FROM SIMPLY SHARING THE CAGE TO LIVING TOGETHER

RECONCILING THE RIGHT OF PUBLIC ACCESS TO DOCUMENTS WITH THE PROTECTION OF PERSONAL DATA IN THE EUROPEAN LEGAL FRAMEWORK

Anu Talus

DOCTORAL DISSERTATION

to be presented for public examination
with the permission of the Faculty of Law of the University of Helsinki,
in Hall Suomen laki, Porthania,
on the 30th of November, 2019 at 12 o'clock.

Helsinki 2019

ISBN 978-951-51-5632-7 (nid.)
ISBN 978-951-51-5633-4 (PDF)

Unigrafia, Helsinki 2019

ACKNOWLEDGEMENTS

Writing this thesis has been a long journey, a journey which I have enjoyed nearly all the way through. When returning to the Ministry of Justice after a research period in 2012, my plan was to finalize the thesis in one year. But you cannot always plan life. I started working with the most intriguing file, which eventually occupied also my free-time, the GDPR negotiations. However, at no point I was willing to compromise my redlines; I only worked on my thesis when I had the spirit for it. Luckily this was often enough.

I would not have been able to finish this journey without the involvement of the people I am surrounded with. I can mention only few, but also those not mentioned here have contributed various ways to my work, which I am very grateful for.

First, I want to thank Professor Tuomas Ojanen. I very much appreciate your availability throughout this project, it has been a true pleasure working with you. I am also very thankful for my preliminary examiners, Chancellor of Justice Tuomas Pöysti and Professor Maja Brkan. I appreciate that you were willing to invest your time in my project and I found your comments on the draft version of the thesis very valuable. Thank you. I also want to thank Professor Richard Rawlings for his comments on the early version of the thesis. I have also had very fruitful discussions with Professor Päivi Leino-Sandberg and Liisa Leppävirta, who gave very detailed comments on the Transparency Chapter, which I am thankful for. Emeritus Professor Ahti Saarenpää has been a great inspiration and the very reason I caught up in the data protection in the first place.

I would also like to thank Niilo Helanderin Säätiö and Suomalainen Lakimies-yhdistys for their generous funding of the thesis. I also want to thank Kate Nascimento for the language check of my thesis.

I have also had a great benefit from the discussions and exchange of thoughts with some of the finest experts in this field when carrying out my duties as civil servant. I am particularly thankful for my colleagues in the DAPIX working party for all the fascinating discussions we had over the years. Seamus, Katrin, Jörg, Jeroen, Johan, Peter, David H., David T., John, Natalie, Damien, just to name some, it was a priviledge to share thoughts on the GDPR and data protection with you all. Those years are certainly one of the most exhausting period of my life, but at the same time so very rewarding. I am also grateful for Bruno Gencarelli and Ralf Sauer for my learning time with the European Commission. I also want to thank Leena Rantalankila, Pekka Nurmi, Eeva Aittoniemi and Anna-Elina Pohjolainen for their input in my project. And finally, Reijo Aarnio, I very much value the countless opportunities, which I have had and still have, to exchange thoughts with you.

Oscar, Nathalie, Ricardo and Hugo. You have made my life much richer now for nearly 30 years. Bad days would have been much worse without your compassion and your capability to make me laugh.

And lastly, the most important, my family. My sister Reetta together with her family, I am very grateful for the dedication you have shown to my children. Mom and Dad, it is beyond words how much I appreciate your support. Not only has it made possible for me to pursue my career and goals, but even more importantly, your support has made it possible to provide sound surroundings for Bea and Cilla to grow up. Bea and Cilla you are my precious. You bring balance to my life.

ABSTRACT

In essence, the transparency and data protection regimes draw from different grounds. The aim of the research was to first identify and analyze the different requirements of the transparency and data protection regimes and thereafter seek the solution for balancing the said requirements. The rules examined in this research regulate the disclosure of information and processing of personal data by the EU institutions. However, the solution for the tension is sought from the European law in a wider perspective.

The analysis of the colliding rules draws from normative legal analysis. Critical legal positivism considers the rules only examples of issues pertaining to the surface level of law and this research draws essentially from the separation of rules and principles based on the doctrines elaborated by such scholars as Ronald Dworkin and Robert Alexy.

The requirements drawing from the data protection legislation and the transparency legislation are contradictory to a certain extent and the tension on the level of rules is apparent. The most apparent contradiction relates to the purpose limitation principle which closely relates to the further processing of personal data and the requirements to reason the disclosure of personal data. Simultaneously, the public access regime builds on a basis where applications for the requests of information do not need to be reasoned.

However, the collision of rules does not necessarily reflect a collision of the underlying principles and the research will seek the balance between the examined rules by reconciling the underlying principles of the data protection and public access to documents regimes.

After the essence of the examined rights has been identified, it will become clear that the collision does not exist on the level of principles. Besides privacy and self-determination, the requirement to have legal basis is considered to form the hard core of protection of personal data. This element also separates it from privacy. It follows that the right to protection of personal data can be reconciled with the right to public access to documents while the essence of both rights are preserved. A suggestion how to reconcile the examined rights will be given and the concluding analysis will also provide tools for balancing the said rights in the current legal framework by interpretation.

