragmatic. Thus, another way to formulate the research question would be, in the spirit of Oliver Wendell Holmes' 'bad man', how one can avoid disagreeable consequences and pursue the agreeable consequences when doing business using non-personal data.[27] This pragmatic angle ensures that the discussion stays focused on the law as it is and as it perhaps will be in the near future. However, in answering the research question only legal dogmatic method is not enough. Also, law and economics framework needs to be applied so that the legal field and regulatory framework around non-personal data is better understood from point of view of companies and of the society. To understand data as an asset, computer science is used. Furthermore, a small-

[27] Wendell Holmes Jr. 1897 4.

scale empirical qualitative analysis is conducted in subchapter 5.4 to reflect on the findings of the other methods. The legal system analysed is that of the European Union[28] and, when an issue is legislated at the national level, its member states though their legal systems cannot be analysed in detail.

I focus on commercial use of non-personal data. Therefore, for example managing non-personal data regarding scientific research projects is excluded. Also business to consumer relations are not discussed. Sector specific legislation, such as the REAC regulation[29] for chemicals or regulations for the pharmaceutical sector is excluded from the scope of this work. The chosen scope will allow me to study the research from a viewpoint that is relevant, for example regarding the developing Internet of Things and industrial data sharing.

By management of rights to non-personal data, I mean the different practises that private market actors, companies, may use to get access to non-personal data, to restrict others from using non-personal data and to decrease the legal risks related to disposing non-personal data. Management of non-personal data between entities can and often involves legal solutions made possible by applicable law and private regulation but also technical solutions or a combination of legal and technical solutions. This thesis does not cover management of non-personal data within an organization which is a separate topic.[30]

In chapter 2, I begin answering the research question by asking what non-personal data is. In other words, I will be going through some of the characteristics that data has as an asset in order to better understand the issues that managing non-personal data should find solutions for. I will also present definitions for data and non-personal data which are then used throughout the work. Then in chapter 3, I will analyse the legal environment around non-personal data, review the relevant legal regimes establishing rights that affect managing non-personal data. In chapter 4, I will review practises that can be used to indirectly manage non-personal data. By indirect I mean that the rights themselves are not managed but directed through different legal, technical and business practises. After that in chapter 5, I analyse how rights on non-personal data can be created by private actors using contract law and how they can then be bargained for. This is

[28] At the time of writing, the United Kingdom was in the process of leaving the European Union ('Brexit') and the possible end date of that process remained unclear. As for example the UK case law presented in this thesis is from the time when the UK was a Member State, European Union in this thesis includes the UK.
[29] Regulation (EC) No 1907/2006 of the European Parliament and of the Council of 18 December 2006 concerning the Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH), establishing a European Chemicals Agency, amending Directive 1999/45/EC and repealing Council Regulation (EEC) No 793/93 and Commission Regulation (EC) No 1488/94 as well as Council Directive 76/769/EEC and Commission Directives 91/155/EEC, 93/67/EEC, 93/105/EC and 2000/21/EC. OJ 30.12.2006 296.
[30] For discussion considering management of big data within organisation, see Brinch 2018 1603.

what I call the direct management of rights to non-personal data. Finally in chapter 6, I end the thesis by providing a conclusion of legal means of managing non-personal data *de lege lata* and give some insights *de lege ferenda*.

While this thesis gives insights to managing non-personal data it must be remembered that the separation between non-personal and personal data may not be as simple in practise. As stated in Art. 2(2) of the Free Flow of Non-Personal Data Regulation, the GDPR shall apply to the inextricably linked data where personal and non-personal data in a data set are inextricably linked. For example due to deanonymization of non-personal data, it is not clear how data can be anonymized even now or indeed, if computation power grows exponentially in the future allowing identifying of individuals from data in unpredictable ways.[31] This outline of personal data is of course, a limitation for the thesis, but one that I believe makes it possible to better focus on non-personal data. Also, while from data protection and compliance standpoint personal and non-personal data are quite different, as an asset they are essentially and technically the same. Therefore, excluding data protection and compliance issues, the thesis may also provide insights on e.g. licensing of personal data.

[31] For example, the development of quantum computers might result in unforeseen data processing capacities. See de Wolf 2017 273.

2. DATA, A PECULIAR ASSET

In this chapter, I will first define data and this definition is then used throughout the remaining thesis. After that, I will introduce some of the characteristics of data which are relevant to understanding legal issues regarding the management of non-personal data. Finally, I will present a value chain for data which will provide insights on how market actors create value from non-personal data.

2.1. Defining Data

While in colloquial language words such as data, information and knowledge may almost be used as synonyms, in computer science each term has been given a distinct meaning. In 1989, Acknoff defined data as symbols that represent the properties of objects and events, information as a collection of data that has been somehow processed and structured, and knowledge as information that answers how-to questions.[32] The concepts laid out by Acknoff have been often represented in a pyramid where each lower level is a requirement for the upper levels and where the usefulness increases towards the top of the pyramid (Figure 2). The concepts can also be viewed as a continuum where the structuration level, usefulness and value grow from data to information to knowledge.

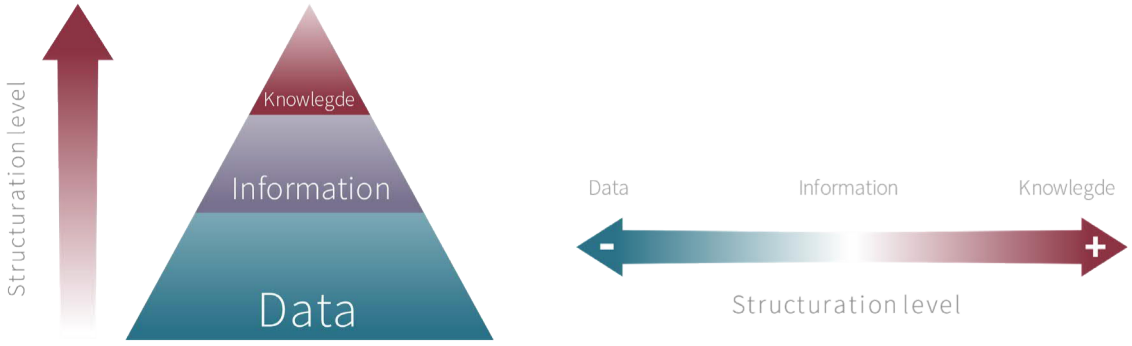

Figure 2 Two visualisations of the relationship between data, information and knowledge. In the pyramid, structuration and usefulness increase towards the top of the pyramid. The structuration level continuum emphasizes that the borders between each concept are not clear-cut.

For example, the capital letter A is written as 01000001 in binary form, using the Unicode UTF-8 encoding.[33] Without information of the standard '01100001' is mere data and has no information value. With the information on the UTF-8 encoding however, '01000001' can be

[32] See, for example Ackoff 1989.
[33] Unicode/UTF-8-Character Table.

attached with certain information value, interpreted as the capital letter A. This example clarifies why data has a dual nature as mere meaningless symbols and as something that has potential to become information. The nature of that potential information may have different legal implications, for example as works protected by copyright or as military secrets.

In this thesis, following Tarkela, I will define data as a raw material and mediation material level phenomenon.[34] When using this definition, on scale *data – information – knowledge* Tarkela sees data as carrier of information. [35] When data is defined like this, the definition does not implicate the economic or legal value of data, for example whether data is subject to personal data protection or trade secret protection. However, in this thesis data that would be considered carrying personal information (personal data under the GDPR) will not be studied. Data is also defined as being on such unstructured level on the *data – information – knowledge* continuum that it cannot be viewed as a work protected by the EU's and its Member States copyright legislation. However, the line between data and information is somewhat thin and arbitrary and thus something that is here considered data could be considered information by someone else. I chose this definition because it allows me to analyse management non-personal data within the context of Internet of Things and machine-learning and other economically and societally increasingly important phenomena.

While data can be both analogical and digital (in a form that computers understand), here I will focus solely on digital data and for convenience, use the word data for digital data due to its importance in data economy. Also, if data is carried in analogical form, for example on paper it can be managed using the well-established rules of tangible items.

Digital data has several characteristics that make its economics unique. Firstly, data is inexhaustible, meaning that data can be copied and accessed indefinite number of times, without changes to its quality. Secondly, data is non-rivalrous and can therefore be accessed by different users without them precluding others from accessing the data. Thirdly, data is non-exclusive because the use of data cannot be limited if the data becomes public.[36] Fourthly, data is processable and mouldable. This means that its usefulness can be increased, for example by using data analytics. [37]

In practise, the value of data can be enhanced in companies by data scientists or statisticians who in their work try to find value from data by transferring it into more usable information

[34] Tarkela 2016 2.1.
[35] Tarkela 2016 2.1.
[36] Osborne Clarke LLP 2016 89.
[37] Tarkela 2016 2.1.

and knowledge through a variety of activities, such as selecting data, pre-processing data to reduce its biases, storing data and mining data using data analysis such as statistical methods.[38] These processes also represent different steps in data value chain introduced in the next subchapter.

The data discussed in this thesis is often included in so-called Big Data. In literature, Big Data is often defined with 3Vs, i.e. volume, variety and velocity, where volume refers to the large amount of data, variety to its collection from multiple sources and velocity to the speed with which the data is processed and transferred.[39] Whether data is considered big or small does not have legal implications as there is no definition for Big Data under EU legislation. However, Big Data as a concept may clarify some of the characteristics of data and its economic value.

Typically data is stored in databases which Art. 1(2) of the Directive 96/9/EC of the European Parliament and of the Council of 11 March 199 on the legal protection of databases[40] (Database Directive) defines as a collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means. Thus database is collection of data that can carry information. Databases are often dynamic which means that their contents change.

The distinction between non-personal data and personal data can be found in the GDPR and the on the Free Flow of Non-Personal Data Regulation, as explained above. Another perspective top approach the issue is to look whether the data originates from a human being or, if there was a connection to a human being, whether the connection has been cut by the connection's remoteness. Tarkela parallels the discussion around the status of data derived from a human to the legal discussions regarding human tissue or cell samples.[41] For example, there are questions to whom the human originated substance should belong and to whom the information that has been acquired by processing the substance should belong to. [42] However, even from this angle, it is from a theoretical point of view fairly easy to make a straightforward distinction and define non-personal data as data that has not had or that does not anymore have connection to a human and cannot be relinked to an identifiable human. In practise, as stated in subchapter 1.2. the distinction may not be as clear-cut.

[38] Haider 2015 529-531.
[39] Brinch 2018 1591.
[40] OJ 27.3.1996 L 77/20.
[41] Tarkela 2016 2.3.
[42] Tarkela 2016 2.3.

2.2. Data-Value Chain

Lim & al. have suggested a theoretical framework for data-based value creation. [43] Their Data-Value Chain consists of nine steps within three areas: data collection, information creation and value creation.[44] (Figure 3) Within data collection area there are steps (1) data source; where data comes from and (2) data collection; how data is collected. On the border of data collection and information creation is step (3) data; what data is collected. The information creation area consists of step (4) data analysis; what information is distilled from the data and step (5) information on the data source, which also extends to the third area, value creation. Value creation area includes (6) the way information is delivered, (7) who the information is delivered to and (8) value in information use. Step (9) consists of the network of providers that are involved in the Data-Value-Chain as different steps may be performed by different actors. [45] The Data-Value Chain framework is later used in this thesis to understand how different legal practises affect the economic value creation.

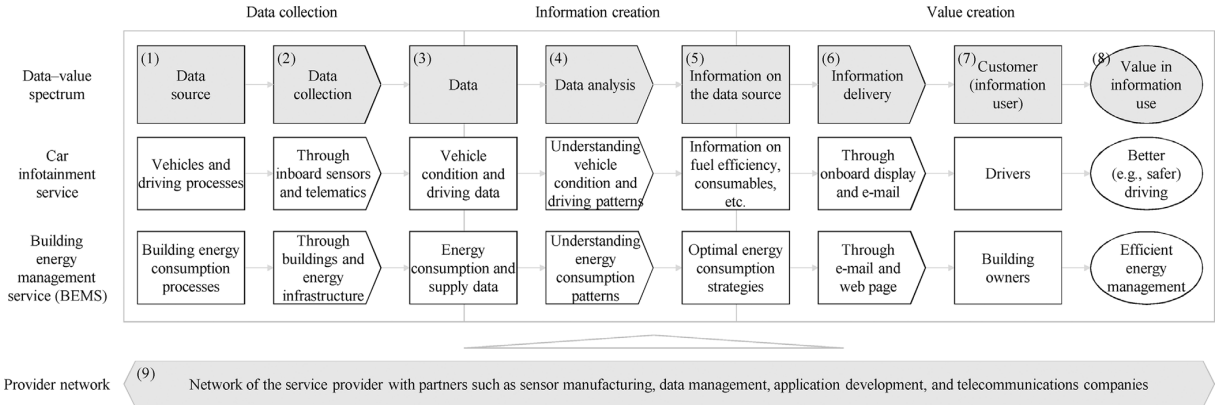

Figure 3 The Data-Value chain shows how value is created using data. Model and examples adapted from Lim et al.[46]

As explained in Figure 3, the Data-Value chain consists of different actors using different processes to process data via information into value. For example, when a building management service provider wishes to provide their customer (7), building owners, efficient energy management (8), they will start by collecting energy consumption data (3) from data source (1), building energy consumption process, through (2) data collection, from buildings and energy

[43] Lim et al.2018 125–126.
[44] The consept of value chain is well-established in economics and organizational studies litterature. See, for example Porter 1985 33–61.
[45] Lim et al.2018 125–126.
[46] Lim et al.2018 126.

infrastructure. The energy consumption data (3) will be processed through data analysis (4), for example using regression analysis to understand the energy consumption patterns, to information on the data source (5), in this case, optimal energy consumption strategies. This information has economical value and is then delivered (5) for example via email to the customer (7). Throughout the process a variety of service providers may be used, such as, sensor manufacturers, data management companies and telecommunication operators. On the other hand, all steps of the Data-Value Chain may be processed by one actor.[47]

It is important to note, that the relationships between different service providers are managed using legal and technical solutions. Thus legal issues arise at different steps of Data-Value chain. For example, in the above example, the building energy management service company A might buy or lease the sensors from sensor provider B that has contractual obligations with company C that developed the software for the sensors. Furthermore data analysis might be conducted by company D which then delivers the information to the building owner via company A's interface, devolved by application developer E. The legal and commercial relationships between the companies can easily grow quite complicated.

When analysing management of non-personal data between organizations, two directions must be considered. A value chain for data begins upstream as tangible devices and sensors record data and then moves downstream as nontangible data chain and a chain of material containing data. Writing about immaterial property rights, Godt has argued that downstream claims of "access" have made immaterial property rights more public while upstream immaterial property rights have become more linked to preceding rights over material and information.[48] Similarly in a value chain for data, the upstream actors, such as sensor providers, could try to secure rights on data. Likewise, downstream in the value chain end-users could try to claim access to data on the grounds that data does not exhaust or that they have a right to the data due to the data systems' physical components being located in their proximity or on the basis that access to data would further some justified interest of theirs.

It is also worth noting, that data value chain is not necessarily linear. Especially combined with efficient algorithms, the gathering and utilisation of data may create positive feedback loops.[49] For example, an automotive platform could harvest data and then, using its algorithms, optimise the data collected by the cars and use that data to develop the automotive platform to perform

[47] Lim et al.2018 125–126.
[48] Godt 2014 230.
[49] Ezrachi – Stucke 2016 238.

better. This could lead into the automotive platform in question becoming more popular compared to its competitors. This could then result in the platform having even more data available to develop its products. While this effect can have both positive and negative consequences, the ability to profit from the positive feedback loop is something that the actors within a data value-chain will try to position themselves into, assuming they aim at maximizing their profits, as is presumed in mainstream neoclassical economics.[50] This affects how non-personal data is managed between them.

Another issue regarding a value chain for data is that when there are multiple vertical actors involved, for example many data sources, there can be actors that may be understood as two-sided markets (multi-sided platforms). According to Hagiu and Wright multi-sided platforms enable direct interactions between two or more distinct sides whilst each side is affiliated with the platform.[51] This is important to note, as it means that in different data-value chains, different actors can have radically different business models, for example due to them being on different sides of the platforms.

The incentives for the parties in a data value chain can be studied using game theory approach. In game theory games are often divided into cooperative games, where cooperation between parties is only possible due to potential external enforcement such as contract law, and non-cooperative games where the co-operation must be self-enforcing.[52] A game theory-based study on decision game of data sharing in supply chain of one manufacturer and one retailer showed that as the parties have incentives to sell data to third-parties or provide the other party with camouflaged fake data, the cooperation does not easily result to a stable equilibrium due to, for example the changing value of data during the relationship.[53] The article shows that parties in a data sharing value chain cannot rely on self-enforcement but something external, such as contract law, is needed to stabilise the relationship. Regarding business partners within supply chains of more than two parties, Yu et al. have showed that information sharing can reduce the risks within supply chains and stabilise the cooperation in them.[54]

The findings of this chapter considering the characteristics of data, the complexity of data value chains and the different incentives for different actors demonstrate that the need for companies to manage non-personal data. The tools for this management will be presented in the following

[50] See for example, Wolff – Resnick 2012 88.
[51] Hagiu – Wright 2015 3.
[52] Zamir – Solan – Maschler 2013 xxv.
[53] Pan – Ma – Wu 2018.
[54] Yu – Yan –Cheng 2001.

chapters. Regarding indirect management in chapter 4 and regarding direct management through contracts in chapter 5. For example the conceptualisation of data can be argued as something not easily defined in contractual terms. However, in addition to the characteristics of data as an asset, the legislation affecting non-personal data needs to be considered, and that will be covered in the next chapter.