There has been earlier study in this field of law. However, this study dates from 2007 and significant changes have taken place after that. A recast process on the Regulation 1049/2001 on public access to documents has been launched and a vast EU data protection reform was finished in the spring 2016. Also, the Court of Justice of the European Union has delivered significant decisions concerning

the relationship between protection of personal data and transparency after 2007. Besides providing a new angle for seeking the solution by balancing the underlying principles, this research also provides first analysis of the relationship between protection of personal data and transparency in the current legal framework.

Keywords
data protection, privacy, personal data, transparency, purpose limitation, further processing, block exemption, democracy

TABLE OF CONTENTS

BIBLIOGRAPHY

BOOKS

Aarnio, A. "On Rules and Principle, A Critical Point of View", in Aerschot (ed.) *Juhlakirja, Kaarlo Tuori, 50 vuotta*, (Helsinki, 1998)

Addink, H. "Principles of Good Governance: Lessons from Administrative Law", in Curtin and Wessel (eds.) *Good Governance and the European Union, Reflections on Concepts, Institutions and Substance*, (Intersentia, 2005)

Alexy, R. "*A Theory of Constitutional Rights*" (Oxford University Press, 2010)

Avril, P. "The democratic institutions of the European countries", in Rieu & Duprat (eds.) *European democratic culture*, (London, 1995)

Bailey, S.H. "*Administrative Law*" (London Sweet & Maxwell, 2005)

Barber, N.W. "A Right to Privacy", in Ziegler (ed.) *Human Rights and Private Law*, (Hart Publishing, 2007)

Bengoetxea, J. "*The Legal Reasoning of the Court of Justice Towards a European Jurisprudence*" (Oxford University Press, 1993)

Bennet C. & C. Raab "*The Governance of Privacy - Policy instruments in global perspective"* (Ashgate Publishing Limited, 2003)

Bicarregui, A. "Rights of Access under European Union Law" in Coppel (ed.) *Information Rights, Law and Practice*, (Oxford, 2010)

Birkinshaw, P. "*Government & Information – the Law Relating to Access, Disclosure & their Regulation*" (Tottel Publishing, 2005)

Birkinshaw, P. "*Freedom of information The Law, the Practice and the Ideal"* (Cambridge, 2010)

Blume, P. *"Juridisk informationssokning"* (Akademisk Forlag, 1998)

Blume, P. "Denmark", in Blume (ed.) *Nordic Data Protection,* (Kauppakaari Oyj, 2001)

Bohlin, A. *"Offentlighets principen"* (Norstedts Juridik, 2001)

Brkan, M. "*The Court of Justice of the EU, privacy and data protection: Judge-made law as a leitmotif in fundamental rights protection*", in Brkan, M. & E. Psychogiopoulou (eds.) Courts, Privacy and Data Protection in the Digital Environment, (Edward Elgar, 2017)

Bronsword, R. "Consent in Data Protection Law: Privacy, Fair Processing and Confidentiality" in S. Gutwith; Y. Poullet; P. De Hert; C. de Terwangne & S. Nouwt (eds.) *Reinventing Data Protection*, (Springen, 2009)

Bygrave, L.A. *"Data Protection Law, Approaching Its Rationale, Logic and Limits"* (Kluwer Law International 2002)

Carey, P. "*Data Protection, A Practical Guide to UK and EU Law*" (Oxford University Press, 2009)

Cariolou, L. "The search for an equilibrium by the European Court of Human Rights", in Brems (ed.) *Conflicts between Fundamental Rights*, (Intersentia, 2008)

Cernic, J. "Democracy as a Trump Card? Combating Hate Speech in Pluralistic Societies", in D. Gozdecka and M.Kmak (eds.) *Europe at the Edge of Pluralism*, (Intersentia, 2015)

Chalmers, D; G. Davies & G. Monti "*European Union Law*" (Cambridge, 2010)

Chydenius, A. "Antti Chydeniuksen omatekoinen elämänkerta", in Kare (ed.) *Anders Chydenius, Suuri Suomalainen valituskirjailija*, (Alea-Kirja, 1986)

Chydenius, A. "*The National Gain"* (London, 1931), translated from the Swedish original published in 1765 with an introduction by Georg Schauman

Deckmyn, V. "*Guide to European Union Information*" (European Institute of Public Administration, 2003)

Delany H. & E. Carolan, "*The Right to Privacy: A doctrinal and Comparative Analysis*" (Thomson Round Hall, 2008)

Driessen, B. "*Transparency in EU Institutional Law: A Practitioner's Handbook*" (Kluwer 2012)

Ducoulombier, P. "Conflicts between Fundamental Rights and the European Court of Human Rights: An Overview", in Brems (ed.) *Conflicts between Fundamental Rights*, (Intersentia, 2008)

Dworkin, R. "*Matter of Principle"* (London, 1985)

Dworkin, R. "*Law's Empire*" (Hart Publishing, 1998)

Dworkin, R. "*Is Democracy Possible Here?*" (Princeton University Press, 2006)

Dworkin, R. "*Taking Rights Seriously"* (Duckworth, 2009)

Ecran, S. "Democratizing Identity Politics: a Deliberative approach to the Politics of Recognition" in D. Gozdecka & M.Kmak (eds.) *Europe at the Edge of Pluralism*, (Intersentia, 2015)

Freeman, J. "Extending Public Accountability through Privatization: from Public Law to Publicization", in Dowdle (ed.) *Public Accountability, Designs, Dilemmas and Experiences* (Cambridge University Press, 2006)

Gerards, J.H. "Fundamental rights and other interests: Should it really make a difference", in Brems (ed.) *Conflicts between Fundamental Rights*, (Intersentia, 2008)

Gisbert, R. "The Right to Freedom of expression in a democratic Society (Art. 20 ECHR)", in Garcia Roca & Santolaya (eds.) *Europe of Rights: A Compendium of the European Convention of Human Rights*, (Leiden, 2012)

Greenstein, S. "*Our Humanity Exposed – Predictive Modelling in a Legal Context*" (Stockholm University, 2017)

Habermas, J. "*Between Facts and Norms*" (The MIT Press, Cambridge, Massachusetts, 1996)

Harmaja, L. "*Antti Chydenius kansantaloudellisena kirjailijana*" (Helsinki, 1929)

Hart, H.L.A. "*Concept of Law*" (Oxford, 1961)

Hesse, K. "*Grundzüge des Verfaussungsrechts der Bundesrepublik Deutschland*" (Heidelberg, 1990)

Hildebrandt, M. "Who is Profiling Who? Invisible Visibility", in S. Gutwith; Y. Poullet; P. De Hert; C. de Terwangne & S. Nouwt (eds.) *Reinventing Data Protection*, (Springen, 2009)

Hirschfeldt, J. "Free access to public documents – a heritage from 1766", in A-S.Lind; J.Reichel & I.Österdahl (eds.), *Transparency in the Future – Swedish Openness 250 years* (Visby, 2017)

Van Hoecke M. & J.Dhont, "Obstacles and Opportunities for the Harmonisation of Law in Europe: Case of Privacy", in V. Heiskainen & K.Kulovesi (eds.) *Function and Future of European Law*, (Helsinki, 1999)

Holm S. & S. Madsen, "Informed consent in medical research – a procedure stretched beyond breaking point?", in O. Corrigan; John McMillian; Kathleen Liddell; M.Richards & C. Wijer (eds.) *The limits of consent, A socio-ethical approach to human subject research in medicine*, (Oxford University Press, 2009)

Hyttinen, P. "*Anders Chydenius, Defender of Freedom and Democracy*" (Kokkola, 1994)

Ieven, A. "Privacy Rights in Conflict: in Search of the Theoretical Framework Behind the European Court of Human Rights' Balancing of Private Life Against Other Rights", in Brems (ed.) *Conflicts Between Fundamental Rights*, (Intersentia, 2008)

Jääskinen, N. "Demokratia vai perusoikeudet?", in Nuolimaa (ed.) *Juhaljulkaisu Pekka Hallberg 1944-12/6-2004*, (Jyväskylä, 2004)

Jääskinen, N. "*Eurooppalaistuvan oikeuden teoreettisia ongelmia*" (Helsinki, 2008)

Karanja, S.K. "*Transparency and Proportionality in the Schengen Information System and Border Control Co-operation*" (Martinus Nijhoff Publishers, 2008)

Kastari, P-L. "*Antti Chydenius ja painovapauden aate*" (Tampereen yliopisto, 1981)

Keane, J. "*The Life and Death of Democracy*" (London, 2009)

Kelsen, H. "*General Theory of Norms*" (Oxford, 1991)

Koops, B-J. "Should ICT Regulation be Technology-Neutral?", in Koops, Lips, Prins & Schellekens (eds.) *Starting Points for ICT Regulation. Deconstructing Prevalent Policy On-Liners*, (Assep Press, 2006)

Kranenborg, H. "*Toegang tot documenten en bescherming van persoonsgegevens in de Europese Unie – Over de openbaarheid van persoonsgegevens*" (Kluwer, 2007)

Kranenborg, H. and W. Voermsns, "*Access to Information in the European Union – A Comparative Analysis of EC and Member State Legislation*" (Groningen, 2005)

Kuner, C. "*European Data Privacy Law and Online Business*" (Oxford University Press, 2003)

Kulla, H. & M.Koillinen, *Julkisuus ja henkilötietojen suoja viranomaistoiminnassa* (Turun yliopisto, 2014)

Lynskey, O. "*The Foundations of EU Data Protection Law"* (Oxford, 2015)

Maes, E. "Constitutional Democracy, Constitutional Interpretation and Conflicting Rights", in Brems (ed.) *Conflicts Between Fundamental Rights*, (Intersentia, 2008)

Manolescu, D. "Data Protection Enforcement: The European Experience – Case Law", in N. Ismail & E.L. Yong Cieh (eds.) *Beyond Data Protection*, (Springer, 2013)

Marauhn T. & N.Puppel, "Balancing Conflicting Human Rights: Konrad Hesse's notion of "Praktische Kokordanz" and the German Federal Constitutional Court", in Brems (ed.) *Conflicts between Fundamental Rights*, (Intersentia, 2008)

Mäenpää, O. "*Julkisuusperiaate*" (Helsinki, 1999)

Neuvonen, R. "*Yksityisyyden suoja Suomessa*" (Lakimiesliiton kustannus, 2014)

Nieto-Garrido, E. & I.A.Delegado, "*European Administrative Law in the Constitutional Treaty*" (Hart Publishing, 2007)

Niiniluoto, I. "*Informaatio, tieto ja yhteiskunta: Filosofinen käsiteanalyysi*" (Helsinki, 1989)