3. LEGAL ENVIRONMENT AROUND NON-PERSONAL DATA

As said, currently there is no (immaterial) property rights regime for non-personal data i.e., there are no *erga omnes* rights for non-personal data. However, non-personal data clearly can have, and often has, asset value. Non-personal data, or rather the right to get access to non-personal data and the right to preclude others from using that data can be viewed as entitlements as conceptualized by Calabresi and Melamed. Using their framework, different regulatory choices by the state (or in this case, also the EU) are their decisions on how to allocate these entitlements to different actors.[55] Even though Calabresi and Melamed do not frame it in such a way, their thinking on how the state may protect entitlements can be described as a three-step process (Figure 4). The first step is the decision on whether the state should or should not allocate entitlements. If the state chooses to allocate the entitlements, other steps follow, if not private actors are left free to create and manage those rights themselves.

In the second step, the state decides whether a right is alienable or inalienable or in other words, can a person decide to give up the right.[56] For example licensing one's computer software under a copyright regime would be possible, thus making such a copyright an alienable right. On the other hand, selling part of one's liver would be prohibited, and such transactions precluded from the markets and the 'right to one's liver' would hence be an inalienable right. While there is discussion on the implications of rights on data that is based on a human, e.g. her genomes, it is hard to imagine that non-personal data could be viewed as an inalienable right.[57]

In the third step, if the right is alienable, the state may enforce the rights by using a property rule or a liability rule and will have to make a regulatory choice considering which rules to use to protect the entitlements. Under a property rule, if a person wants to have another person's entitlement, they will have to come up with a voluntary agreement in order to get that entitlement. For example, they can buy or license the entitlement from the other party.[58] Property rules are protected by remedies such as injunction and replevin (getting back the object taken).[59] If on the other hand, an entitlement is protected by a liability rule, a person may take another person's entitlement from them or use their entitlement while having to pay an objectively determined price set by a court.[60] In practise, liability rules can mean remedies such

[55] Calabresi – Melamed 1972.
[56] Calabresi – Melamed 1972 1092–1093.
[57] Considering human originated data, see Tarkela 2016 4.3.
[58] Calabresi – Melamed 1972 1092.
[59] Schroedert 1999 413, 432.
[60] Calabresi – Melamed 1972 1092.

as damages. There can be both property rules and liability rules considering a certain entitlement, for example in trade secret law and copyright law both of which are presented later.

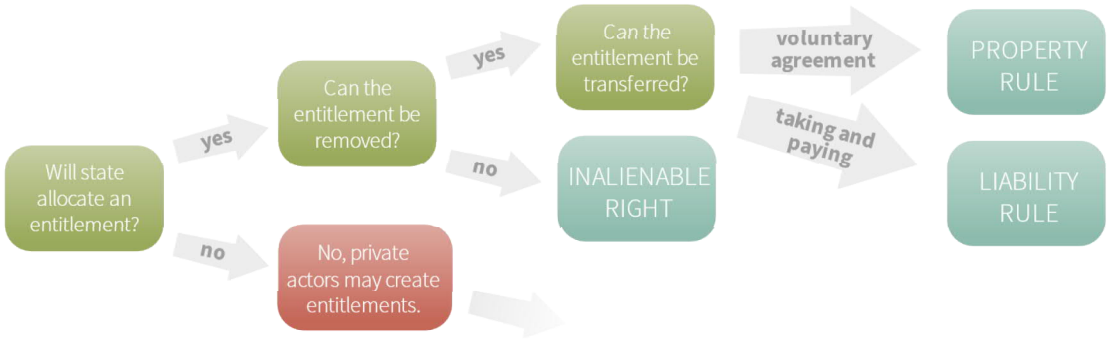

Figure 4 A decision tree showing options available to a state considering whether to allocate entitlements and which protective rules assign to the entitlements.

In this chapter, I will examine different regimes by asking whether the state (in this context, national or EU legislator) has allocated entitlements to private actors, and, if it has, what kind of entitlements have been allocated to them. I will use the framework suggested by Calabresi and Melamed in analysing these regimes from the viewpoint of managing non-personal data. Situation where entitlements have not been distributed by legislator / state and are now being created or distributed by private actors will be examined in chapters 4 and 5 regarding indirect management of non-personal data and direct management of rights to non-personal data.

Although business-to-government (B2G) data exchange is not in the focus of this thesis, possibilities and risks stemming from B2G data sharing affect how companies manage non-personal data and is a field that is among others developed by the Commission. For example, in January 2019 the Parliament, the Council and the Commission reached a political agreement regarding a new Directive on Open Data and Public Sector Information (PSI) Directive that provides rules for the availability and re-use of public sector data.[61] The agreed directive would replace Directive 2013/37/EU of the European Parliament and of the Council of 26 June 2013 amending Directive 2003/98/EC on the re-use of public sector information.[62] From viewpoint of companies, public data can offer possibilities to access data that they otherwise would not have resources for.[63]

[61] IP/19/525, 2019.
[62] OJ 27.6.2013 L 175.
[63] Regarding B2G data sharing, see for example COM(2018) 232 Final. 12–14.

3.1. Trade Secrets Directive

The European Union's recently introduced Trade Secrets Directive has been seen by some as a regime that could create specific rights on data and prevent unauthorised third-party access to data.[64] The Directive aims to lay down rules on the protection against the unlawful acquisition, use and disclosure of trade secrets. According to Art. 2(1) of the Directive, trade secret is information which meets all of the following requirements: (a) it is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question; (b) it has commercial value because it is secret; (c) it has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.

I will first address the Trade Secrets Directive's ability to preclude a cooperative party from having rights to data in a data exchange relationship and secondly consider the Directive's ability to protect data from third-party access.

If we look for example a scenario where a company has installed its sensor at other party's (end-users) facility, all these requirements could be interpreted in one way or the other. Regarding the requirement of generally known or readily accessible, it can be argued that for example the end-user company would have general knowledge or readily access to the data, but they have chosen to access the data by using the sensor-providers product. When it comes to the constraint of commercial value based on secrecy, there are two issues in relation to non-personal data. Firstly, the data is a recording of an actual event and that would have had to been kept secret as well. Secondly, it can be argued that the value of data is not built on secrecy but on sharing and refining the data. Concerning the third requirement, the data stored itself may have been subject to reasonable steps to keep it secret but once again, the question is whether the original event has been subject to secrecy.[65]

Trade Secrets Directive also has effects on third-party use of trade secrets as provided by Art. 4(4) of the Directive: the acquisition, use or disclosure of a trade secret shall also be considered unlawful whenever a person, at the time of the acquisition, use or disclosure, knew or ought, under the circumstances, to have known that the trade secret had been obtained directly or indirectly from another person who was using or disclosing the trade secret unlawfully as

[64] Osborne Clarke LLP 2016 10; Riva 2018.
[65] Drexl et al. 2016 7.

defined in the directive. Regarding third party access, situation is somewhat similar. If the information is publicly accessible the requirement of secrecy is not fulfilled. Often, the individual data items are also not as such commercially valuable. [66] If data itself has not any information value as such but still carries information, is there any way to claim it is a trade secret?

The Directive does not aim primarily at addressing data economy.[67] Based on the language of its preambles, the Directive was not originally meant for unstructured data, at least not when it is a mere recording of events. For example preamble 1 of the Trade Secrets Directive states that trade secrets consist of know-how and business information. Neither does the Directive aim at affecting the application of any other relevant law in areas including intellectual property rights and the law of contract, as provided in its preamble 39.

According to preamble 2, companies value a diverse range of information as trade secrets; information that extends beyond technological knowledge to commercial data such as information on customers and suppliers, business plans, and market research and strategies. Even though the word data is used, its use implies that it is used in a meaning that more resembles information on the *data-information-knowledge* continuum. The Directive's preamble 16 clearly states that in the interest of innovation and to foster competition, the provisions of this Directive should not create any exclusive right to know-how or information protected as trade secrets. Thus, the independent discovery of the same know-how or information should remain possible. To make an aggravating example, non-personal data about the weather could not be secret even if a company would try to keep the recorded data secret by taking precautions as the event itself is freely observable by everyone.

Moreover, the Directive openly permits the acquisitions of trade secrets through reverse engineering. According to Art. 3(1b), observation, study, disassembly or testing of a product or object that has been made available to the public or that is lawfully in the possession of the acquirer of the information is free from any legally valid duty to limit the acquisition of the trade secret. This makes data that is inside publicly available devices even more difficult to protect by relying on Trade Secrets Directive. As noted in the OAD report, if the number of products with the data is small, for example in case of industrial devices, the problem can be mitigated with contractual arrangements.[68]

---

[66] Drexl et al. 2016 7.
[67] Drexl et al. 2016 7.
[68] Osborne Clarke LLP 2016 12.

However, there have been arguments that trade secret law could protect some data, especially as part of a database or data sets.[69] These databases would of course have to fulfil the criteria of the Trade Secrets Directive. It is possible that the protection offered by Trade Secrets Directive will apply to some databases and perhaps even to some data. But especially when the data is collected by a party that is not physically located at the place of the data collection, it is hard to see how, for example a sensor-provider could claim that something is a secret just because they have collected data about some event that has occurred in a space that is not secret as such or that belongs to another actor, not the sensor-provider. Regarding the interpretation of the Directive, the role of the Court of Justice of the European Union will be crucial since the Trade Secrets Directive remains ambiguous until the Court will provide case law.[70]

If Trade Secrets Directive and its national implementations protect some data, the law would allocate entitlements to the trade secret protected data. The remedies protecting such data would be both property rules (Art. 12 injunctions and corrective measures) and liability rules (Art 14. damages). As noted in the OAD report, the remedies could be hard to enforce in practise, if the data has been disclosed for example on the Internet and many third-parties have potentially accessed it.[71] As the trade secret protected data covered by these property and liability rules can be licensed by companies, it could offer market actors with options to rely on the said remedies in case their contracting parties or third-parties would misuse the data. Regarding remedies, it is noteworthy that the EU legislator tried to keep remedies of Trade Secrets Directive separated from remedies stipulated in Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights[72], as specified in recital 39 of Trade Secrets Directive.

3.2. Copyright and Database *sui generis* Protection

Copyright

Copyright is legislated partly on EU and partly on national level. However, different copyright regimes have grown more similar due to international agreements such as the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) and introduced EU legislation. Copyright protection covers only works which data cannot be at this structuration level on the Data-Value chain. As Art. 9(2) of the TRIPS agreement provides, copyright protection extends

[69] Drexl et al. 2016 7–8.
[70] Osborne Clarke LLP 2016 10.
[71] Osborne Clarke LLP 2016 12.
[72] OJ 30.4.2004 L 157.

to expressions but not to ideas, procedures, methods of operation or mathematical concepts as such. There is a minimum standard of author's own intellectual creation that need to be surpassed if information or data is to be considered as work.[73] As the object of copyright protection is different, copyright protection does not seem well-suited for data, especially machine-generated.

Furthermore, most data is collected by machines, for example, in an industrial Internet of Things setting. Consequently, in addition to the criterion of work, the criterion of author should be fulfilled. While there is discussion about the possibility of works attributed to machine-learning algorithms, the authority criterion does not make it easier for data to qualify as copyrightable.[74] Currently, there is no case law suggesting that automatically collected data could be protected under copyright.[75] Due to these arguments, the copyright protection of individual data items is not further discussed in this thesis.

Considering collections of data, databases, the situation is different. The copyright of databases is specifically addressed in Chapter II of the Database Directive. Art. 3(1) of the Directive provides that those databases which, by reason of the selection or arrangement of their contents, constitute the author's own intellectual creation shall be protected as such by copyright. The Directive's Art. 3(2) clarifies that copyright protection of databases provided does not extend to their contents and shall be without prejudice to any rights subsisting in those contents themselves. Therefore, even if a database is subject to copyright, the data items are not.

In *Football DataCo v Yahoo* the Court of Justice of the European Union held that even if setting up a database contains significant labour and skill of its author, copyright protection is not justified, if that labour and that skill do not express any originality in the selection or arrangement of that data.[76] The judgement seems to further ascertain that the threshold for originality is not reached without substantial creativity that especially machine-generated data, even as part of databases, can hardly cross.

Another question is, whether the technology used to collect, store and transfer data would be subject to immaterial property rights such as copyright, and in some case for example patents. This question will be briefly discussed in chapter 4 regarding indirect management of non-personal data.

---

[73] Osborne Clarke LLP 2016 13.
[74] Regarding the discussion whether works by AI should fall under copyright, see for example Guadamuz.
[75] Osborne Clarke LLP 2016 13.
[76] C-604/10, *Football DataCo v Yahoo,* EU:C:2012:115, paragraph 42.

Sui generis database right

In addition to copyright, the Database Directive establishes a *sui generis* database right in its Chapter III. Database directive is generally seen as unsuitable for protecting data items, for example based on its conceptualisation for database and its structure, not individual data items.[77] Furthermore, the protection of individual database contents was agreed to be excluded when the Directive was introduced.[78] The substance of the *sui generis* right and some EUCJ case law is, however, briefly explained to establish an understanding whether the Directive could have effects on management of non-personal data. According to the Art. 7(1) of the Directive, Member States shall provide for a right for the maker of a database which shows that there has been qualitatively and/or quantitatively a substantial investment in either the obtaining, verification or presentation of the contents to prevent extraction and/or re-utilization of the whole or of a substantial part, evaluated qualitatively and/or quantitatively, of the contents of that database.

The substantial investment, mentioned in Art. 7(1) of the Directive, must be in producing the database, not in producing the activity from which the valuable data is recorded.[79] Often, in a data value chain, the activity itself (for example an industrial process) is costly, but the investment of the database is not substantial. The Court of Justice of the European Union has addressed the issue in its case law. In *British Horseracing Board v William Hill* the Court held that the investment in the obtaining of the contents of a database in Art. 7(1) of the Directive refers to the resources used to seek out existing independent materials and collecting them in the database and that does not cover the resources used for the creation of materials which make up the contents of a database. Similarly, investment in the verification of the contents does not cover resources used for verification during the stage of creation of materials which are subsequently collected in a database.[80] In subsequent *Fixtures marketing* cases the Court affirmed its position.[81] The case law can be viewed as the EUCJ's attempt to incentivise creating databases from information that exists, not from gathering new data from real-world events that have not been previously recorded.[82]

---

[77] Drexl et al. 2016 4.
[78] Drexl et al. 2016 4.
[79] Osborne Clarke LLP 2016 14.
[80] C-203/02, *British Horseracing Board Ltd & Others v. William Hill Organization Ltd*, EU:C:2004:695, paragraph 42.
[81] C-46/02*, Fixtures Marketing Ltd v. Oy Veikkaus AB*, EU:C:2004:694; C-338/02, *Fixtures Marketing Ltd v. Svenska Spel AB*, EU:C:2004:696; C-444/02, *Fixtures Marketing Ltd v. Organismos Prognostikon Agonon Podosfairou*, EU:C:2004:697.
[82] Drexl et al. 2016 4.

According to Art. 7(2), extraction means permanent or temporary transfer of all or a substantial part of the contents of a database to another medium by any means or in any form. Re-utilization means any form of making available to the public all or a substantial part of the contents of a database. The EUCJ clarified that expression 'substantial part' in *British Horseracing Board v William Hill*, holding that substantial part refers to the scale of the investment of the subject of the act of extraction and/or reutilisation, regardless of whether that subject represents a quantitively substantial part of the contents of the protected database.[83] It is also noteworthy, that according to the Article, the first sale of a copy of a database within the Community by the right holder or with his consent shall exhaust the right to control resale of that copy within the Community. This further weakens the Directive's ability to prevent distribution of data once a database containing it has been sold.

Furthermore, according to Art. 8(1) of the Directive, the maker of a database which is made available to the public in whatever manner may not prevent a lawful user of the database from extracting and/or re-utilizing insubstantial parts of its contents, evaluated qualitatively and/or quantitatively, for any purposes whatsoever. Regarding this article, the question on what constitutes insubstantial part, is crucial, and the EUCJ clarified the expression in *British Horseracing Board v William Hill* stating that any part which does not fulfil the definition of a substantial part, evaluated both quantitatively and qualitatively, falls within the definition of an insubstantial part of the contents of a database.[84]

In addition, Art. 8(2) of the Database Directive provides that a lawful user of a database which is made available to the public in whatever manner may not perform acts which conflict with normal exploitation of the database or unreasonably prejudice the legitimate interests of the maker of the database. In *British Horseracing Board v William Hill,* the EUCJ held that actions described in Art.8(2) could be unauthorised actions for the purpose of reconstituting, through the cumulative effect of acts of extraction and/or re-utilization of whole or a substantial part of the contents of a database protected by the *sui generis* right.[85] Furthermore, according to Art. 8(3) a lawful user of a database which is made available to the public in any manner may not cause prejudice to the holder of a copyright or related right in respect of the works or subject matter contained in the database.

---

[83] C-203/02, *British Horseracing Board Ltd & Others v. William Hill Organization Ltd*, EU:C:2004:695, paragraph 82.
[84] C-203/02, *British Horseracing Board Ltd & Others v. William Hill Organization Ltd*, EU:C:2004:695, paragraph 73.
[85] C-203/02, *British Horseracing Board Ltd & Others v. William Hill Organization Ltd*, EU:C:2004:695, paragraph 89.