Nissenbaum, H. "*Privacy in context – Technology, Policy, and Integrity of Social Life*" (Stanford University Press, 2010)

Nouwt, S. & B.R. de Vries & R. Loermans, "Analysis of the Country Reports", in S. Nouwt, B.R. de Vries & C.Prins (eds.) *Reasonable Expectations of Privacy? Eleven Country Reports on Camera Surveillance and Workplace Privacy*, (Asser Press, 2005)

Palmen, E.G. "*Anders Chydenius*" (Helsingfors, 1903)

Pöysti, T. "*Tehokkuus, informaatio ja eurooppalainen oikeusalue*" (Helsinki, 1999)

Pöysti, T. "Hallintoeettiset toimintasäännöstöt hyvä hallinnon toteuttamisessa" in I.Koivisto; T.Ojanen; O.Suviranta & M.Sakslin (eds.) *Olli Mäenpää 60 vuotta*, (Edita, 2010)

Raz, J. "*The Authority of Law, Essays on Law and Morality*" (Oxford University Press, 1979)

Reichel, J. "The Swedish right to freedom of speech, EU data protection law and the question of territoriality", in A-S.Lind; J.Reichel & I.Österdahl (eds.) *Transparency in the Future – Swedish Openness 250 years* (Visby, 2017)

Robertson, G. "The media and judicial corruption", in D. Rodriguez & L. Ehrichs (eds.) *Global Corruption Report 2007, Corruption in Judicial Systems – Transparency International*, (Cambridge University Press, 2007)

Rodotà, S. "Data Protection as a Fundamental Right", in S. Gutwith; Y. Poullet; P. De Hert; C. de Terwangne & S. Nouwt (eds.) *Reinventing Data Protection*, (Springen, 2009)

Rosas, A. & L.Armati, "*EU Constitutional Law*" (Oxford, 2010)

Rosenfeld, M. "*Law, Justice, Democracy, and the Clash of Cultures*" (Cambridge University Press, 2011)

Saarenpää, A. "Finland", in Blume (ed.) *Nordic Data Protection*, (Kauppakaari, 2001)

Saarenpää, A. "Legal Infomatics Today – The View from the University of Lapland", in A. Saarenpää & K. Sztobryn (eds.) *Lawyers in the Media Society, The Leal Challenges of the Media Society*, (Lapin yliopisto, 2016)

Schartum D.W. "Norway", in Blume (ed.) *Nordic Data Protection,* (Kauppakaari Oyj, 2001)

Scheinin, M. "*Ihmisoikeudet Suomen oikeudessa*" (Suomalainen Lakimiesyhdistys, 1991)

Van Der Schyff, G. "Cutting to the Core of the Conflicting Rights: The question of inalienable Cores in Comparative Perspective" in Brems (ed.) *Conflicts between Fundamental Rights*, (Intersentia, 2008)

Seipel, P. "Sweden", in Blume (ed.) *Nordic Data Protection,* (Kauppakaari Oyj, 2001)

Sharland, A. "Information rights under European Union Law", in Coppel (ed.) *Information Rights*, (London Sweet & Maxwell, 2007)

Sharland, A. "The Influence of the European Convention on Human Rights", in Coppel (ed.) *Information Rights*, (London Sweet & Maxwell, 2007)

Singleton, S. "*Tolley's Data Protection Handbook*" (LexiNexis, 2004)

Smith, G. "*Democratic Innovations*" (Cambridge, 2009)

Snijders, H.J. "Privacy Contract", in Ziegler (ed.) *Human Rights and Private Law*, (Hart Publishing, 2007)

Tridimas, T. "*General Principles of EU Law*" (Oxford, 2005)

Trudel, P. "Privacy Protection on the Internet: Risk Management and Networked Normativity", in S. Gutwith; Y. Poullet; P. De Hert; C. de Terwangne & S. Nouwt (eds.) *Reinventing Data Protection*, (Springen, 2009)

Tuori, K. "Law, Power and Critique", in Tuori et al. (eds.) *Law and Power, Critical and Socio-Legal Essays*, (Deborah Charles Publications, 1997)

Tuori, K. "*Critical Legal Positivism*" (Hants, 2002)

Tzanou, M. "*The Added Value of Data Protection as a Fundamental Right in the EU Legal Order in the Context of Law Enforcement*" (EUI, 2012)

Uhr, C. "*Antti Chydenius 1729–1803, Adam Smithin Suomalainen edelläkävijä*" (Helsinki, 1965)

Virrankoski, P. "*Anders Chydenius, Demokratisk politiker I upplysningens tid*" (Jyväskylä, 1995)

Voutilainen, T. "*Oikeus tietoon – Informaatio-oikeuden perussteet*" (Edita, 2012)

Wallin A. & P.Nurmi, "*Tietosuojalainsäädäntö*" (Jyväskylä, 1991)

Zucca, L. "*Constitutional Dilemmas, conflicts of fundamental legal rights in Europe and the USA*" (Oxford University Press, 2007)

Zucca, L. "Conflicts of Fundamental Rights as Constitutional Dilemmas" in Brems (ed.) *Conflicts Between Fundamental Rights*, (Intersentia, 2008)

ARTICLES

Adamski, D. "*Approximating a workable compromise on access to official documents: The 2011 developments in the European courts*" in Common Market Law Review 49 (2012), 521–558.

Alamanno, A. "*Unpacking the Principle of Openness in EU Law: Transparency, Participation and Democracy*" in European Law Review 39 (2014), 72–90.

Benediek, A and M.Römer, "*Externalizing Europe: the global effects of European data protection*" in Digital Policy, Regulation and Governance 21 (2019), 32–43.

Birkinshaw, P. "*Review of V.Deckmyn and I. Thompson (eds.), Openness and Transparency in the European Union*" in European Public Law 4 (1998), 614–622.

Brimsted, K. "*The Right to be forgotten: can legislation put the data genie back in the bottle?*" in Privacy and Data Protection 4 (2011) 6–9.

Brkan, M. "*Data Protection and Conflict-of-laws: A Challenging Relationship*" in European Data Protection Law Review, 2 (2016), 324–341.

Brkan, M. "*Data protection and European private international law: observing a bull in a China shop*" in International Data Privacy Law, 5 (2015), 257–276.

Brkan, M. "*The Concept of Essence of Fundamental Rights in the EU Legal Order: Peeling the Onion to its Core*", in European Constitutional Law Review, 2(2018), 332–368.

Brkan, M. "*The Unstoppable Expansion of the EU Fundamental Right to Data Protection: Little Shop of Horrors?"* in Maastricht Journal of European and Comparative Law, 23 (2016), 812–841.

Buitelaar, J.C. "*Child's best interest and informational self-determination: what the GDPR can learn from children's rights*" in International Data Privacy Law 8 (2018), 293–308.

Clifford, D. and J.Ausloos, "*Data Protection and the Role of Fairness*" in Yearbook of European Law 37 (2018), 130–187.

Curtin D.M. "*Citizens' fundamental right of access to EU information: an evolving digital passepartout? "* in Common Market Law Review 37 (2000), 7–41.

Curtin D. and P.Leino, "*In search of transparency for EU law-making: Trilogues on the cusp of dawn*" in Common Market Law Review 6 (2017), 1673–1712.

Custers B, F.Dechesne, A. M. Sears, T. Tani & S. van der Hof, "*A comparison of data protection legislation and policies across the EU*" in Computer Law & Security Review 34 (2018), 234–243.

Dimitrova A. and M.Brkan, "*Balancing National Security and Data Protection: The role of EU and US Policy-Makers and Courts before after the NSA Affair*", in Journal of Common Market Studies (2017) DOI.10.1111/jcms.12634.

Driessen, B. "*The Council of the European Union and access to documents*" in European Law Review 30 (2005), 675–696.

Erdos, D. "*From the Scylla to the Charybdis of License? Exploring the Scope of the 'Special Purposes' Freedom of Expression Shield in European Data Protection*" in Common Market Law Review 52 (2015), 119–154.

Erdos, D. "*European Union Data Protection Law and Media Expression: Fundamentally off Balance*" in International and Comparative Law Quarterly 65 (2016), 139–183.

Feiler, L. "*The Legality of the Data Retention Directive in Light of the fundamental Rights to Privacy and Data Protection*" in European Journal of Law and Technology 3 (2010).

Franck T.M. "*The Emerging Right to Democratic Governance*" in The American Journal of International Law 86 (1992), 46–91.

De Freitas, T. "*Administrative Transparency in Portugal*" in European Public Law 2 (2016), 667–688.

González Fuster, G. "*Fighting For Your Right to What Exactly? The Convoluted Case Law of the EU Court of Justice on Privacy and/or Personal Data Protection*" in *Birbeck Law Review*, 2(2) (2014), 263–278;

González Fuster G. & R. Gellert, "*The fundamental right of data protection in the European Union: in search of an uncharted rights*" in International Review of Law, Computers & Technology 1(2012), 73–81.

Greer, S. "*'Balancing' and the European Court of Human Rights: a Contribution to the Habermas-Alexy debate*" in The Cambridge Law Journal 63 (2004), 412–434.

Harden, I. "*The Revision of Regulation 1049/2001 on Public Access to Documents*" in European Public Law 2 (2009), 239–256.

Hughes, K. "*A Behavioural Understanding of Privacy and its Implications for Privacy Law*" in The Modern Law Review 75(5) (2012), 806–836.

De Hert, P. & V. Papakonstantinou, "*The rich UK contribution to the field of EU data protection: Let's not go for "third country" status after Brexit*" in Computer Law & Security Review 33 (2017), 354–360.

Jans, J.H "*Proportionality Revisited*" in Legal Issues of Economic Integration, 27(2000).

Koillinen, M. "*Oikeudesta anonyymiin julkisen vallan käyttöön*", in Lakimies 1 (2016), 26–53.

Korkea-aho, E. & P.Leino, "*Who owns the information held by EU agencies? Weed killers, commercially sensitive information and transparent and participatory governance*" in Common Market Law Review 4 (2017), 1059–1092.

Koops, B-J. & J.P. Sluijs, "*Network Neutrality and Privacy According to Art. 8 ECHR*" in European Journal for Law and Technology 3 2(2012).

Kranenborg, H. "*Access to documents and data protection in the European Union: on the public nature of personal data*" in Common Market Law Review 45 (2008), 1094–1096.

Leino, P. "*Just a little sunshine in the rain: The 2010 case-law of the European Court of Justice on access to documents*" in Common Market Law Review 48 (2011), 1215–2011.