In practise, the database *sui generis* right has not been proven to have the effects it was enacted for. The Commission's latest evaluation of the Directive concludes that the *sui generis* right has not been shown to stimulate investments in database nor create an effective access regime.[86] The OAD Report points out that the current case law of the EUCJ and especially its interpretation of investment being linked to the creation of database itself, instead of the activity data records, may be subject to discussion when the automatically generated databases become more valuable.[87] For example the Max Plant Institute argued that the *sui generis* protection of databases should not be expanded or reinterpreted to grant exclusive rights in individual data items and held such developments unnecessary and unjustified.[88]

From a company's point of view the database *sui generis* right and the protection offered to the right could be seen as falling to the same category as criminal law. By this I mean that it might provide a kind of backstop to exploitation of database that is not normal within the meaning of Art. 8(2). While this would not protect individual data items, it at least protects companies from, for example, their competitors extracting the whole database. However, database *sui generis* right's practical usefulness is limited, since if database is used within the limits of the Directive's Art. 8, and the data is extracted to another database and then transferred to a third-party, database right would offer no protection against such behaviour.

If the backstop function of database *sui generis* right or other possible situations where database *sui generis* right would apply to non-personal database, the remedies could be of both types, liability rules and property rules. While Art. 12 of the Directive leaves providing appropriate remedies to Member States, for example the Finnish Copyright Act (404/1961) provides under its Section 56a holders of database *sui generis* right similar protection as those offered to copyright holders (prohibition to infringe [56g], compensation and renumeration [57]).

Unlike other immaterial property rights, the *sui generis* database right does not similarly have its basis in international agreements and thus does not exist in the US markets, for example. For companies managing rights to non-personal data in an international context, this issue is something to be considered.[89]

---

[86] SWD(2018) 146 Final. 2018 46.
[87] Osborne Clarke LLP 2016 14.
[88] Drexl et al. 2016 3.
[89] Similar regimes have been introduced in Japan and South Korea. See OECD 2015, 190.

3.3. Framework for the Free Flow of Non-Personal Data Regulation

According to Art. 1 of the Framework on the Free-Flow of Non-Personal Data Regulation, the Regulation aims to ensure the free flow of data other than personal data within the Union by laying down rules relating to data localisation requirements, availability of data to competent authorities and porting of data for professional users. The Regulation aims at supporting the creation of a competitive data economy within the internal market.[90] As already explained in subchapter 1.1, the distinction between non-personal and personal data may not be as clear-cut as suggested by the Free-Flow of Non-Personal Data Regulation and this must be regarded in when interpreting the Regulation.

Rules prohibiting data localisation are introduced in Art. 4 of the Regulation. According to Art. 4(1) data localisation requirements are prohibited, unless they are justified on grounds of public security in compliance with the principle of proportionality. Art. 4(4) intensifies the prohibition by providing that Member States shall make the details of any data localisation requirements laid down in a law, regulation or administrative provision of a general nature and applicable in their territory publicly available via a national online single information point. For companies, the framework set by these rules provides opportunity to move data across national borders more freely and to learn about the remaining data localisation requirements through the national online single information points. The Regulation's data localisation rules provide an example of an inalienable right meant by Calabresi and Melamed, but here the inalienability in a way requires the decision of both national and EU legislator, as the data must fall within the specification of both EU legislator and Member State authorities. The Regulation allows the government to hold data carrying certain information inalienable, as long as that information considers, for example military, secrets or other public security information, in compliance with the principle of proportionality, as stipulated in its Art. 4. (1).

The Free-Flow of Non-Personal Data Regulation ascertains data availability for competent authorities. According to its Art. 5(1), the Regulation shall not affect the powers of competent authorities to request, or obtain, access to data for the performance of their official duties in accordance with Union or national law. Access to data by competent authorities may not be refused on the basis that the data is processed in another Member State. Art. 5(4) provides Member States with the ability to impose effective, proportionate and dissuasive penalties for failure to comply with an obligation to provide data, in accordance with Union and national

[90] IP/18/4227, 2018.

law. From point of view of companies, these data availability provisions are obligations to provide data and, as such, need to be regarded if operating in market segments where authorities might have a right to access data.

For management of rights to non-personal data, the most important provision of the Regulation may turn out to be its Art. 6, regarding porting of data. According to the Article, the Commission shall encourage and facilitate the development of self-regulatory codes of conduct at Union level, in order to contribute to a competitive data economy, based on the principles of transparency and interoperability and taking due account of open standards. The Article further stipulates that codes of conduct shall be developed for best practices for facilitating the switching of service providers and the porting of data, minimum information requirements for professional users before concluding contracts and approaches to certification schemes that facilitate compression of data processing products and services. For example, codes of conduct facilitating the switching of service providers might prevent vendor lock-ins, situations where a customer is so reliant on a vendor's products or services that it cannot move to another vendor without costs and technical difficulties.[91] Art. 6.2 requires the Commission to make sure that all relevant stakeholders, such as associations for SMEs and start-ups, users and cloud service providers participate in developing the codes of conduct.

The codes of conducts have a possibility to produce innovative rules. On the other hand, if field of non-personal data is compared to fields of, for example, personal data or intellectual property law there are (at least not yet) similarly situated big platforms. That could make the non-binding agreements quite different to the ones seen in, for example, the field of copyright and trade mark rights where the non-binding regulation has been conducted through Internet platforms.[92] But markets could evolve and change so that there would be bigger non-personal data related players.

From the viewpoint of this thesis, the most important rules are probably the vendor lock-in rules. These will probably guide market practice towards more open vendor-customer data practices, and it could be beneficial to take into account these considerations even now. On the other hand, those companies, for example SMEs, who are trying to get access to data could benefit from the new rules. Some big actors might lose ability to gain some market power or maybe the legislation will hinder the development of such big players.

---

[91] Toosi – Calheiros – Buyya 2014 7.
[92] Regarding non-binding agreeements and trademarks, see Tusikov 2016.

The Free Flow of Non-Personal Data Regulation naturally does not provide for any remedies for not complying with the non-binding code of conducts. Perhaps most significant is what the regulation does not cover. The enaction of the Regulation could have been a possibility for the EU to make different regulatory choices. The fact that the regulation was adapted implies that at least now EU is not going to implement more regulation regarding non-personal data, for example regarding property regimes. The regulation does not provide rules regarding third-party access to data, as the ability of non-binding agreements to create effect on third parties is very limited. At most, they may provide a market practice, which, if not followed, might exclude the non-compliant companies from data markets. Their another effect could be to reduce the transaction costs involved in data licensing. This could indeed have positive effect on data-driven economy, especially for smaller players.

Looking at the Free Flow of Non-Personal Data Regulation, excluding provisions restricting data localisation, from point of view of Calabresi and Melamed's framework, it could be argued that through the Regulation, the legislator has softly allocated entitlements to non-personal data or that the entitlements are in a transitional stage. In the transitional stage, the entitlements have a potential to become strictly allocated in the future or to remind flexible.

3.4. Criminal Law

Criminal law provides some limits to third-party use of non-personal data. For example, according to the Art. 6 of the Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, Member States shall take the necessary measures to ensure that intercepting, by technical means, non-public transmissions of computer data to, from or within an information system, including electromagnetic emissions from an information system carrying such computer data, intentionally and without right, is punishable as a criminal offence, at least for cases which are not minor. The provision is implemented in the national legislation of Member States in their penal codes and can be seen as a backstop that prevents data anarchy, totally uncontrolled use of data other people has legitimate interests in.

The OAD report addresses the criminal law systems of England and Wales, France, Germany and Spain. [93] In the UK, the courts have held, for example in *Oxford v. Moss*[94] case, that as data is not property, it cannot be stolen. In French case law, the *Cour de cassation* (Supreme Court) held in its decision that downloading of data without their owner's consent, which the defendant knew to be protected, constituted a theft.[95] In Germany, some scholars are arguing that, based on criminal law data can be owned while others view that this does not constitute ownership.[96] In Spain, there has not been too much discussion considering data and criminal law from a point of view other than trade secret protection.[97]

The situation is somewhat interesting, since civil law has no property rights regimes for data, but criminal law still provides protection from interception of data with the condition of lack of right of interception. It is as if river water was owned by none, but still if somebody started to intercept water and then another person started to collect that water too without right would be sanctioned under criminal law. To my understanding the criminalization on intercepting of data means, that the right to computer data means a right to have access to a system with the said computer data. Thus, such legislation does not concern the interception of data *per se*, but some of the practices, how data is accessed through different means. This is close to the technical practises of indirect management of non-personal data, a subject which will be covered in subchapter 4.2.

Here, I cannot go in to the detail regarding the usefulness of criminal law as a tool to manage non-personal data, but there are many questions that should be answered to. These questions include, for example, how effective criminal law is able to decide which private person should belongs to or what kind of transaction costs arise when questions regarding who data belongs to are subjected to a criminal law process.

Entitlements regarding non-personal data, can be seen in two ways. Firstly, as property rules protecting data as a property. Secondly and perhaps more validly criminal law can be seen as creating an inalienable right by prohibiting certain behaviour of the perpetrator or looked from the victim's viewpoint, an entitlement to be protected against certain behaviour by state. This points out that criminal law focuses more on the behaviour of perpetrator than on the object

---

[93] Osborne Clarke LLP 2016 30, 45.
[94] (1979) 68 Cr App Rep 183. The English case is quite old and from analogue age. Courts in another common law jurisdiction, New Zeland, have found otherwise. This could indicate that the case law could change also in the UK. See, Ken – Carter 2015.
[95] Cour de cassation, criminal chamber, published 20 May 2015, N°: 14-81336, FR:CCASS:2015:CR01566.
[96] Osborne Clarke LLP 2016 60–61.
[97] Osborne Clarke LLP 2016 70–71.

matter of the crime.[98] Also, as criminal law could be considered to be a way for the state to regulate its use of its monopoly of violence[99], criminal law might be an inflexible means to solve issues regarding unauthorised use of data between private parties.

Use of criminal law to protect data would not solve issues considering how data misuse can be proven. Actually the level of proof required is higher than it is in civil litigations, as for example under English criminal process, charges have to be proved beyond reasonable doubt whereas in civil processes the requirement is proof based on the balance of probabilities.[100] Furthermore, from a company's point of view criminal law is slow in data-driven economy and standpoint of criminal law is always *ex post*. In an international context the jurisdiction of different authorities and courts would need to be taken into consideration. These conditions do not make criminal law suitable for managing non-personal data.

3.5. Competition Law

Companies may gain market power by collecting and getting access to data, particularly when potential competitors do not have the same ability.[101] In some cases, the market power and the company's actions could cross the threshold of competition law aims at balancing the market power of different companies within a market. Competition law is enforced by EU and national authorities based on competition legislation. The legal grounds for competition law are found in Articles 101 and 102 of the Treaty on the Functioning of European Union (TFEU)[102].

One of the competition law doctrines that could affect the management of non-personal data is the essential facilities doctrine. The doctrine refers to a situation where an undertaking in dominant position has an essential facility and uses the facility itself while refusing other companies access to it without objective justification or only allows access based on less favorable terms than it gives its own services.[103] The Commission Directorate-General GROW (Internal Market, Industry, Entrepreneurship and SMEs) has suggested enforcing competition law based on the essential facilities doctrine as one possible option to deal with market abuses preventing access to data.[104]

---

[98] Binder 2016 1.
[99] Binder 2016 2.
[100] See for examle, Law 2018.
[101] Drexl et al. 2016 10; Autorité de la Concurrence and Bundeskartellamt 2016 11–12.
[102] OJ 26.10.2012 C 326.
[103] See for example, OJ 18.1.1994 L 15, 94/19/EC: Commission Decision of 21 December 1993 relating to a proceeding pursuant to Article 86 of the EC Treaty (IV/34.689 - Sea Containers v. Stena Sealink - Interim measures), para. 66.
[104] König 2016 6.

Access to data could be an exceptional remedy under Art. 102 TFEU, but the access would always be granted *ex post*.[105] Since competition law processes can take years, which compared to the dynamics of data collection and utilization in the Internet of Things is substantially long time, it is unlikely that competition law could provide dynamic access to data in its current form. At least from the viewpoint of human and fundamental rights, what makes sharing non-personal data more plausible, is that, regarding non-personal data, there are no similar concerns as to the sharing of personal data collected by personal data intense companies where data privacy and the right to privacy must be considered. Therefore, competition law could in some instances provide access to data for companies that have less market power due to them not having access to non-personal data.

On the other hand, even if the risk may be low, companies should not forget competition law regarding data. As the value of data has been noticed by competition authorities[106], companies should make sure that their non-personal data management practises do not violate competition law provisions. Especially, when declining to share data or using closed technical solutions to restrict new entrants from using data, while having substantial market power there could be competition law issues to consider.

As the role of competition law is based on *ex post* analysis, its relevance to this thesis is limited and not discussed much further. If competition law is seen as a tool to grant access rights to actors with little market power, more flexible remedies would have to be introduced which would be a radical change to current competition law policies.

3.6. Reflections

In 2017 Commission Staff Working Document, a data producer's right for non-personal or anonymised data, was envisioned as one legislative approach. The data producer's right could have been a right *in rem* enforceable against third-parties and given the data producer an exclusive right to utilise and license certain data. Another alternative could have been a purely defensive right which could have given data holders right to protect their data from third-parties in a similar fashion to Trade Secrets Directive. Remedies, such as right to seek injunctions that would have prevented third-party use of data or injunction to prevent products built on basis of misappropriated data, were suggested as possible regulatory approaches.[107]

---

[105] Drexl et al. 2016 9–10.
[106] See, Autorité de la Concurrence and Bundeskartellamt 2016.
[107] SWD(2017) 2 Final. 2017.

In the end, the data producer's right was not introduced, and the Free-Flow of non-personal Data Regulation was chosen as legislative approach instead, and, there are no current plans for *sui generis* rights for data within the EU. However, as the previous subchapters have provided, there are multiple legal regimes that affect the management of non-personal data in companies. Still from view point of management of non-personal data, there are uncertainties both within and between national legal systems and at the EU level.

If some data would have some kind of protection under an immaterial property right or under another regime presented in this chapter, there would still be considerable issues regarding evidencing misuse of data. In practise, it would be difficult for an allegedly infringed party to provide evidence that another party has used the specific data items that is subject to the allegedly infringed party's rights. This is due to the characteristics of data presented in the previous chapter, for example the moldability of data and its ability to be refined which would make the object matter of the rights difficult to grasp, especially in litigation. Also, for similar reasons, and for the fact that the value of data depends on many factors, the value of damages could be hard to show if a company managed to prove that their rights have been breached.

An interesting issue to study could be whether fundamental or human rights could have implication on managing non-personal data. In references to this chapter, there have been no arguments for such implications.[108] As non-personal data is quite far or totally removed from humans, it could be hard to define to whom, to which particular human beings, fundamental rights would create entitlements relating to non-personal data. Should for example owner of a machine have right to the data produced by the machine based on certain human or fundamental rights? The issue was brought up, for example in the incident referred at the vey beginning of this work where farmers argued that they had right to data that the tractors they own produce.[109] The issue could be approached similarly to Godt's analysis of fundamental rights based on upstream and downstream claims. Upstream, issues such as should tractor owners have right to the data produced by their tractor could be examined. Downstream, questions such as, what interests, e.g. right to health, could create a right to access data that is in somebody else's possession, could be asked.[110] The question is out of the scope of the thesis but interesting topic for research.

---

[108] Though, in the explanatory memorandum accompaning the proposal for a regulation on free flow of non-personal data, the proposed regulation was argued to have positive impact on the freedom to conduct a business. COM(2017) 495 Final. 2017 8.
[109] Charles 2014.
[110] Godt 2014.

Considering possible future legislation, it is important to note that Art. 118 of the TFEU provides that in the context of the establishment and functioning of the internal market, the European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall establish measures for the creation of European intellectual property rights to provide uniform protection of intellectual property rights throughout the Union and for the setting up of centralised Union-wide authorisation, coordination and supervision arrangements. Though the Free-Flow of Non-Personal Data Regulation was adopted in accordance with Art. 114 (establishing and functioning of the internal market), Art. 118 would grant the European Union right to create intellectual property rights to non-personal data. As there were some inconsistencies, for example, in Member States' criminal law systems considering data, EU level legislation might be useful in order to secure the functioning of the internal market when the importance of data-driven economy grows.

For companies managing rights to non-personal data, legal certainty is desirable. If the EUCJ for example started to interpret the Database Directive differently, stepping aside from its established case law to include individual data items, it would change the law surprisingly. A similar position has been indicated by the Max Planck institute.[111] Regarding Trade Secrets Directive and Free-Flow of Non-Personal Data Regulation, companies are left to wait for case law or the non-binding codes of conducts to learn how these pieces of legislations are interpreted and what their actual effect will be.

After getting to know the legal environment around non-personal data, the next chapter will introduce how non-personal data can be managed indirectly. In indirect management of non-personal data, the legal environment forms part of the overall environment surrounding non-personal data which in addition to legal factors consist of physical, technical and societal aspects.

[111] Drexl et al. 2016 3.

4. MANAGING NON-PERSONAL DATA INDIRECTLY

According to Calabrasi and Melamed, when two or more people or groups of people have conflicting interests the state must decide whom to favour. Otherwise, they claim, the conflict will be decided on 'might makes right' basis.[112] Regarding traditional conflicts of interests such as, who gets to use a certain piece of land, or, who a barrel of wheat belongs to, violence could be a potential way to solve these conflicts. However, regarding assets such as non-personal data, 'might' or rather power looks quite different compared to violence and is achieved through different technical, legal and business practices. I call practises establishing this power indirect management of non-personal data since the rights and obligations or physical or virtual parameters are attached to something else than to the data itself. In a way, data is managed by channelling the data using technical, legal or business practises. To put it in other words, indirect management of non-personal data is getting leverage over other actors by implementing practises that prevent others from accessing data or provide the actor in question with access to data.