Li, W. "*A tale of two rights: exploring the potential conflict between two rights to data portability and right to be forgotten under the General Data Protection Regulation*" in International Data Privacy Law 8 (2018), 309–317.

Lloyd, I. "*From ugly duckling to Swan. The rise of data protection and its limits*", in Computer Law and Security Review 34 (2018), 779–783.

Lupia, A. & Matsusaka J.G. "*Direct Democracy: New Approaches to Old Questions*" in The Annual Review of the Political Science 7 (2004), 463–482.

Maes, M. "*Le refronte du reglement (CE) n 1049/2001 relatif a l'access du public aux documents du Parlement europeenne, du Conseil et de la Commissio*" in Revue du Droit de l'Union Europeenne 3 (2008), 577–590.

Malmström, C. "*Sveriges agerande i Öppenhetsmål inför EG-domstolen – politik och juridik hand in hand"* in Europarättslig tidskrift 10 (2008) 11–20.

Möller, K. "*Balancing and the structure of constitutional rights*" in Constitutional Law 5 (2007), 453–468.

Niemivuo, M. "*Good Administration and the Council of Europe*" in European Public Law 4 (2008), 545–563.

Ojanen, T. "*Privacy Is More Than Just a Seven-Letter Word: The Court of Justice of the European Union Sets Constitutional Limits on Mass Surveillance: Court of Justice of the European Union, Decision of 8 April 2014 in Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others, Participation and Democracy*" in European Law and Polity 3 (2014), 528–541.

Pöysti, T. "*Scandinavian Idea of Informational Fairness in Law – Encounters of Scandinavian and European Freedom of Information and Copyright Law*", in Scandinavian Studies in Law 65(2007), 221–248.

Pöysti, T. "*Trust on Digital Administration and Platforms*", in Scandinavian Studies in Law 65(2018), 321–363.

Ragnemalm, H. "*The Community Courts and Openness Within the European Union*" in Cambridge Yearbook of European Legal Studies 2 (1999), 19–30.

Raz, J. "*Legal Principles and the Limits of Law*" in The Yale Law Journal 81 (1972), 823–854.

Raz, J. "*the Authority of Law, Essays on Law and Morality*", (Oxford, 1979), 53–77.

Reed, C. "*Taking Sides on Technology Neutrality*" in SCRIPT-ed 4 3(2007).

Rossi, A. "*How the Snowden Revelations Saved the EU General Data Protection Regulation"* in The International Spectator Italian Journal of International Affairs 53(2018), 95–111.

Ritleng, D. "*Does the European Court of Justice take democracy seriously? Some thoughts about the Macro-Financial Assistance case"* in Common Market Law Review 53 (2016), 11–34.

van der Sloot, B. "*Decisional privacy 2.0: the procedural requirements implicit in Article 8 ECHR and its potential impact on profiling*" in International Data Privacy Law 7 (2017), 190–201.

Tiilikka, P. "*Access to Information as a Human Right in the Case Law of the European Court of Human Rights*" in The Journal of Media Law 5(1) (2013), 79–103.

Tolonen, H. "*Rules, Principles and Goals: the interplay between law, morals and politics*", in Scandinavian studies in law 35(1991), 269–293.

Vedaschi, A. "*Privacy and data protection versus national security in transnational flights: the EU-Canada PNR agreement*" in International Data Privacy Law 8 (2018), 124–139.

de Vries, S.A "*Balancing Fundamental Rights with Economic Freedoms According to the European Court of Justice*" in Utrecht Law Review 9(1) (2013), 169–192.

Wachter S. & B.Mittelstadt "*A Right to reasonable interference: Re-thinking data protection law in the age of big data and AI*" in Columbia Business Law Review 2 (2019).

Weiss, F. & S. Steiner, "*Transparency as an element of Good Governance in the Practice of the EU and the WTO: Overview and Comparison*" in Fordham International Law Journal 30 (2006), 1545–1586.

Whitman, J.Q. "*The Two Western Cultures of Privacy: Dignity versus Liberty*" in Yale Law Journal 113(2004), 1151–1221.

CASE NOTES

Bobek, M. "*Case C-345/06, Gottfried Heinrich, Judgement of the Court of Justice (Grand Chamber) of 10 March 2009*" in Common Market Law Review 46 (2009) 2077–2094.

Bobek, M. "*Joined Cases C-92 & 93/09, Volker und Markus Schecke GbR and Hartmut Eifert*" in Common Market Law Review 6 (2011), 2005–2022.

Cameron, I. "*Balancing data protection and law enforcement needs: Tele2 Sverige and Watson*", in Common Market Law Review 54 (2017), 1457–1496.

Granger, M.-P. & K.Irion, "*The Court of Justice and the Data Retention Directive in Digital Rights Ireland: Telling Off the EU Legislator and Teaching a Lesson in Privacy an Data Protection*" in European Law Review 39 (2014), 835–850.

Hins, W. "*Case C-73/07, Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy, Judgment of the Grand Chamber of 16 December 2008*" in Common Market Law Review 47 (2010), 215–233.

Kadelbach, S. "*Case Law A. Court of Justice*", in Common Market Law Review 38 (2001), 179–2001.

Leino, P. "*Case annotation of Case C-353/99 Council v Heidi Hautala*" in Common Market Law Review 39 (2002), 621–632.

Lynskey, O. "*Data protection and freedom of information; reconciling the irreconcilable?*" in Cambridge Law Journal 70 (2011), 37–39.

Ojanen, T. "*Making the essence of fundamental rights real: the Court of Justice of the European Union clarifies the structure of fundamental rights under the Charter*" in European Constitutional Law Review 2 (2016), 318–329.

Tambou, O. "*Opinion 1/15 on the EU-Canada Passenger Name Record (PNR) Agreement: PNR Agreement Need to Be Compatible with EU Fundamental Rights*", in European Foreign Affairs Review 23 (2018), 187–202.

CASE-LAW

COURT OF JUSTICE

Case C-331/88, *R v Minister Agriculture, Fisheries and Food, ex parte Fedesa etc.,* ECLI:EU:C:1990:391

Case C-353/99 P, *Council of the European Union v Heidi Hautala*, ECLI:EU:C:2001:661

Case C-112/00, *Schmidtberger*, ECLI:EU:C:2003:333

Joined cases C-465/00, C-138/01 and C-139/01 *Österreichischer Rundfunk and Others*, ECLI:EU:C:2003:294

Case C-101, *Lindqvist*, ECLI:EU:C:2003:596

Case C-211/01, *Commission v Council*, ECLI:EU:C:2003:452

Case C-36/02, *Omega*, ECLI:EU:C:2004:614.

Case T-2/03, *Verein für Konsumenteninformation v Commission*, ECLI:EU:T:2005:125

Case C-178/03, *Commission v Parliament and Council*, ECLI:EU:C:2006:4

Case T36/04, *API v Commission*, ECLI:EU:T:2007:258

Joined cases C-39/05 P and C-52/05 P *Sweden and Turco/ Council*, ECLI:EU:C:2008:374

Case T-42/05, *Williams v Commission*, ECLI:EU:T:2008:325

Case C-64/05 P, *Sweden* v *Commission and Others*, ECLI:EU:C:2007:802

Case T-166/05, *Borax Europe Ltd. v Commission*, ECLI:EU:T:2009:65

Case C-266/05 P, *Sison v Council*, ECLI:EU:C:2007:75

Case C-341/05, *Laval un Partneri*, ECLI:EU:C:2007:809

Joined cases C402/05 P and C415/05 P, *Kadi and Al Barakaat International Foundation* v *Council and Commission*, ECLI:EU:C:2008:461

Case C-438/05, *The International Transport Workers' Federation ja The Finnish Seamen's Union*, ECLI:EU:C:2007:772

Case C-158/06, *ROM-projecten*, ECLI:EU:C:2007:370

Case C-275/06, *Promusicae*, ECLI:EU:C:2008:54

Case C-345/06, *Heinrich*, ECLI:EU:C:2009:140

Case C-73/07, *Satakunnan Markkinapörrsi and Satamedia*, ECLI:EU:C:2008:727

Case C-139/07 P, *Technische Glaswerke Ilmenau GmbH*, ECLI:EU:C:2010:376

Joined cases C-514/07 P, C-528/07 P and C-532/07 P *Sweden and Others v API and Commission*, ECLI:EU:C:2010:541

Case C-553/07, *College van burgemeester en vethounders van Rotterdam v E.E: Rijekeboer*; ECLI:EU:C:2009:293.

Case C-28/08P*, Bavarian Lager*, ECLI:EU:C:2010:378

Case C-506/08 P, *Sweden v MyTravel and Commission*, ECLI:EU:C:2011:496

Joined cases C-92/09 and C-93/09 *Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen*, ECLI:EU:C:2010:662

Case C343/09, *Afton Chemical,* ECLI:EU:C:2010:419

Joined cases C539/10 P and C550/10 P, *Al-Aqsa* v *Council*, ECLI:EU:C:2012:711

Joined cases C581/10 and C629/10 *Nelson and Others*, ECLI:EU:C:2012:657

Case C-135/11 P *IFAW International Tierschutz-Fonds gGmbH /European Commission,* ECLI:EU:C:2012:376

Case C283/11, *Sky Österreich*, ECLI:EU:C:2013:28

Case C101/12, *Schaible*, ECLI:EU:C:2013:661

Case C-131/12, *Google Spain and Google Inc*, ECLI:EU:C:2014:317

Joined cases C-141/12 and C-372/12 *YS e.a.*, ECLI:EU:C:2014:2081

Case C-350/12 P, *Council v Sophie In 't Veld*, ECLI:EU:2014:2039

Joined cases C-446/12 to C-449/12 *Willems and Others*, ECLI:EU:C:2015:238

Joined cases C-293/12 and C-594/12 *Digital Rights Ireland and Kärtner Landesregierung*, ECLI:EU:C:2014:238