Combination of legal and technical solutions to achieve certain economic goals is not a new phenomenon in law. For example, traditionally in property law, there have been arrangements where a pledge has been verified by locking up an object and the depositing the key to the pledgee.[113] To manage non-personal data technical and legal aspects can be combined in a similar, albeit digital way. To make a simple example, an original equipment manufacturer (OEM) for an automotive manufacturer could protect their data collecting sensor in a car by a technical solution so that the sensor would send all data to the OEM while the car's manufacturer or user would only receive part of the data as processed information. This way the OEM could try to gain competitive advantage by having more data to use in its research and development activities.

Two actors have been suggested to be best positioned to manage (non-personal) data indirectly. The Commission has identified the manufacturers of Internet of Things object to be privileged in determining who can access and use data generated by such objects.[114] When these Internet of Things objects are built within complicated supply-chains, the question arises, who is the manufacturer of the object, as illustrated by automotive OEM example above. On the other hand, Seppälä et al. have suggested that naturally the owner of the device or service has the

[112] Calabresi – Melamed 1972 1090.
[113] See for example, Tammi-Salminen 2015 271.
[114] COM(2018) 232 Final. 9.

capacity to manage data when there are no contractual arrangements.[115] I am critical to the suggestion that a scenario without contracts is a natural start point for Internet of Things objects and data, as there are relatively many factors affecting the relationships between actors as can be seen in ithe Data-Value Chain described in chapter 2.2. However, the two premises presented suggest to me that no actor has a natural ability to manage non-personal data. Rather, that ability is a combination of technical, legal and business practices that the companies seize and use.

In this chapter, I will start by having a look at different relationships in data markets. Then, I will introduce the different practises, by first introducing technical practises, then legal practises and finally business practises, for factual management of non-personal data. In each of the subchapters, I will first focus on practises within the dyadic relationship of two parties. After that, I will provide insights on how factual management could be used to solve the problem of unauthorized third-parties accessing and using data.

4.1. Roles and Relationships in Data Markets

There are several different roles and relationships between companies regarding sharing of data which I try to map out here in order to better understand the issues that indirect and direct management of non-personal data face. The several different roles companies can have in data economy can be conceptualized in several ways. For example, Krönke has mapped the shareholders of data from a point of view of smart (Internet of Things) objects and divided the shareholders to owner, user, manufacturer, third parties, and governmental authorities.[116] Due to its centring around smart objects, Krönke's breakdown can be argued to neglect some parts of the Data-Value Chain, especially what happens after the data has been collected from the sensors.

A Staff Working Document by Commission approaches the issue of data relations by introducing three different business models, an open data approach, data monetisation on a data marketplace and data exchange in a closed platform, the choice between which depends on type of data and strategical choices. Open data approach is a model where data supplier makes data available to an open range of users. Monetisation of data on a data platform refers to a model where data providers sell their data to data users through an intermediary, using bilateral contracts. Data exchange on a closed platform refers to a scenario where either one central data provider or user or an independent intermediary sets up a data platform where data is exchanged

[115] Seppälä – Juhanko – Mattila 2018 3.
[116] Krönke 2018 369–371.

for monetary compensation or value-added services.[117] From the Commissions approach, the roles of data supplier, data user and intermediary can be distilled. Importantly, same actors can hold many of these roles and there may be different level data providers, for example, if a data user also provides data downstream to other data users.

Building on Krönke's and the Commission's approach and the Data-Value Chain presented in chapter 2.2, I will approach the relationships by first defining the following roles 1) sensor base possessor 2) sensor provider, 3) data platform provider or integrator 4) user of data. Compared to the Data-Value Chain, all of these roles fall within data collection phase. By sensor base possessor, I mean, for example, a car owner whose engine contains a sensor, in other words, the sensors base (where the sensor is physically located and installed) belongs to the car owner. Possession needs not equate ownership but can in addition be, for example, leasing or other arrangements. By sensor provider, I mean the actor who has manufactured and provided the sensor and for example, could have had the possibility to design the software of the sensor. By data platform-provider I mean a data provider, data user or independent intermediary who is legally or technically positioned to control how data flows from a sensor to data user. By data user, I mean an actor who uses the data and through data analysis provides information based on the data and then in one way or another shares the information forwards.

One actor can hold one or more of these different roles, even all. Since specialization often leads to more efficient operations different companies will often perform their distinct roles in the data value chain. This on the other hand leads to different data relationships which the parties will try to manage with contract law, such as:

1) Sensor base possessor → Sensor-provider → Data user, or
2) Sensor-provider → Sensor base possessor → Data Platform provider → Data user → Sensor base possessor.

Using this terminology, for example the Commission data business models could be described easily. In open data approach, data platform receives data from sensor providers or sensor base provers and shares it to an open set of data users. In the monetisation model, data platform provider licenses data from sensor-providers and then licenses data to data users for monetary compensation. Furthermore, these roles do not take a stand on whether the parties act lawfully or have contractual arrangements. Thus a data user, for example, may be a third-party receiving data without sensor-providers permission from another data user.

---

[117] SWD(2018) 125 Final. 2018 5.

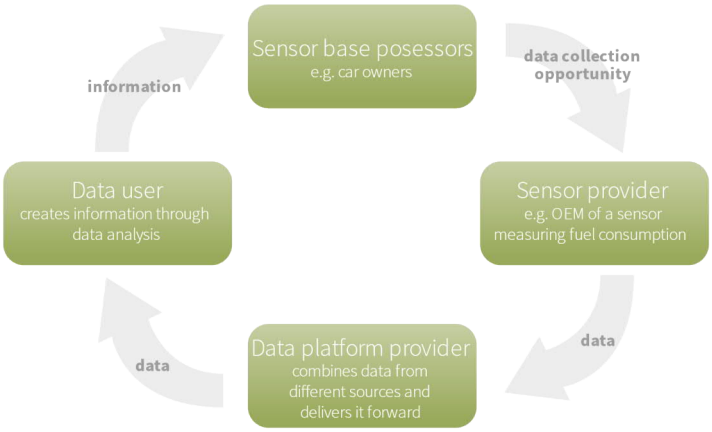

Figure 5 An example of data related relationships. Roles can belong to one or more actors or some roles might not be required in every value chain for non-personal data.

In the following thesis, I will use these roles in analysing relationships between companies in data intensive relations. A further suggestion of the Commission Staff Working Document will also be used in the analysis, the Commission's key principles regarding products and services that rely on non-personal machine-generated data created by IoT objects. The five key principles, 1) transparency, 2) shared value creation, 3) respect for each other's commercial interests, 4) ensure undistorted competition and 5) minimised data lock-in, can be viewed as public policy goals, based on which different practises may be evaluated.[118]

4.2. Technical Practises

Technical safeguards have been and are a common way to protect assets in the Internet. For instance, they have been suggested as primary protective measures for example for databases as they have been viewed as appropriate for the open nature of Internet, by means of protecting information even without adequate judicial protection.[119] Similarly, as there is no right with *erga omnes* effect for non-personal data, technical practises can be argued to have a crucial role for managing non-personal data indirectly.

While not an exhaustive or perfect list, I will conceptualise technical practises for indirect management non-personal data in the following way:

1) restricting access to non-personal data and

[118] COM(2018) 232 Final.10.
[119] Karo 2001 175.

2) changing the non-personal data by
    a) encoding it or
    b) anonymising it by removing some data
3) making data transactions traceable.

The categories enable exploring what benefits the different practises can have for companies. To explain the categories using analogic metaphors, we can think of a foreign language library where category 1 practises restrict access by preventing all except certain traffic from passing through the library doors, category 2 practises as either restricting a visitor from reading the books by removing visitor's dictionary or censoring the contents of the books by cutting pages with identifiable content and category 3 practices as including a borrower sheet on a book's inside cover, with information on who has borrowed the book and when.

Starting with category 1, restricting access to non-personal data, I mean quite simply excluding another actor from connecting to the data using technical means so that there is no factual access for the end-user. This can be done by, for example, not offering a physical wired or wireless connection to the sensor. This is the simplest technical practise to manage data indirectly and what to my understandings Seppälä et al. mean by factual management.[120] The other option is to prevent that connection digitally, for example by using firewalls. Firewall is technology that blocks unauthorized traffic between an internal network and outer network, usually the Internet.[121]

Category 2a means coding data so that it still carries information, but the information is not accessible by unauthorised parties. This can be done for example by using the sensor-providers own standard for the data file or encrypting the data so that its reading requires encryption key. This way, even if the data is accessed without contractual arrangements or other authorization, the information that could be analysed using the unencrypted data, is not available to the unauthorized data user.[122] For example cryptography algorithms such as attribute-based encryption, where encrypted data, ciphertext, can only be decrypted with a key that matches both the ciphertext's and user's key, may be used to encrypt data.[123]

Even technical measures that protect non-personal data could require legalisation. From the field of immaterial property rights, an analogy could be drawn to DRM (Digital Rights Management) technologies that can be used to protect for copyrighted works or databases

[120] Seppälä – Juhanko – Mattila 2018.
[121] Oppliger 1997 94.
[122] Goyal et al. 1.
[123] Goyal et al. 2.

protected by the *sui generis* database right. DRM software has been used for instance to protect music or audio-visual recording from unauthorised use.[124]

However, circumventing DRM software is in the EU prohibited based on Art. 6 and Art. 7 of the Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society[125]. Art. 6(1) of the Directive provides that Member Stare shall provide adequate legal protection against the circumvention of any effective technological measures, which the person concerned carries out in the knowledge, or with reasonable grounds to know, that he or she is pursuing that objective, and Art. 7(1) required Member States to provide protection against any person knowingly performing without authority any of the following acts: (a) the removal or alteration of any electronic rights-management information; (b) the distribution, importation for distribution, broadcasting, communication or making available to the public of works or other subject-matter protected under this Directive or under Chapter III of Directive 96/9/EC from which electronic rights-management information has been removed or altered without authority. Furthermore, according to Art. 6(2) of the directive, Member States shall provide adequate legal protection against the manufacture, import, distribution, sale, rental, advertisement for sale or rental, or possession for commercial purposes of devices, products or components or the provision of services which 1) are promoted, advertised or marketed for the purpose of circumvention of, or 2) have only a limited commercially significant purpose or use other than to circumvent, or 3) are primarily designed, produced, adapted or performed for the purpose of enabling or facilitating the circumvention of any effective technological measures. However, as individual data items are not protected under copyright or the Database Directive's *sui generis* right, there would be no such specific legislation providing for protection from use of software to circumvent the cryptography like the protection described above.

Considering category 2b, anonymisation means changing the data so that confidential information cannot be distilled from it. Non-personal data could be aggregated so that the data could be shared without the fear of some identifying characteristics revealing information that, for example, from a factory that the sensor provider deems confidential. An example could be data that carried information regarding location of the sensor base or serial number of the sensor. The Commission has mentioned anonymization as one possible service that a data-monetisation platform could provide.[126] The problem with anonymizing data is that even the

[124] Regarding DRM and its problems, see for example Trivedi.
[125] OJ 22.6.2011 L 167.
[126] SWD(2018) 125 Final. 2018 10.

anonymized data could, if combined with other data, be deanonymized again, and this would have to be considered when using this practise.

Since the state does not act as a centralized allocator of rights on data, a decentralized solution could be considered. These solutions fall into the category 3 described above. For example, blockchain (distributed ledger) technology that allows all parties considered to see what transactions have been done on the blockchain. As the information considering transactions in blockchain could be inerasable, blockchain could probably be used so that the parties can review if data has been shared with third parties or if it has been changed.[127] This could open possibilities to work without a central hub controlled by one of the parties. This way some of the problems of public key encryption could be avoided, for example the fact that one actor must have access to the public key even if its use is restricted by contractual means.[128]

When these technical practises are used, parties have no need to define what data is or describe its quality. They only need to make sure that enough network capacity to transfer the data, and enough processing capacity to process it, are available. The practises of course require that corresponding contracts are used so that the practises do not become illegal, in other words, data is collected, transferred and stored with permission. Therefore, from a legal point of view these technical practises could be viewed as strengthening the enforcement of the agreement or as non-judicial incentives for the parties to continue their co-operation, within the parameters set by a legal-technical framework.

While looking at the issue of third-party use of non-personal data we can see that practises in categories 1 and 2 can prevent continuous access by third-parties to data. However not all of them prevent access to data if one of the members of data value-chain gives a third-party for example access to the encryption key. While not removing it completely, the technical practises evaluated can be viewed as functional ways to reduce the effect of the third-party unauthorised access problem. In the future, especially blockchain based practises could be interesting as they would enable the parties to see information regarding who has accessed the data, who the access has been given by, and if the data been altered.

[127] See for example, Crosby et al. 2016; Blockchain is also mentioned as one possible technology that could act as a data sharing technical enabler in the Commission Staff Working Document SWD(2018) 125 Final. 2018 11.
[128] See for example Wang – Zhang – Zhang 2018.

4.3. Legal Practises

This subchapter aims to explore how those fields of law that are not *per se* strongly linked to non-personal data, could form part of management of non-personal data as legal practises. While these practises may take many forms that cannot be covered here extensively, the goal is to explore questions related to these legal practises and perhaps provide topics for further research.

As established, non-personal data itself cannot be owned but the sensors, cables, systems, data storages and other tangible things which collect, store or carry data can be owned or subject to different property rights regimes, such as leasing. Also, for example the software that is used to access data can be protected by copyright. Thus, there are *erga omnes* rights in proximity of non-personal data, even when such rights do not extend to non-personal data itself. This provides possibilities for management of non-personal data even considering the issue relating to third-parties.

Regarding property rights of tangible items companies have several choices. For example, when a sensor forms part of a larger system there are several options. Firstly it can be sold to the sensor base possessor who will then have wide discretion to decide what to do with the sensor and if the seller of the sensor (sensor-provider) wants to access the data, they will have to have a contractual relationship with the sensor base provider. Secondly, the sensor-provider could lease the sensor to the end-user so that the sensor-provider would retain the ownership to the sensor and its use by the end-user would be subject to a contract between the end-user and the sensor-provider.

The two alternatives have many differences. In the first alternative, the sensor-provider would only have rights based on the contractual relationship between the parties. On the other hand, in the second alternative, if the contractual relationship ended, the sensor-provider would still have access to data as long as the sensor operated due to it being owned by the sensor-provider or at least right to recover the sensor and, if the sensor stores data, receive that data. Also, if the sensor were modified without authorization, the sensor provider would have both civil and criminal law remedies that they could rely on. In addition, the sensor-provider would for example be free to update the software of the sensor and change its functioning in some ways that are within the limitations of the contract.

Even more complicated arrangements combining property and contract law could be possible. For example, companies could agree that the data flow from one company to other company represents a debt between the companies. Then this debt would be secured by setting up a pledge

arrangement on the data related instrument that would then be executed if the pledgor would not provide the data agreed to pledgee. The instrument would become the property of the pledgee who could then rely on getting the data even in the future. This kind of remedy could be better suited for data licensing than contractual remedies the value of which might be difficult to set even by the parties themselves.

One thing that companies must consider when relying on property rights is that they are mainly based on national legal systems. Therefore, the legalisation affecting pledge, for example, might vary from country to country. For example, English courts have held that data cannot be subject to common law lien in *Your Response v Datateam Business Media*[129].[130] As there is not too much case law considering non-personal data, or other data issues than data protection, in many jurisdictions, this could result in legal uncertainties for companies.

According to Art. 1(2) of the Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs[131], copyright protection applies to the expression in any form of a computer program. However, ideas and principles which underlie any element of a computer program, including those which underlie its interfaces, are not protected by copyright under the Directive. Copyright protected software could be used so that the data would be readable only using specific software. On the other hand, other software could be developed to communicate with the data, for example via so-called application programming interfaces (API). An API is a set of software facilities that enables computer programs to interact with the software that provides interface of that software.[132] The EUCJ took a stand of copyright protection of APIs in case *SAS Institute v World Programming* where World Programming had designed a software emulating SAS's software component so that SAS System users could run scripts developed to SAS System on Word Programming System in order to work with their data.[133] The EUCJ held that Art. 1(2) of Directive 91/25 must be interpreted so that functionality of computer program or programming language or the format of data files used in a computer program do not constitute a form of expression of that program and are not, as such, protected by copyright in computer programs.[134] Thus, the ideas and functions on how APIs work are not copyrightable under EU law.[135]

---

[129] [2014] EWCA Civ 281 25
[130] Osborne Clarke LLP 2016 30.
[131] OJ 1991 L 122.
[132] Ince 2013.
[133] C-406/10, *SAS Institute Inc. v World Programming Ltd*, EU:C:2012:259, paragraphs 23–24.
[134] C-406/10, *SAS Institute Inc. v World Programming Ltd,* EU:C:2012:259, paragraph 46.
[135] Reaching a different conclusion, the United States Court of Appeals for the Federal Circuit held in case *Oracle America v. Google* that Google's usage of Oracles Java software's APIs as part of its Android software violated

Another legal indirect management practise that could be used to share non-personal data in larger scale might be shelling the non-personal data in a company that could then be sold to another company. This may sound too far-fetched but within the realm of personal data markets, personal data has been considered one of the main drivers for example for the purchase of WhatsApp by Facebook.[136] Of course, transferring rights to data via acquisition of companies is not a flexible way, but due to its comprehensive nature it could in some cases be a viable option. For management of immaterial property rights such as copyright and trademark, so called intellectual property holding companies have been used, though mainly for minimizing taxes.[137]

Of these indirect legal management practises of non-personal data some would have effects on third-parties due their nature. For example, if sensor-provider retains ownership right in the sensor, they could control where the sensor sends data. Therefore, these practises could be suitable additions to contracts between two parties, especially from the viewpoint of executing contracts. While uncomprehensive in nature, the main idea of this subchapter was to demonstrate that the existing legal frameworks allows various legal arrangements that could be used to manage non-personal data. The subchapter establishes that even without data rights with *erga omnes* effect, clearly, management of non-personal data cannot be viewed in a legal vacuum but as a practise where different legal regimes and practises need to be considered, depending on the situation along with for example technical practises.

4.4. Business Practises

Business practises used to indirectly manage non-personal data are practises where the non-personal data-sharing relationship is linked to company's offerings other than non-personal data in order to facilitate the data sharing relationship. That is, some other element of the business relationship between companies than mere data-exchange is used to further the aims of that data-exchange.

One of the business practises that can be used to indirectly manage non-personal data is servitization, a phenomenon which means that companies add service components to their offering.[138] Servitization practises could be viewed as a solution to the third-party problem since

---

Oracle's copyright. Though the facts of the case were somewhat different, the case illustrates differences in the US and European approach. *Oracle America, Inc., v. Google LLC*, No. 17-1118, (Fed. Cir. Mar. 27, 2018).
[136] Autorité de la Concurrence and Bundeskartellamt 2016 17.
[137] Cowan – Newberry 2013.
[138] Eloranta 2016 1.

it provides different actors within the value chain for data with incentives to have agreements with each other. For example, a tractor manufacturer that is both a sensor-provider and a data platform provider could offer added-value services for the farmers (sensor base possessor) that enter into data-sharing agreement with them. These added-value service could be based on the information analysed from the shared data.

In addition to managing non-personal data, servitization could have other business benefits as the data could feed in the product development feedback-loop and for example products could be developed based on the data with software updates through iterative development processes. This could benefit both the data platform provider and the sensor base possessor. Data platform would be able to develop better products which could increase their profits and the end-user (sensor base possessor) could, using the improved products, increase their productivity. Servitization could work especially in cases where the end-users are a closed group, for example if tractors are offered as a service or as a product infused with service components, the data platform provider has a relationship with all the farmers using the service.

An example can be given considering copyright. When distribution from old technology with analogue carriers of information, for example audio cassettes, transferred to digital media, this caused a spark in illegal copying of copyrighted material referred to as online piracy. Later, streaming companies such as Spotify emerged that provided users with a service where content and its delivery were tied. This has resulted, according to some studies in lower piracy.[139] While other studies advocate that online piracy has still grown, there has at least been a change in how piracy is conducted.[140] This suggests, in any case, that changes in how content is delivered affect unlawful sharing as well.

As we can see by making an analogue between the above tractor example and the Spotify case, what matters is whether end users are content with not having wide ownership-like rights or if they are dissatisfied and want to gain wider access to non-personal data, for example. Thus using business practises, companies should, in addition to making sure that the technical and legal aspects are covered, make sure that the data management practises are commercially viable.

Similarly, it is possible that new actors emerge who, based on their business models, solve issues regarding sharing of non-personal data effectively. The scope of this chapter is not to speculate on such potential endeavours. The aim is simply to point out that it is unlikely that a

[139] YouGov 2018.
[140] See for example, Global Piracy Increases throughout 2017, MUSO Reveals. 2018.

pure legal or pure technical practise for management of non-personal data will prevail as all practises used by companies to manage non-personal data must be, at least in some level or on some time scale, commercially sustainable.

Another business practise that a company may use to manage non-personal data indirectly is to use the non-data related relationship between a company and its business partner to ascertain that the business partner continues to follow their data obligations. For example, this could be done, by having contractual provisions that allows the company to stop delivering its products to the business partner in case they do not fulfil their data obligations. In a dyadic relationship a company may use this tactic rather easily, but it cannot be used towards a third-party that uses data without authorization. Also, a company might not be able to stop for example payments when it receives data to a business partner, if contract provisions between parties would not specifically allow it. In a more complicated data sharing network, this practise could be more difficult to use.

Even business models could be based for facilitating the management of non-personal data. For example, businesses have emerged providing platforms for management of data. For instance, a company called Microshare offers a product called digital ombudsman through which parties can transfer data. Microshare's platform then manages the different rights to the data within the platform using four levels of decision making or access that the company calls ownership levels: data originator, primary data owner, co-owners, and enabled parties.[141] Another company offering real-time data sharing, Nallian, develops a platform for companies working within vertical-supply chains. The platform allows companies providing data to the platform the retain control over the data.[142] Naturally, the challenge with these kinds of services is that each actor within the value chain for data should participate in the platform.

Another aspect regarding business practises is that companies may need to make a strategic choice regarding non-personal data, such as how much data they are willing to share and with whom. Strategic choices stem from data relationships and should be considered.[143] This choice would then affect their tactics on managing non-personal data and how they organise their functions.[144] These kinds of intraorganizational issues are however out of the scope of this thesis.

---

[141] Rock – Moran 2018.
[142] SWD(2018) 125 Final. 2018 11.
[143] SWD(2018) 125 Final. 2018 6.
[144] Dallemule – Davenport 2017.

4.5. Reflections

Indirect management of non-personal data can be seen as a diverse category of practises which are hard to categorise specifically in categories of legal, technical and business practises. In most cases all the angles should be considered. Indirect management of non-personal data also functions together with contract law by strengthening what the parties have agreed and has effects on third-parties. Indirect management of rights to non-personal data operates within the parameters set by the legal, societal, commercial and physical realms. In practise, a multidisciplinary approach may be needed in companies to successfully implement these practises.

If contract law is criticised for granting stronger players more leverage than weaker ones, so is the indirect management of non-personal data, the whole idea of which is to gain higher-ground compared to other market actors. Thus it is easy to be critical towards these practises. The EU legislator can be seen trying to hinder the practises of using incompatible data to one's advantage through the non-binding agreement and self-regulatory codes of conduct developed based on Art. 6 of the Free-Flow of Non-Personal Data Regulation.

From a societal point of view, indirect management of non-personal data can however result in practises that allow companies to share, utilise and refine data and add value to their existing and new products and services. When companies rely on indirect management of non-personal data practises, they need not consider, for example, the limitations of contract law regarding *erga omnes* rights, or, the possibly slow development of statutory and case law.

When indirect management solutions are used on large scale it is quite possible, that some market actors will gain market power through, for example, platform or network effects. This will have implications from a competition law point of view and need to be considered. However, such implications are outside the scope of this work.

In this chapter practises of indirect management of non-personal data were presented. From a legal angle another way to manage data is to create rights on the non-personal data and then manage those rights using non-personal data. That is what will be covered in the next chapter.

5. MANAGING RIGHTS TO NON-PERSONAL DATA DIRECTLY THROUGH CONTRACTS

According Calabresi and Melamed, when there is a conflicting interest between people or groups of people, the state must decide which side to favour.[145] When two actors wish to voluntarily enter into an exchange relationship, they have at least some aligning interests and therefore the state does not need to allocate entitlements between them, as the conflict of interests can be bargained to find a mutually satisfactory solution.

In this chapter, I focus on situations where unlike the scenarios presented by Calabresi and Melamed, the state has not defined specific property right regimes on non-personal data and, naturally, cannot have allocated these undefined rights.[146] The scenario could be described as *status quo ante* state allocation (Figure 4). From another viewpoint, in these situations the state has allocated two entitlements for market actors. The first entitlement is to be freely able to bargain about their relationship related to certain non-personal data (which the legislator actually has encouraged through the Free Flow of Non-Personal Data Regulation). The second entitlement is to have the results of bargaining, contracts to be enforced by the court system[147] using the rules that have been chosen by the parties when they entered into contract.[148] It is these two bases, that have made contract law a powerful tool for commerce.

I will first examine some of the characteristics of contract law and how these characteristics affect how contracts can be used in direct management of rights to non-personal data. Then, I will analyse the different roles and relationships that companies may have in a data-intensive market. Next, I will present what provisions data licensing agreements have been suggested to include. After that, I will analyse how non-personal data related issues are managed in contracts by using publicly available general terms and conditions. Finally, I will reflect on contract law as a tool of managing rights to non-personal data.

---

[145] Calabresi – Melamed 1972 1090.
[146] Considering 'non-propertized' resources, see Chang 2015 475.
[147] Here, regarding contract law, court system should be understood broadly, covering also alternative dispute resolution such as arbitration.
[148] See Calabresi – Melamed 1972 1106.

5.1. Relevant Characteristics of Contract Law

Next, I will discuss how different characteristics of contract law affect how it is used to manage rights to non-personal data. Characteristics explored are those of freedom of contract, enforceability only *inter partes* and the transnational nature of contract law.

Freedom of contract

Based on the principle of freedom of contract, contract law is an adaptive area of law that provides private parties with flexible measures with which to regulate their relationships and their assets. This flexibility allows contract law to address emerging new technologies and business models.[149] The adaptiveness of contract law is illustrated by the facts that parties are able to bargain regarding assets such as non-personal data, even when no property rights for data have been defined by the state. Bargaining, in modern societies framed under contract law, is for example under the Coase theorem viewed as a way to effectively allocate externalities, as long as there are no transaction costs and property rights are well defined.[150] In case of non-personal data, transaction costs relating to sharing data are small, but the lack of property rights creates transaction cost as data has to be defined.

The externalities that market actors are trying to allocate, regarding management of non-personal data, stem from the characteristics of data introduced in chapter 2. When production of data is costly, but transaction costs for transferring and reproduction of data are small while property rights are not defined, companies are incentivised to use data that they did pay the production costs of. As exemplified by the decision game study by Pan et al.[151], it is unlikely that the parties could sustain their data relationship without the ability to enforce their relationship by external pressure. There being no immaterial property regime for non-personal data, contract law seems the most promising way to achieving this.

In practise, contract law is currently the legal instrument used by companies to manage their non-personal data related relationships.[152] This shows that contract law has the ability to adapt to changing societal and technical phenomena. However, contract law places a lot of responsibility on the parties considering what kind of contract provisions are agreed, and thus

[149] Savelyev 2016, 7.
[150] Coase 2013. Considering the role of contract law in modern societies, Henry Maine famously argued that civilizations move from an emphasis to status to an emphasis to contract. Maine 1861.
[151] Pan – Ma – Wu 2018.
[152] Osborne Clarke LLP 2016 28; SWD(2018) 125 Final. 2018 6.

may give leverage for parties that have more resources. [153] This could leave for example SMEs in worse situations than large companies, as is perhaps reflected on the wording of Art. 6(2) Free-Flow of Non-Personal data regulation, which requires the Commission to ascertain that small and medium sized enterprises and start-ups are involved in talks for self-regulatory codes of conduct regarding non-personal data.

There is not much case law regarding contracts and data on the EU level. But in *Ryanair v. PR Aviation*[154] the Court of Justice of the European Union has confirmed that if a database does not fall under the database *sui generis* right protection, the holder of such a database can impose contractual limitations on the use of the database. The case referred to the Court by the Dutch supreme court Hoge Raad der Nederlande considered PR Aviation's website that collected flight data including price data from various sources, among them a dataset on Ryanair's website. On the PR Aviation site customer could compare airlines and book flights.[155] When accessing the Ryanair site, user was to accept certain conditions by checking a box. These conditions included that Ryanair's website was the exclusive website distributing Ryanair's services and that the use of website was only allowed for certain private, non-commercial purposes. The website's terms of use also explicitly prohibited the use of automated systems or software to extract data from the website's data set without a written license agreement with Ryanair.[156]

The Dutch supreme court asked the EUCJ that if Ryanair's database was not protected neither under Database Directive's Chapter II by copyright nor under Database Directive's Chapter III by the *sui generis* right, would the database still fall within the scope of the Database Directive. If it would the contractual freedom of Ryanair would be limited based on Articles 6(1) and 8 of Directive. Regarding copyright protection, Art. 6(1) gives lawful users right to use the contents of database normally without the authorization of the author of the database. Regarding *sui generis* right, Art. 8 inter alia allows the lawful user of the database to extract and or re-utilize insubstantial parts of databases contents. In addition, Art 15 states that any contractual provision contrary to Articles 6 (1) and 8 shall be null and void. Based on the purpose and structure of Database Directive, the EUCJ concluded that said Articles are not applicable to a database which is not protected either by copyright or by the *sui generis* right under Database Directive. Thus, the directive would not preclude the adoption of contractual clauses concerning the

[153] Osborne Clarke LLP 2016 28.
[154] C-30/14, *Ryanair vs. PR Avion,* EU:C:2015:10.
[155] C-30/14, *Ryanair vs. PR Avion,* EU:C:2015:10, paragraph 15.
[156] C-30/14, *Ryanair vs. PR Avion,* EU:C:2015:10, paragraph 16.

conditions of use of such databases. In other words, in *Ryanair vs. PR Avion* the EUCJ confirmed that where Database Directive is not applicable, freedom of contract prevails.[157]

Contract law can provide dynamic solutions to managing non-personal data, because in contract law, there is no need for a dichotomy of ownership and not owning something. Therefore, for example joint management of non-personal data with different rights for various stakeholders is possible. The problem of course is who has the right to provide other actors with these rights. As explained in subchapter 4.4 regarding business practices of indirect management of non-personal data, there are companies that provide such data sharing platforms and the legal element of the platforms is based on contract law. Also the business model data monetisation on a data marketplace envisioned by the Commission was based on bilateral contracts.[158]

***Inter partes* effect**

Contracts are enforceable *inter partes*, between parties, and there can be two or more parties to a contract. However, what contract law cannot provide, due to the doctrine of privity of contract, is obligations on third-parties. This reduces the usefulness of contract law in managing non-personal data and requires the parties to solve the issue regarding third-parties by for example using the legal or technical solutions as established in chapter 4. The inability to have effect on third-parties is lessened by the fact that some data sets loose significance over time. When the value of the data lessens as time passes, the lack of protection against third-party use of data is not always an important issue as with tangible products, the value of which does not lessen over time as that of data. This is also true when a data stream, instead of a static data set, is licensed since a data stream licensor may more easily block the use of the data stream compared to a data set licensor.

As contracts create effects only between parties, contract law creates uncertainties if one of the parties to the data licensing agreement goes bankrupt.[159] If a party has access to data but that access is contractually restricted, those restrictions could perhaps cease to exist in the event of insolvency. Another problematic situation would be when a data licensee would have been waiting to receive non-personal data from a licensor who went bankrupt. Insolvency law will however be left out from the scope of this work.

When private regulation of non-personal data is compared to another fairly new phenomenon, so-called open source software, the lack of property rule or liability rule entitlements can be

[157] C-30/14, *Ryanair vs. PR Avion,* EU:C:2015:10, paragraph 39.
[158] SWD(2018) 125 Final. 2018 5.
[159] König 2016 4.

seen as leaving data licensing relationships without efficient backstop. When a software developer wants to license its software as open source, it uses specific licensing terms, such as GNU General Public license GPL[160], to inform the public that they are willing to make a contract through these specific terms. If a licensee then distributes the software without the licensing terms to third parties, the copyright holder can rely on copyright to get legal protection for them. For non-personal data, such possibilities do not exist, and other means need to be relied on.

Transnational legal order

A characteristics of contract law is that it is simultaneously national and supra-national law.[161] Some of the basic contract law doctrines and practises are common between jurisdictions but on the other hand national law affects how contracts are interpreted and how they are enforced. In this regard there are major differences between common and civil law systems, also in practises.[162] For companies, this is something to consider.

The effects of different contracting practises may be alleviated by the nonbinding best practises facilitated by the Commission based on Art. 6 of the Free-Flow of Non-Personal Data Regulation. Also, the Commission is planning to collect model contract terms through its Support Centre for data sharing which could make it easier to make data related contracts in different member states.[163]

5.2. Provisions of Data Licence Agreements

Data licence agreements require special attention in order for them to be compliant with applicable law and with the strategic interests of the parties.[164] In the OAD report conducted for the Commission, the law firm Osborne and Clark identified what kind of provisions their offices in several EU Member States use in data licence agreements. The provisions mentioned in the report include the object of a data licence, "owner" of data, quality of data, exploitation rights, type of licence, duration, duty to forward any obligation, technical and organisational measures, audit rights and contractual penalties.[165]

[160] GNU General Public License 3.0.
[161] Regarding develpoment of transnational contract law, see Calliess 2007.
[162] Osborne Clarke LLP 2016 75.
[163] SWD(2018) 125 Final. 2018 6.
[164] SWD(2018) 125 Final. 2018 6.
[165] Osborne Clarke LLP 2016 90–93.

Using the provisions listed in the OAD report, I categorise the provisions of data-licensing agreements in four groups:

1) provisions describing data,
2) provisions defining the rights and obligations of contracting parties,
3) provisions regarding third-parties to the original contact, provisions regulating relationships between a party to the contract and their subsequent contracting parties,
4) supporting provisions that strengthen the execution of the agreement.

In addition to the above categories, general provisions such as those defining parties, applicable law and dispute resolution need to be defined in data licence agreements. [166]

It is important to note that a data licence can be part of another agreement between companies – intentionally or unintentionally. Different agreements between companies, for example a non-disclosure agreement and general terms and conditions signed by parties, might be inconsistent with each other. All agreements between the parties and their mutual applicability order should be considered when interpreting what parties have agreed to regarding non-personal data. Next, I will introduce the provisions mentioned in OAD report and provisions suggested by other sources using the above-mentioned categories.

Provisions describing data

As non-personal data is not a state-established asset and due to the characteristics for data as an asset explained in chapter 2, data license agreements need to include provisions that define data in a way that corresponds to the intentions of the parties. Of the provisions mentioned in the OAD report, the object of data licence and quality of data fall into this category.

Defining the object of data licence, i.e. the data that is licensed, can be done in various ways. Parties should first define, whether the data sharing considers a static data set or a data stream.[167] After that, the licensed data can be identified by describing the database or in case of dynamic databases, the data stream licensed.[168] Another option is to describe data using attributes of the information the data carries as concretely and precisely as possible. For example
the data could be described as R&D data or diagnostics data.[169] Alternatively, the source or origin of data collection can be described. Moreover, for example the frequency of how often

[166] SWD(2018) 125 Final. 2018.
[167] SWD(2018) 125 Final. 2018 6.
[168] Osborne Clarke LLP 2016 90.
[169] SWD(2018) 125 Final. 2018 6.

data is updated could be agreed.[170] Defining data is easy on paper but can be, in practise, difficult due to the characteristics of data as being mouldable and a carrier of information level phenomenon as described in chapter 2.

The same concerns the definitions of quality of data, though, as industry standards or best practises emerge, they may facilitate the issue.[171] The OAD report mentions a sample dataset as one way for the parties to ensure the quality of data in an agreement.[172] For example Hoeren has argued that an interdisciplinary discussion is needed to develop a framework for quality of data.[173] The framework could be established within the ISO system and would set the normative level for data quality.[174] This kind of framework could be useful also from a societal point of view, as it would lower the transaction costs of entering and enforcing data licence agreements considerably.

It is also important to define what the licensed data is not or what information it does not carry. For example, unless that is the intention, no personal data or data that carries information that is protected under intellectual property rights should be transmitted. This is to ascertain that the data exchange complies with applicable legislation.[175] Furthermore, the parties should exclude data that carries information incorrectly. Thus, missing, duplicate and unstructured data could be excluded.[176]

It is of crucial importance how data is described for the enforcement of the agreement. If a court cannot interpret what the object of the agreement is, it is not able to decide the case. In that sense, the provisions describing data can be seen as constituting data as a legal object without which the other contractual provisions could not have any meaning.

Provisions defining the rights and obligations of contacting parties

When intellectual property is licensed and is protected for example by copyright or other *erga omnes* right that protects from third-parties, the licence usually provides exceptions to the rights-holder's exclusive property right in question. Since there is no property right regime for data, based on which the right-holder would be able to grant use-rights or licenses, data licences should, as a main rule, prohibit the licensee from using the licensor's data and, as exceptions to

---

[170] SWD(2018) 125 Final. 2018 6.
[171] A traditional example of a standard lowering transaction costs is the shipping contrainer that is seen to have contributed to the increase of global trade, see den Butter – Groot – Lazrak 2007.
[172] Osborne Clarke LLP 2016 91.
[173] Hoeren 2017 37.
[174] Hoeren 2017 37.
[175] SWD(2018) 125 Final. 2018 6.
[176] SWD(2018) 125 Final. 20186.

the main rule, allow for certain ways of use.[177] This distinction between data and other intellectual property assets can be taken into account by defining the 'owner' of data in the agreement in a metaphorical sense.[178] This ownership of course, has no applicability towards third-parties, but the word has been seen as quite comprehensibly descriptive for non-lawyers especially, as the exclusive 'base' right to data which is created by the agreement.[179] It has been argued that, in practice, the factual right possessor is the party who owns a machine that collects data or who collects and stores the data as they are in the natural position to transfer data.[180] However, as explained in chapter 4, it might not be as simple as that and for example property rights to tangible sensors should be considered.

After the base of the data licence agreement has been established with the "ownership" clause, specific exploitation rights can be granted in other provisions. Schefzig has classified data exploitation rights in five categories: right to access data, right to store data, right to use of data, right to change data, and right to transfer data. Access right provides the licensee with a right to read the data while storage right means permanent storing of data. Schefzig defines right to use data as a right to process data without changing it, for example copying and analysing of data. Right to change data allows licensee to change the data within a data item and right to transfer data covers transferring the data from one storage to another and granting another actor access to data.[181]

In the OAD report, type of licence is presented as a choice between an exclusive and nonexclusive licence, that is, whether the licensor may license the data in question to one or several licensees.[182] The OAD report points out that exclusive licence can also be granted for specific purpose.[183] Provisions regarding type of licence could also include stipulations considering for example the geographical extent of the licence or for example whether the data can be used for non-commercial purposes only or only by certain professional groups, such as farmers.[184]

In case exploitation rights are not meant to be permanent, the agreement is suggested to include clauses that prohibit exploitation of data after the termination of the contract. Otherwise the licensee could continue using data indefinitely, even without the restrictions set up in the data

[177] Osborne Clarke LLP 2016 90.
[178] Osborne Clarke LLP 2016 90.
[179] Osborne Clarke LLP 2016 99.
[180] Seppälä – Juhanko – Mattila 2018.
[181] Osborne Clarke LLP 2016 91.
[182] Osborne Clarke LLP 2016 91.
[183] Osborne Clarke LLP 2016 91.
[184] SWD(2018) 125 Final. 2018 7.

licence agreements. Provisions for the deletion or returning of data have also been suggested to be included in data licence agreements.[185] However, it could be argued that if data has been modified or if information has been analysed based on the data, these kinds of provisions are ineffective.

Provisions regarding third-parties to the original contact

As explained above, contract law does not have *erga omnes* effect. However, this can be partly mitigated by either prohibiting the other party from giving rights to data to third-parties or if sublicensing is wanted, introducing the licensee with a duty to forward any of its obligations to its sublicensees. The first option is in theory easier, but in practise data is often transferred or stored using third-party data platform providers, such as cloud storage. In that case, the licensor should require the licensee to agree with their cloud storage providers that they may not access or use the data stored on their servers.

If sublicensing is aspired for, the licensee's duty to forward any obligation can be strengthened by awarding the licensor direct contractual claims to the sublicensees. Nevertheless, if the licensee does not forward these duties to the sublicensee, the licensor will not have the right to contractual claim and will have to rely on a regressive claim towards the licensee or to try to protect the data based on the legislation introduced in chapter 3, for example Trade Secrets Directive.[186] From the point of view of data licensee, being open considering data use by sublicensees can be seen as adding trust of data licensor.[187]

Supporting provisions

Supporting provisions consist of a variety of stipulations that aim to ensure that the data exchange is successful. Supporting provisions are supportive in the sense that they do not constitute the essence of the data exchange relationship but support the execution of the agreement.

The parties may agree on technical and organisational measures which aim to protect the data from, for example, unauthorized use of data by third-parties or deterioration of data.[188] For example, the parties could require compliance with certain data security standards.[189] Also

[185] Osborne Clarke LLP 2016 92; Tollen 2016 7.
[186] Osborne Clarke LLP 2016 92.
[187] SWD(2018) 125 Final. 2018 7.
[188] Osborne Clarke LLP 2016 92.
[189] Tollen 2016 6; SWD(2018) 125 Final. 2018 7.

certain level of access (frequency, connection speed) can be defined or the service level offered to the data licensor.[190]

Audit rights can be used to provide the licensor with a right to monitor the licensee's use of data and for example their data security measures.[191] Audit rights naturally require that the licensor *de facto* has the capacity to conduct the audits on the data use of licensee. If it has, then the threat of audits could be more credible way to direct the other party's behaviour than relying on, for example, the public judicial system which might not be as efficient in data exchange related issues.

Contracting parties should pay attention to how contracts are enforced. As damage or loss caused by a breach of contract can be difficult to show, contractual penalties or liquated damages agreed upon signing of the contract may be an efficient remedy for breach of data sharing licences.[192] Regarding contractual penalties it must be remembered that, depending on the jurisdiction, the courts may assess the balance of the contractual penalties which the parties could also consider when agreeing on contractual penalties. [193] As an alternative to contractual penalties, bank securities, such as letters of credits may be used. An advantage of such arrangements is that they may protect the claims of licensor in case of the licensee's insolvency, considering the rules on recovery of assets in the jurisdiction. Considering enforcement of contract, difficulty of evidencing breach of contract needs to be taken into account.

5.3. Data in Example GTCs

When compared with public regulation, it is difficult to form an overview of the private regulation around a legal issue. It is especially problematic regarding the management of non-personal data due to the lack of established best practises or industry standards. Therefore I will next try to form an understanding of the current situation by looking at actual general terms and conditions that may have clauses relevant to management of rights to non-personal data. This change of angle from how companies *can* manage non-personal data, using contracts, to how they actually *do* manage non-personal data is done to test what was stated in the previous subchapter and to get insights on management of rights to non-personal data.

[190] SWD(2018) 125 Final. 2018 7.
[191] Osborne Clarke LLP 2016 92.
[192] Tollen 2016 7.
[193] Osborne Clarke LLP 2016 93.

To accomplish this, I have chosen to analyse general terms and conditions, both upstream (supply side) purchase general terms and conditions and downstream (customer side) sales general terms and conditions that are currently or have been recently used by the twenty largest Finnish companies.[194] Studying both supply and customer side general terms and conditions helps me to analyse the value chain in its middle, where both upstream and downstream considerations need to be regarded. I have selected this group of companies since I believe it is more likely that non-personal data management is considered in larger companies than in the smaller ones. If I have instead of the Finnish parent company found its foreign subsidiary's general terms and conditions, I have reviewed them as I believe they also offer insights on contracting practises.

I also note that these general terms and conditions are not final agreements but more like general offers that the companies are stating as the provisions they would want to make agreements based on. Whether they are accepted as such or not depends on many things, for example the parties' bargaining power.[195]

The aim is not to get a comprehensive generalizable overview of how data is licensed. Using this method it would not even be possible. Rather the aim is to make observations about how and whether non-personal data related issues are considered. This will provide valuable understanding on how management of non-personal data is currently viewed in large Finnish companies.

The found provisions will be analysed based on certain criteria. When compared to public regulation it is impossible to know why private actors have wanted to commit themselves to certain contractual conditions, for example due to the lack of *travaux préparatoires*. However, based on economics we can assume, that market actors are trying to maximise the value of their possession.[196] Since data has value, it can then be assumed, that companies are trying to maximise the amount of valuable data they possess. Secondly, contractual provisions can be evaluated based on whether adherence to them would promote pareto improvement, that is to say if none of the contracting parties are made worse by the changes and some are made better off.[197] Thus these criteria, maximising of valuable data and pareto improvements, are used in analysing the provisions.

---

[194] Nordic Market Data AB.
[195] Barnhizer 2005 150–151.
[196] See for example, Wolff – Resnick 2012 88.
[197] Regarding Pareto efficency, see for example Rawls 1999 57–60.

Step 1 Gathering GTCs

The first step has been gathering the available general terms and conditions, such as general terms and conditions for suppliers, from these companies, using three publicly available internet search providers, Google, Bing and DuckDuckGo during February 2019.[198] If more than one supply or customer side general terms and conditions was found, I chose the newest one. I have excluded general terms and conditions that are dated before 2015. During the first step I have read the found general terms and conditions and examined which of the general terms and conditions contain data related provisions (Table 1).

	Company	General terms and conditions found from year	Data provisions found	Purchase	Sales
1	Nokia Oyj	2017	Yes	X	
2	Neste Oyj	2017	Yes	X	X
3	Kesko Oyj	2016	No		X
4	Stora Enso Oyj	not found			
5	UPM-Kymmene Oyj	2016	Yes		X
6	KONE Oyj	2016	Yes		X
7	Suomen Osuuskauppojen Keskuskunta, SOK	not found			
8	Outokumpu Oyj	not found			
9	Sampo Oyj	not found			
10	UPM Sales Oy	*See UPM-kymmene*	-	-	-
11	Metsäliitto-konserni	2017	Yes	X	
12	Wärtsilä Oyj Abp	2018	Yes	X	
13	Fortum Oyj	2018	Yes	X	
14	North European Oil Trade Oy	not found			
15	Outokumpu Stainless Oy	*Subsidiary of Outokumpu Oyj*	-	-	-
16	Cargotec Oyj	2016, found agreement for subsidiary Kalmar that covers Cargotec	Yes		X

[198] https://www.google.fi; https://www.bing.fi; https://duckduckgo.com/.

17	Valmet Oyj	2015	Yes	X	
18	Konecranes Oyj	2016, found agreement for Konecranes Inc., the US subsidiary of Konecranes	Yes	X	
19	Huhtamäki Oyj	2014	No	X	
20	Metso Oyj	not found			

Table 1 Finland's 20 largest companies by 2017 turnover[199] and whether general terms and conditions for purchase or sales were found.[200]

Of the twenty companies two were subsidiaries of other companies on the list. Of the remaining 18 companies, 12 had general terms and conditions available publicly on the internet. Of these 12 companies, 10 had data related clauses. A clause has deemed as data related, if the word data has been used in a meaning that clearly is not meant to designate personal data or if for example the word technical information is used in a similar way as data has been defined in this thesis. The main finding of this step of the analysis was in fact that the distinction between data and information, for example, is not clear, as illustrated by the example of confidentiality provisions below.

Several reviewed general terms and conditions also had confidentiality or non-disclosure provisions which did not explicitly mention data, or anything that clearly indicated to having similar meaning as data in this thesis. As non-disclosure agreements and provisions typically aim to restrict the other party from using certain information and the distinction between data and information being somewhat flexible, non-disclosure provisions may have implications regarding the management of non-personal data. For example, the use of information designated as confidential by these provisions may be restricted to 'purpose' of agreement. For instance:

> The parties hereto undertake towards each other during the term of the supply relationship and three (3) years thereafter to keep in the strictest confidence **all confidential information and trade secrets** received from the other party in connection with the supply relationship, and to **use the said information for the purposes of the supply relationship only**.[201] [emphasis added]

These kinds of provisions may prove ambiguous to interpret as it is unclear whether the parties have indeed intended the confidentiality provisions to include mere data. An analogy could here be drawn to the Trade Secrets Directive, the scope of which I argued in chapter 3 was not

[199] Nordic Market Data AB.
[200] See Attachment 2 for detailed information regarding the GTCs and links to them.
[201] Huhtamäki General Terms and Conditions of Purchasing 2014 11.1.

originally meant to include data. If a litigation arose of whether data can be considered as information, the courts could have wide discretion on which to base their decision. Some very similar confidentiality provisions include the word data, and these provisions I have included in the analysis as data related provisions. Nevertheless it is difficult to assess if the object of this later example provision would be interpreted differently to the first provision:

> The supplier **shall not disclose to third parties nor use for any other purpose than the proper fulfilment of this Agreement** any information of confidential nature, such as **technical information and data**, drawings, price structures, costs, and volume information, received from the purchaser ("Information"), without the prior written permission of the purchaser . . . [202]

Step 2: Categorizing data provisions

The second step of the analysis was to categorise the found data provision. This has been done by operationalising the categories presented in section 5.3 as categories of the qualitative analysis (C1 = provisions describing data, C2 = provisions defining the rights and obligations of contracting parties, C3 = provisions regulating relationships between a party to the contract and their subsequent contracting parties and C3 = provisions strengthening the execution of the agreement). If a provision or its part fell into more than one category the provision was placed in all of them.

Company	GTC Type	Year	C1 = Description of data	C2 = Data related rights and obligations	C3 = Data and third-parties	C4 = Execution strengthening provisions
Nokia Oyj	Purchase	2017	X			
Neste Oyj	Purchase and Sales	2017		X		
UPM-Kymmene Oyj	Sales	2016		X		
KONE Oyj	Purchase	2016		X		
Metsäliitto-konserni	Purchase	2017		X		

[202] Kone General Terms and Conditions of Purchase ("GTC") 2016 7.1.

Wärtsilä Oyj Abp	Purchase	2018	X	X	X	X
Fortum Oyj	Purchase	2018				X
Cargotec Oyj	Sales	2016		X		
Valmet Oyj	Purchase	2015				X
Konecranes Oyj	Sales	2016		X		X
Total			*2*	*8*	*1*	*4*

Table 2 Data related provisions categorized using categories operationalised from the categorisation of chapter 5.4.[203]

As seen from Table 2, most data related provisions fell into the category of data related rights and obligations. While the sample of the analysis is too small to draw any statistically meaningful conclusions, it is interesting to note, that what non-personal data is or what the quality of data is, was only described in two general terms and conditions. In other general terms and conditions data is included in the definition of information or intellectual property rights (for example, "*All intellectual property rights related to the Services and Products delivered by Kalmar including, without limitation, any and all software and/or documentation or data included in, with or comprising Products or Services ("IPR")*")[204]. The lack of data definitions could point to the speculation above, that the meaning of data or the distinction between data and information has not been thought as important by the contracting parties. A second option is that, perhaps the word data has been included to incorporate a better safe than sorry mentality, with wishes to cover the *data-information-knowledge* spectrum as widely as possible. A third alternative is that the concept of data has not been thought of and has been intended to cover all structuration levels on the *data-information-knowledge* spectrum. Provisions written with better safe than sorry mentality or without too much consideration could in some cases hinder pareto improvements by being overly restrictive on the possibilities of parties. Whatever the case, the defective definitions cannot be viewed as increasing the certainty on how the contracts are interpreted.

[203] See Attachment 2 for detailed information regarding the GTCs and links to them.
[204] Kalmar General Conditions of Service 13.

Another finding is that provisions regarding the relationship between a party and a third-party are not widely used. This could suggest, that the special nature of data as an asset has not been considered by the companies. In other words, contract drafters might be used to relying on intellectual property rights regimes as safeguard for third-party wrong-doing. Another alternative is that companies identify relationships regarding data as requiring special data licence agreements and therefore do not have comprehensive data provisions in the general terms and conditions.

Step 3: Analysing data related provisions

The third and final step of the analysis is evaluating the found non-personal data related clauses against the model provisions described in the previous section 5.3, especially the provisions regarding data as an object and third-party use of data.

Provisions describing data

In the first category, provisions that describe data, only one definition of data was found in addition to one clause that defined the quality of data. The definition found clearly identifies data as digital data that has been collected using sensors. In this provision, the digital nature of data has been emphasised with the word technical:

> "Technical Data" refers to all data relating to the **technical operating parameters** of any Supply [goods, equipment, accessories, tools, . . . designs, documentation, services, software, firmware, hardware, consultancy ....] delivered, including without limitation, **all information gathered from sensors, instruments, monitors, or other industrial control or SCADA devices** located at the Wärtsilä end-customer's site or on the Supply[205] [emphasis added].

As the sensory data meant in the provision is clearly dynamic, the definition can be viewed as appropriate, as it captures the nature of data based on its source.[206] Therefore questions, such as, which specific database are covered, need not be addressed. This definition seems to be created for industrial purposes, since for example Supervisory Control and Data Acquisition (SCADA) devices that are used in industrial processes are mentioned.[207]

The only clause found regulating the quality of data set arguably quite high demands to the quality of data: “Supplier warrants that any data and other information provided to Nokia under this clause are in all respects complete and correct.”[208] Firstly, the nature of data as carrier of

[205] Wärtsilä General Terms and Conditions for Supply and Purchase 2018 2.8–2.9.
[206] This approach in defining data is suggested for example in SWD(2018) 125 Final. 2018 6.
[207] Daneels – Salter 1999.
[208] Nokia General Terms and Conditions for the Purchase of Hardware and Software 2017 17.8.

information does not go well with the word correct that implies a truth-value. Secondly, the clause can be viewed as overly restrictive especially in the context of dynamic databases. Of course it could be argued that data here is used in what is meant by information in this thesis. However, this kind of clause points out the need for industry best practises for the quality of data as the complex issue cannot be covered by these kinds of simple provisions. Nor it is efficient for each data market actor to come up with their own quality standards for data as that increases the transaction costs of each data exchange as it costs to describe data.

Data related rights and obligations

All in all, seven of the general terms and conditions with data related provisions had provisions that are categorized as establishing rights or obligations for the parties. The category was however quite diversified. This meant that not all of the seven included a comprehensive set of provision with regards to non-personal data related rights and obligations but covered only some issues.

A central aspect of data licensing agreement suggested in the OAD report was that a data licence should as a main rule allocate the data to the other party and then grant specific exceptions to the main rule. [209] This provision seems to do exactly that, as the first subclause provides that all data belongs to the customer and the second that the vendor has only a right to use the date for the supply:

> 13.3 All intellectual property rights to documents, data and other results created in the performance of the Services shall vest in the Customer.
> 13.4 The vendor shall have the right to use the information, materials, data and intellectual property rights defined in Clauses 13.1 and 13.3 only in the extent needed for the supply.[210]

One of the provisions where data was mentioned was a limitation of liabilities provision where loss of data was mentioned as one situation where a contracting party would not be liable for the damage caused to the other party. This shows that drafter of the terms acknowledges the importance of data for the possible agreement and wishes to limit the possible consequences of data loss.

> In no event shall either Party be liable to the other Party, in contract (including breach of warranty), tort, negligence, strict liability, breach of statutory duty or otherwise, for any ... (e) loss of use or corruption of software, data or information...[211]

[209] Osborne Clarke LLP 2016 90.
[210] Metsä Group General Terms and Conditions for Purchases of Goods and Services 2017 13.
[211] Neste General Terms & Conditions for Sales and Purchases of Crude Oil and Products 2017 7.1.

Another provision, with the heading ‘data protection’, was drafted interestingly in such a way that it is unclear whether it was intended to include only personal data or also non-personal data:

> The data necessary for contract fulfilment is recorded in compliance with the appropriate legal requirements. When processing an order or providing a service, data may be transmitted to Affiliates and third parties for the purposes of contract fulfilment and commissioned data processing. The Purchaser acknowledges that data may be transmitted to countries which are not members of the European Union and which are not in accordance with the European data protection standards. The Supplier may also use the data collected during the business relationship with the Purchaser to inform the Purchaser about the Supplier's products. In case the Purchaser does not want to receive such information, it may at any time notify the Supplier accordingly.[212]

The general terms and conditions where the provision appears is dated to October 2016, five months after the GDPR entered into force but before it was applicable (Art. 99 GDPR). Thus the spirit of the GDPR and its requirements can be seen in how the provisions describe data recording to be compliant with legal requirement and how the issue of transferring data outside the European union is handled (Art. 3 GDPR). However, nothing in the provision suggests that its scope would be limited to personal data. Thus, the provision could be seen as granting the parties a right to transmit data to their affiliates and third parties, as long as the transmission is aimed at fulfilling the purposes of the contract and commissioned data processing. The later requirement could be seen as requiring the parties to explicitly agree that their contractual relationship includes processing data. What these provisions do not seem to make possible is to use the data to develop the Supplier’s product. This can be viewed as a deficiency because then data cannot be fed to data-value chain feedback loop which is one of the most lucrative aspects of data economy. It can be asked, would it not be beneficial to separate personal data and non-personal data contract terms clearly, as the use of stricter personal data legislation to model provisions limits the use of non-personal data for no reason. From standpoint of maximizing valuable data, the above provision is clearly suboptimal.

On the contrary, another provision seems to provide a party with the possibility to use collected data to extra-contractual activities, such as product development. Here the word “belong” is used to create an ownership-like, all-encompassing, *inter partes* right to data which probably also aims at precluding the other party from using the data. The provision also enables the sharing of data to third parties:

> The Supplier agrees that the Technical Data shall belong to Wärtsilä, and shall be transmitted to Wärtsilä for purposes including, but not limited to, developing its products, solutions and services. Wärtsilä shall own all works, products, reports and improvements

[212] General Sales Terms of Upm-Kymmene Group for Paper Products and Services 2016 14.

> based upon, derived from or incorporating Technical Data may be transferred to (a) Wärtsilä affiliates and (b) to third parties who act for or on Wärtsilä behalf for processing in accordance with the non-exclusive purpose(s) listed above or as may otherwise be lawfully processed.[213]

Similarly, the general conditions of service of Kalmar, a Cargotec subsidiary, provide them a right to install a remote diagnostic tool to their product and then use it to gather data to purposes that go beyond the scope of the contract. In this provision the right of the other party to use data is not precluded as it was in the previous.

> Kalmar shall have the right, notwithstanding any other terms and conditions of the Contract, to install remote diagnostic tools into the Equipment and gather and store Equipment related data during and after the term of the Contract including but not limited to information concerning efficiency, availability, condition and downtime of the Equipment. Such information may be used for optimizing the Equipment or the related services as well as for Kalmar's internal business purposes. Kalmar shall be responsible for complying with applicable laws and regulations[214]

Optimizing the equipment or related services and the company's internal purposes can be seen as a relatively wide use right of data though it does not allow sharing of data to third parties. On the other hand it is balanced with the company's responsibility to comply with applicable regulation.

This provision by Konecranes US subsidiary also creates a nonexclusive licence to use data to internal purposes, thus third party sharing of data is not possible. The nature of the nonexclusive licence is well established though as it is described as worldwide, irrevocable and royalty free.

> Buyer hereby grants to Seller a worldwide, irrevocable, royalty-free, nonexclusive license to collect, store and use any data collected by Seller through a Data Connection (as defined below) for any internal purposes of Seller, including but not limited to research and development.[215]

If we compare these data related provisions, we see that they handle two issues differently. Firstly whether they allocate one party an ownership-like exclusive right or whether they allocate a party nonexclusive licence to use data for specific purposes only. Secondly, we see that some provisions allow sharing the data to third-parties. However, none of these general terms and conditions explicitly state that data would be sold or licensed to third-parties. This may be purposeful as an open mention could have made the contracting party to question the agreement. On the other hand, sharing data to third-parties could make product development more effective.

---

[213] Wärtsilä General Terms and Conditions for Supply and Purchase 2018 3.19.
[214] Kalmar General Conditions of Service 2016 14.4.
[215] Konecranes USA Standard Terms and Conditions of Sale (Equipment) 2016 11.

Data and third parties related provisions

The hypothesis for this category was to find provisions which require the data licensee to forward any obligation to its sublicensees. However, these kinds of provisions were not found. There could be a few reasons. One is that as the provisions reviewed were those of general terms and conditions the more sophisticated data related issues would be handled in separate data licensing agreements. Another possible reason is that companies do not embrace data as a sharable asset, the value of which could increase during the sharing process. If data is only seen as something that is transferred within the dyadic relationship between the contracting parties, data-based transactions are simpler to understand than within a multilateral network of different actors.

The only provision where third-parties were mentioned was a provision that allows the sharing of data to a third party instead of hindering it. While a lack of such provision would not necessarily mean that data cannot be shared, the explicit permission is more evident for the contracting parties and might reduce different interpretations:

> Technical Data may be transferred to (a) Wärtsilä affiliates and (b) to third parties who act for or on Wärtsilä's behalf for processing in accordance with the non-exclusive purpose(s) listed above or as may otherwise be lawfully processed. [216]

None of the provisions found hindered other third-parties ability to use non-personal data if they somehow received it from the parties. This is positive regarding contracts law ability to allocate data effectively.

Provisions that strengthen the execution of agreement

The category of provisions that aim to strengthen the execution of agreement comprised of four provisions that were quite dissimilar in nature. This was not unexpected as several kinds of provisions fell under the category.

This provision aimed to make sure that the data collection is not affected by ending of the contract or any other events between the parties. This reflects the aim to make sure that no restrictions hinder the use of data even after other contracts between parties have been signed or in case the contract is terminated:

> Wärtsilä's rights to use Technical Data shall survive the termination or expiration of this Agreement, any applicable warranty period and any other commercial contract between the Supplier and Wärtsilä. [217]

---

[216] Wärtsilä General Terms and Conditions for Supply and Purchase 2018 3.19.
[217] Wärtsilä General Terms and Conditions for Supply and Purchase 2018 3.19.

The other provisions aimed at strengthening the agreement by committing the other contracting party to certain legal or technical conditions. For example, the other party was obliged to enter data security agreement if they were granted access to the other party's system: "Upon Purchaser's request, a confidentiality and data security agreement in case of access to Purchaser's information systems is granted, shall be made.".[218]

Another provision provided how data is in practise accessed by the other party and placed its contracting party under obligations that would make the access to data *de facto* possible:

> The goods purchased by Buyer may have functionality through an included data connection ("Data Connection") that monitors, transmits and records data related to certain aspects of equipment usage. Buyer acknowledges and agrees that Seller may activate the Data Connection immediately upon or at any time following installation of goods or equipment and the data collected will be transmitted to and collected by Seller or its affiliates through the Data Connection.[219]

Also data security related obligations were placed upon the other party. For example, here supplier was required to protect its contracting party from loss and alteration of data or from intrusions that could result in it:

> Supplier shall take appropriate precautions to a) prevent loss and alteration of any data or programs, b) to prevent improper access to Purchaser's information and communications technology (ICT) environment or confidential information and c) prevent introduction of viruses, worms, spyware or the like malware to Purchaser's ICT environment. Supplier shall comply with Purchaser's information security requirements.[220]

Summing up the findings

Considering the goals of data value maximization and pareto improvements both could be found in the provisions. Many provisions aimed at maximising the data available to the party suggesting the terms and conditions. However none of the provisions can be seen as putting one of the parties in worse position than they would have been without the data license, thus all the examined provisions can be seen as pareto improvements. On the other hand, in many cases the other party did not, at least directly gain, anything from giving access to its data to the party suggesting the terms and conditions. Pareto efficiency is however difficult to evaluate. In some cases for example, granting sensor-providers exclusive rights to non-personal data may incentivise them to manufacture more useful products to sensor base providers (end-users). Due

[218] Valmet General Purchase Conditions GPC 2015 5.2.3.
[219] Konecranes USA Standard Terms and Conditions of Sale (Equipment) 2016 15.
[220] Fortum's General Terms and Conditions for Procurement of Products and Services 2018 18.2.

to this dynamic effect, even excluding the sensor base provider from data collected by the sensor-provider on the sensor base could in some cases be indirectly pareto optimal.

Of course, it was expected that complicated data provisions would not be found in the general terms and conditions documents. If this finding is put into context with the discussions about the growing importance of data as an ingredient in the value creation for example within the Internet of Things context it is somewhat surprising that most general terms and conditions lack non-personal data related provisions. Especially the small number of data definitions is fascinating, as it suggests that attention has not been paid on what data is and what distinctive issues data as commodity creates.

It is also interesting to note what is missing from the general terms and conditions reviewed. For example, no provisions requiring deletion of data after the termination of contract were found. This was likely because the reviewed documents, the general terms and conditions, where one-sided propositions for agreements and perhaps these kinds of provisions would have been included in the final, negotiated agreement. Also as noted above there were no obligations to forward duties between contracting parties to third-party sublicensees. Nor were there any conditions that would have required the licensee to impose direct contractual claims between the data licensor and the sublicensee of data.

As it is hard to valuate data, contractual penalties have been suggested as remedies for non-compliance with data related provisions.[221] Within the reviewed documents no contractual penalties were found. Possible reasons for these are again multiple. Perhaps contractual penalties that would be specific for data are considered too conspicuous if data licensing is not the main purpose of the agreement. Maybe, contractual penalties would be more suitable for stand-alone data licensing agreements.

Also, all the found general terms and conditions were of general nature. If data sharing was provided for in the contracts, it was for all data instead of some data. This is peculiar as one could ask why in all these cases a dichotomy of all data being shared or none is the most efficient, instead of the parties choosing what data should be shared and what data should not be shared. Perhaps once again, these kinds of more complex and more detailed questions are felt better left to be answered in special data licence agreements.

In addition, co-possession of data is advocated in none of the general terms and conditions even though it could be an efficient way to allocate data keeping in mind its characteristics. Either it

[221] Osborne Clarke LLP 2016 93.

has not been thought of by the drafters or it has not been considered a viable option as being too uncertain for example. Or, maybe it has been considered too complicated for the general terms and conditions documents and if such arrangements have been deemed useful, they have been introduced in special agreements. However, from a macro economical point of view this could be criticised as there is no reason to believe that exclusionary data licensing is the most effective way to allocate data.

On the other hand, there were some provisions that were not mentioned in the OAD report such as those regarding limitations of liability. If the data licensing may result in significant liability for example due to data erroneously recording certain events that results in economic or other harm, such provisions can be lucrative for companies.

The provisions of the general terms and conditions were reflected on the principles of neoclassical economics, data value maximization and pareto improvements. Another viewpoint could have been public policy goals such as the EU Commission's key principles for business to business sharing: 1) transparency, 2) shared value creation 3) respect for each other's commercial interests 4) ensuring undistorted competition 5) minimised data lock-in.[222] According to the Commission, transparency consists of contractual provisions that transparently identify who will have and what kind of access to data and for what purpose. [223] All of the requirements for transparency were hardly met in any of the agreements but, for example Kalmar's provision which defined that data will be 'used for optimizing the Equipment or the related services as well as for Kalmar's internal business purposes' can be seen as transparent regarding the purpose of data use.[224] Shared-value creation was not identified in the provisions examined. Respect for other's commercial interests cannot be assessed based on the general terms and conditions as the other party has yet to agree on their terms. No provisions that could *per se* be argued to hinder competition were found. Considering data lock-in, there were no contractual provisions that would have required the sensor base providers to only share data with sensor-providers.

5.4. Reflections

Contract law is identified both in theory and in practise as the most appropriate legal regime for the management of rights to non-personal data. The question, however, is, whether contract law

[222] COM(2018) 232 Final. 10.
[223] COM(2018) 232 Final. 10.
[224] Kalmar General Conditions of Service 2016 14.4.

practises function optimally in that regard. Eigen has suggested the assumed behaviour of contracting parties in a free market economy can be viewed as follows:

1) parties know what they want (they understand their preferences),
2) they have relatively clear expectations about what their contracting counterparts want (they have a good sense of their counterparts' preferences);
3) they understand when they have entered into a contract;
4) they generally feel bound to perform as obligated by lawful contracts into which they knowingly entered; and,
5) if they breach, they know that they are breaching.[225]

After empirically analysing the general terms and conditions we see that these criteria are clearly not fulfilled regarding most companies' clauses considering non-personal data. Of course, these were their general terms and conditions and companies might use more sophisticated provisions when they engage in relationships they see as more data intensive. However for example the way data is defined points out to ambiguities and suggest that these issues might not be considered important or the understanding of their importance does not manifest in contractual clauses.

One conclusion could be that the companies have not identified their position within the data value chain[226]. This prevents them from choosing the appropriate contracting practises, for example, regarding third-parties and implies that these companies have not considered non-personal data to be a strategically important asset.

Imbalance between contracting parties is a risk if contract law is the main legal instrument relied on. Will contracts be too restrictive for markets to allocate the rights to data efficiently? Or indeed, are the provisions overly restrictive even from the companies' point of view? The Free-Flow of Non-Personal Data Regulation and its non-binding industry best practises could provide some solutions to the issue as they are prepared together with representatives from small and middle-sized enterprises and start-ups and facilitated by the Commission (Art.6).

The legal implication of different data licencing provisions will remain unclear until courts develop case law regarding these provisions.[227] The problem is that it can take quite a while for the case law to develop. Also, as contract law mainly falls within national jurisdictions, courts

[225] Eigen 2012 3.
[226] Lim et al.2018 125–126.
[227] Osborne Clarke LLP 2016 99.

in different Member States, or in some cases the CJEU, may reach dissimilar outcomes considering data licensing provisions.

However, the uncertainty should not prevent companies from introducing data related provisions in their agreements since the possibilities of data economy are so advantageous. Also, the risk of not contracting could be thought as a bigger problem. Decision not to enter into contracts is also a decision and that decision leaves the data without even contractual protections.

In addition companies should focus on how data is defined. Currently data is used to refer to different concepts such as software object code, which of course, can be distilled to mere data but also is protected by intellectual property regimes, such as copyright and related rights and the entitlements related to it. Similar issue considers trade secrets and personal data which should not be confused with non-personal data. In many cases, being ambiguous regarding legal concepts creates ineffectiveness as different legal concepts are protected by different legal regimes.

Keeping this restriction in mind, contract law is a promising tool for managing non-personal data. However if attention is not paid to the management of non-personal data and data provisions are created ‘just to be safe’ it is not appropriate and may result in unforeseen consequences.

One aspect which favours contract law is that contractual remedies can easily be set by the parties before they enter into contract. Therefore no valuation problems will emerge if the transactions end up to litigation. Nor is the state left pondering if some kind of injunction would be an efficient remedy as the parties may have agreed whether is to be granted in case of breach of contract or not.

6. CONCLUSIONS

The research question of this thesis was *how private market actors can get access to non-personal data and to restrict others from using non-personal data*. The general-level answer formulated in this work is that companies can manage rights to non-personal data either directly through contracts or indirectly using legal, technical and business practises while taking into consideration characteristics of data as an asset and the relevant legislation that affects non-personal data. Metaphorically speaking, the legal environment constitutes the walls and ceiling of the bakery where the direct and indirect management practises can be used to make bread, to extract value, out of the ingredient, non-personal data.

Roles of sensor base possessor, sensor provider, data platform provider and data user were conceptualized for better understanding of the different relationships in which non-personal data is managed and how those relationships affect what the most suitable ways of managing data are. These roles were seen to affect what kind of practises a company should seek to use when it manages non-personal data. The concept of sensor base possessor allowed analysing the legal position of users of Internet of Things objects.

One of the challenges regarding the management of rights on non-personal data that popped out continuously as a finding was the inconsistency of terms such as data and information within both public and private regulation. This problem of conceptualization of data could be seen as a key deficiency concerning regulation of non-personal data. These problems within the conceptual network around data leaves the norms without stable legal meaning which results in problems when intention of both legislators and parties to contracts are unclear, for example whether they intended to protect data or information. If the conceptual framework is not clear, it is difficult to see what for example non-personal data related litigation would be about?

I believe that ambiguous conceptualisation of non-personal data lessens the efficiency of regulation and contracts. The main point of this critique is not that for example concepts from computer studies should be used as such in legal texts, but that legal texts should be able to dictate clearly what their intention is. A practical solution to this problem might come when best practises regarding data definitions and the quality of data are created for example based on the Free-Flow of Non-Personal Data Regulation. Another option to solve these problems could be standards by industries or perhaps standards within the ISO system which could ease data sharing even beyond the borders of the EU.[228]

[228] Considering ISO standardisation, see Hoeren 2017 37.

In regard to conceptualization, a rather simple but important finding was, that due to the EU's two regulations on data (GDPR and the Free-Flow of Non-Personal Data Regulation) the distinction between personal and non-personal data is legally useful for companies. Even though both areas may in practise have some overlaps, regulation on non-personal data is so weak that making a company level distinction on the two types of data enables maximization of valuable data both taking advantage of non-personal data and using personal data in accordance with the applicable law.

The CJEU will most likely have a key role in shaping out the legislation, for example regarding the uncertainties of the Trade Secrets Directive.[229] What businesses will be looking forward to is legal certainty. While property rights have not been defined nor allocated the legislator has left a lot of regulatory interpretation in the hands of the judiciary. Perhaps the judiciary can better and more dynamically consider how the markets evolve. On the other hand the court system clarifies regulation from *ex post* point of view which means that some established practises may be challenged by court decisions.

A few remarks de lege ferenda

> The development of the legal-regulatory system, much as the development of other economic institutions, is not an outcome of a fully rational choice of "optimal" solutions, but rather a gradual, incremental and evolutionary process. Moreover, to the extent that the process through which economic forces shape the legal system is itself a form of competitive and evolutionary mechanism, it reveals a number of similarities to the market and should be analyzed with the help of some of the same tools as those used to explain economic phenomena
>
> Instead, contrary to the common economists' assumption that a system of property rights is a precondition of a market economy, the development of market institutions is often a prerequisite for a viable private property regime.[230]

The above quotation by Rapaczynski contemplates the role of state and the market in establishing property rights in post-soviet Eastern Europe. While the context of the extract is quite different compared to non-personal data, Rapaczynski describes stunningly how the relationship between state allocating entitlements and economy is far from linear. Market institutions and property rights interrelate one another and neither can develop without the other.

---

[229] Osborne Clarke LLP 2016 11.

[230] Rapaczynski 1996 102. Similar views have been presented in markets-as-practice literature which is an approach of economic and cultural sociology. The approach holds that the ideas of different market actors, such as businesses, consumers and governments bring markets into existence. See for example, Kaartamo – Pelto 2017.

When rights are created on intangible assets, how the rights represent the objects is always interesting and political. For example considering the copyright protection of films, Anne Barron has argued that the nature of United Kingdom's copyright law has hovered between formalism that does not consider the specificities of film and physicalism that reduces film to physical entity.[231] Similarly, non-personal data can be approached using these two different angles and the choice between them could benefit others while leaving others in poorer situations.

Throughout the thesis, the framework suggested by Calabresi and Melamed was used to analyse the options of legislator regarding allocating entitlements to non-personal data. Curiously, the most useful view to their framework was not the distinction between liability and property rules but the question whether the legislator is at all allocating the entitlements. While Calabresi and Melamed reflected in what situations a liability rule would be more suitable than a property rule, in the context of non-personal data the framework seems ill-suited. How does a liability rule work when there is no clear set of rules based on which the courts could value data? How does property rule work when its object of protection is mouldable, inexhaustible, non-rivalrous and non-exclusive? However, the framework provided a good tool for seeing how different data is as an asset compared to other tangible and intangible assets. One could argue that with the growing importance of non-personal data as an asset, Calabresi and Melamed's theory is being empirically tested, albeit with such a peculiar asset as data.

A stakeholder dialogue conducted by the Commission provided that stakeholders view the current regulatory framework as sufficient for development of data economy. Freedom of contract was seen as a functioning cornerstone for the development of business-to-business data exchange. 'Data-ownership' right was not favoured by the stakeholders.[232]

If immaterial property rights for data were to be introduced, they should only be developed with diligent law and economics analysis. Legislation may be difficult to enact when data economy is developing, and technology and data related commercial practises evolve. For example, the OAD report noted that maturing of the commercial and legal landscape might have to be waited, before deciding the legislative response to the property law status of data.[233] What seems clear is that the issue of non-personal data should be legislated at the EU level. The data market is at least union wide. Perhaps even international cooperation would be beneficial to avoid local

[231] Barron 2004 193–194.
[232] COM(2018) 232 Final. 9.
[233] Osborne Clarke LLP 2016 7.

regimes such as the database *sui generis* protection. That way the global economy could benefit from the characteristic of data as easily transferrable asset.

If markets are working efficiently, as they should, non-personal data should be allocated efficiently. As data economy and the markets for non-personal data are growing, research on non-personal data will be needed also from competition law point of view, so that the efficiency of this growing market will be verified. Issues, such as, are certain actors excluded from data markets will need to be studied. Also for example regarding SMEs, questions such as does the Commission facilitated codes of conduct put SMEs in better position than without them, could be interesting.

There has been some discussion if a special access right should be created for data. Speaking to an audience from the German Association for the Protection of Intellectual Property (GRUR), Michael König, the department head of intellectual property at Directorate-General GROW presented three options for data-access regime. The first option was relying on the market forces, the second a competition law inspired predefined regime and the third a regime of default access with exceptions and defences.[234] In the legislative process the first option seems to have been chosen with the introduction of the Free Flow of Non-Personal Data Regulation, but that does not mean that the other two options could not be dig up if need be. Max Planck Institute has also pointed out that a specific need for an access right regime could arise within a particular sector, due to public interest requirements for example.[235]

The field is transforming fast due to technological, political and legal changes. Therefore it is possible that new issues will emerge rapidly. Also, when first case law regarding non-personal data will be presented it will direct the behaviour of market actors even without further legislative developments. Therefore it is important that the issue of managing non-personal data is researched in the future. This allows the legislator and the judiciary, as well as private actors, to come up with effective regulation.

Writing about intellectual property intermediaries and injunctions against them, Husovec has suggested that effective legal regimes take into account all costs that result from their use. These costs include direct expenses to parties for requesting or administering the remedies as well as costs to state for administering the remedies. In addition to these direct cost, indirect costs arising from use of the measures, such as hindering of societal or technological developments,

[234] König 2016 7.
[235] Drexl et al. 2016 11–12.

need to be regarded.[236] Similarly, the dynamic societal and technological developments should be considered before introducing any legal regimes related to non-personal data. As these developments are difficult to predict, it may be safest not to place too much regulation on data markets. The same is true regarding future case law and courts should consider the dynamic effects of their rulings so that future technological or business developments are not hindered unnecessarily.

Since data economy is expected to grow and the regulatory field may change, research on the topic is needed also in the future. For example, due to the important role of contracts in the data economy, an empirical study on data licence agreements could provide information regarding current practises. In addition, the role of sensor base providers should be studied, both upstream and downstream, in a value chain for data. Also, the relationship between non-personal and personal data should be further studied, as both the GDPR and the Free-Flow of Non-Personal Data Regulation were only just introduced.

[236] Husovec 2017 26–27.

Attachments

Attachment 1: Findings in the GTCs

Company	Agreement	Year	Data clauses	C1 = Data described	C2 = Data related rights and obligations	C3 = Data and third-parties	C4 = Execution of agreement strengthened	Confidentiality provisions	Document name	Website
Nokia Oyj	Supply	2017	Yes	Supplier warrants that any data and other information provided to Nokia under this clause are in all respects complete and correct.					General Terms and Conditions for the Purchase of Hardware and Software, 2017	https://www.nokia.com/sites/default/files/general_terms_and_conditions_for_hw_and_sw_2.pdf
Neste Oyj	Supply and customer	2017	Yes		7.1 In no event shall either Party be liable to the other Party, in contract (including breach of warranty), tort, negligence, strict liability, breach of statutory duty or otherwise, for any ... (e) loss of use or corruption of software, data or information....			23.1 The Parties agree that the terms of the Agreement and all information disclosed under the Agreement, except for information in the public domain, shall be considered confidential and shall not be disclosed to any other person without the prior written consent of the Party which owns such confidential information. This obligation of confidentiality shall remain in force during the term of the Agreement and for a period of five (5) years thereafter.	General Terms and Conditions for Sales and Purchase of Crude Oil and Products.	https://www.neste.com/sites/default/files/attachments/neste_gtcs_2017.pdf
UPM-Kymmene Oyj	Customer	2016	Yes		The data necessary for contract fulfilment is recorded in compliance with the appropriate legal				General Sales Terms of Upm-Kymmene Group	http://assets-upmpaper.upm.com/Shared%20Docume

					requirements. When processing an order or providing a service, data may be transmitted to Affiliates and third parties for the purposes of contract fulfilment and commissioned data processing. The Purchaser acknowledges that data may be transmitted to countries which are not members of the European Union and which are not in accordance with the European data protection standards. The Supplier may also use the data collected during the business relationship with the Purchaser to inform the Purchaser about the Supplier's products. In case the Purchaser does not want to receive such information, it may at any time notify the Supplier accordingly				for Paper Products and Services	nts/services/general-terms-2016-in-english.pdf
KONE Oyj	Supply	2016	Yes		7 Confidentiality 7.1 The supplier shall not disclose to third parties nor use for any other purpose than the proper fulfillment of this Agreement any information of confidential nature, such as technical information and data, drawings, price structures, costs, and volume information, received from the purchaser ("Information"), without the prior written permission of the purchaser, except Information which (a) was in possession of the supplier prior to disclosure hereunder; (b) was or becomes part of the public domain without breach of the confidentiality obligations herein; or (c) was independently developed by personnel of the supplier having no access to the Information.				KONE General Terms and Conditions of Purchase ("GTC")	https://www.kone.co.il/en/Images/brochure-general-terms-and-conditions-for-suppliers_tcm202-68608.pdf
Metsäliitto-konserni	Supply	2017	Yes		13.1 All rights to the documents and other materials (e. g. plans, drawings, technical documents, software) made available by the Customer to the Vendor for the supply of the Goods and/or the fulfilment of the Services shall remain the property of the Customer. 13.2 The Vendor is responsible for making sure that no rights of third parties will be infringed in conjunction with the supply of				General Terms and Conditions for Purchase of Goods and Services	https://www.metsagroup.com/en/Documents/Purchasing/General-Purchasing-Conditions-of-Goods-and-Services.pdf

					the Goods and/or performance of the Services. 13.3 All intellectual property rights to documents, data and other results created in the performance of the Services shall vest in the Customer. 13.4 The vendor shall have the right to use the information, materials, data and intellectual property rights defined in Clauses 13.1 and 13.3 only in the extent needed for the supply					
Wärtsilä Oyj Abp	Supply	2018	Yes	2.9 "Technical Data" refers to all data relating to the technical operating parameters of any Supply delivered, including without limitation, all information gathered from sensors, instruments, monitors, or other industrial control or SCADA devices located at the Wärtsilä end-customer's site or on the Supply	The Supplier agrees that the Technical Data shall belong to Wärtsilä, and shall be transmitted to Wärtsilä for purposes including, but not limited to, developing its products, solutions and services. Wärtsilä shall own all works, products, reports and improvements based upon, derived from or incorporating Technical Data may be transferred to (a) Wärtsilä affiliates and (b) to third parties who act for or on Wärtsilä's behalf for processing in accordance with the non-exclusive purpose(s) listed above or as may otherwise be lawfully processed.	Technical Data may be transferred to (a) Wärtsilä affiliates and (b) to third parties who act for or on Wärtsilä's behalf for processing in accordance with the non-exclusive purpose(s) listed above or as may otherwise be lawfully processed.	Wärtsilä's rights to use Technical Data shall survive the termination or expiration of this Agreement, any applicable warranty period and any other commercial contract between the Supplier and Wärtsilä.		General Terms and Conditions Supply and Purchase	https://cdn.wartsila.com/docs/default-source/default-document-library/gtc-supply-and-purchase-2018.pdf?sfvrsn=6c7bea44_4
Fortum Oyj	Supply	2018	Yes				Supplier shall take appropriate precautions to a) prevent loss and alteration of any data or programs, b) to prevent improper access to Purchaser's information and communications technology (ICT) environment or confidential information and c) prevent introduction of viruses, worms, spyware or the like malware to Purchaser's ICT environment. Supplier shall comply with		Fortum's General Terms and Conditions for Procurement of Products and Services	https://www.fortum.com/sites/g/files/rkxjap146/files/documents/fortum_s_general_terms_and_conditions_4.6.2018.pdf

							Purchaser's information security requirements.			
Cargotec Oyj	Customer	2016	Yes		All intellectual property rights related to the Services and Products delivered by Kalmar including, without limitation, any and all software and/or documentation or data included in, with or comprising Products or Services ("IPR"), and all ownership rights in and to the IPR shall remain solely and exclusively with Kalmar. 14.4 Kalmar shall have the right, notwithstanding any other terms and conditions of the Contract, to install remote diagnostic tools into the Equipment and gather and store Equipment related data during and after the term of the Contract including but not limited to information concerning efficiency, availability, condition and downtime of the Equipment. Such information may be used for optimizing the Equipment or the related services as well as for Kalmar's internal business purposes. Kalmar shall be responsible for complying with applicable laws and regulations				General Conditions of Service	https://www.kalmarglobal.be/globalassets/services/kalmar-general-conditions-of-service-2016.pdf
Valmet Oyj	Supply	2015	Yes				Upon Purchaser's request, a confidentiality and data security agreement in case of access to Purchaser's information systems is granted, shall be made.		General Purchase Conditions GPC 2015	https://www.valmet.com/globalassets/about-us/procurement/valmet-gpc-2015.pdf
Konecranes Oyj	Customer	2016	Yes		Buyer hereby grants to Seller a worldwide, irrevocable, royalty-free, nonexclusive license to collect, store and use any data collected by Seller through a Data Connection (as defined below) for any internal purposes of Seller, including but not limited to research and development.		The goods purchased by Buyer may have functionality through an included data connection ("Data Connection") that monitors, transmits and records data related to certain aspects of equipment usage. Buyer acknowledges and agrees that Seller may activate the Data Connection immediately upon or at any time following installation of goods or equipment and the data collected will be transmitted to and collected by Seller or its affiliates through the Data Connection.		Standard Terms and Conditions of Sale (Equipment)	https://www.konecranesusa.com/sites/default/files/download/industrial_cranes_beta_-_us_terms_and_conditions_08.01.2016_english.pdf