Case C-212/13, *Ryneš*, ECLI:EU:C:2014:24

Case C-127/13 P, *Strack v Commission*, ECLI:EU:C:2014:2250

Case C-615/13 P, *ClientEarth and PAN Europe v EFSA*, ECLI:EU:C:2016:489

Case C-650/13, *Delvige*, ECLI:EU:C:2015:648

Case C-201/14, *Samaranda Bara and others*, ECLI:EU:C:2015:638

Case C-230/14, *Weltimmo*, ECLI:EU:C:2015:639

Case C-362/14, *Schrems,* ECLI:EU:C:2015:650

Joined cases C-439/14 and C-448/14, *SC Star Storage SA etc*, ECLI:EU:C:2016:688

Case T-493/14, *Mayer v EFSA*, ECLI:EU:T:2017:100

Case C-562/14 P, *Sweden and Spirlea v European Commission*, ECLI:EU:2017:356

Case C582/14, *Patrick Breyer v Bundesrepublik Deutschland*, ECLI:EU:C:2016:779

Case C-419/14, *WebMindLicenses,* ECLI:EU:C:2015:832

Case C-191/15, *Verein fur Konsumentioninformation v Amazon*, EU:ECLI:C:2016:612

Case C-203/15, *Tele2 Sverige*, ECLI:EU:C:2016:970

Case C-271/15 P, *Sea Handling SpA, in liquidation, formerly Sea Handling SpA v Commission*, ECLI:EU:C:2016:557

Case C-331/15 P, *French Republic v Carl Schlyter*, ECLI:EU:C:2017:639

Case C-398/15, *Manni*, ECLI:EU:C:2017:197

Case C-491/15 P, *Typke v European Commission*, ECLI:EU:C:2017:5

Case C-536/15, *Tele2 (Netherlands) and others*, ECLI:EU:C:2017:214

Case T-540/15, *De Capitani v Parliament*, ECLI:EU:T:2018:167

Case C-13/16, *Rigas satiksme*, ECLI:EU:C:2017:336

Case C-210/16, *Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH,* ECLI:EU:C:2018:388

Case C-434/16, *Nowak*, ECLI:EU:C:2017:994

Case C-207/16, *Ministerio Fiscal*, ECLI:EU:C:2018:788

Opinion of the Court (Grand Chamber) of 26 July 2017 pursuant to Article 218(11) TFEU, ECLI:EU:C:2016:656

Case C-25/17, *Tietosuojavaltuutettu*, ECLI:EU:C:2018:551

Case T-345/17, *Buivids,* ECLI:EU:C:2019:122

GENERAL COURT

Case T-194/94, *Carvel and Guardian Newspapers v Council*, ECLI:EU:T:1996:156

Case T-174/95, *Svenska Journalistförbundet v Counci*l, ECLI:EU:T:1998:127

Case T-20/99, *Denkavit Nederland* v *Commission*, ECLI:EU:T:2000:209

Case C-41/00 P, *Interpoc v Commission*, ECLI:EU:C:2003:125

Joined cases T-110/03, T-150/03 and T-405/03, *Sison v Council*, ECLI:EU:T:2005:143

Joined cases T-391/03 and T-70/04, *Franchet and Byk*, ECLI:EU:T:190

Case T-161/04, *Valero Jordana v Commission*, ECLI:EU:T:2011:337

Case T-264/04, *WWF European Policy Programme v Council*, ECLI:EU:T:2007:114

Case T-194/04, *Bavarian Lager v Commission*, ECLI:EU:T:2007:334

Case T-166/05, *Borax Europe Ltd. v Commission*, ECLI:EU:T:2009:65

Case T-121/05, *Borax Europe v Commission,* ECLI:EU:T:2009:64

Case T-412/05, *M v European Ombudsman*, ECLI:EU:T:2008:397

Case C-139/07 P, *Commission v Technische Glaswerke Ilmenau*, ECLI:EU:C:2010:376

Case T-3/08, *Coedo Suarez v Council* (OJ C 64, 8.3.2008, p. 54-55)

Case T-383/08, *New Europe v Commission*, ECLI:EU:T:2009:114

Case T -82/09*, Dennekamp v Parliament*, ECLI:EU:T:2011:688

Case T-233/09*, Access Info Europe / Council of the European Union*, ECLI:EU:T:2011:105

Case T-436/09, *Julien Dufour v European Central Bank*, ECLI:EU:T:2011:634

Case T-115/13, *Dennekamp v Parliament*, ECLI:EU:T:2015:497

Case T-343/13, *CN v Parliament*, ECLI:EU:T:2015:926

Case T-395/13*, Samuli Miettinen*, ECLI:EU:T:2015:648

Joined cases T-424/14 and T-435/15 *ClientEarth v Commission*, ECLI:EU:T:2015:848

Case C-73/16, *Puskar v Financne riaditel'stvo Slovenskej republiky etc*, EU:ECLI: C:2017:725

Case T-94/16, *Psara v European Parliament,* ECLI:EU:T:2018:602

AG'S OPINIONS

Opinion of AG Maduro in joined cases C-39/05 P and C-52/05 P, *Sweden and Turco/ Council*, ECLI:EU:C:2007:721, delivered 29 November 2007

Opinion of AG Sharpston in Case C-28/08, *Bavarian Lager*, ECLI:EU:C:2009:624, delivered 15 October 2009

Opinion of AG Bobek in Case Case C-213/15 P, *Commission v Breyer*, ECLI:EU:C:2016:994, delivered 21 December 2016

EUROPEAN COURT OF HUMAN RIGHTS

ECtHR 2 August 1984, *Malone v the United Kingdom* (ECLI:CE:ECHR:1984:0802J UD000869179)

ECtHR 7 July 1989, *Gaskin v the United Kingdom*

ECtHR 19 February 1998, *Guerra and Others v Italy*, (1998-I)

ECtHR 25 November 1999, *Nilsen and Johnsen v Norway* (1999-VIII)

ECtHR 8 July 1999, *Sürekand Ödzemir v Turkey* (Grand Chamber)

ECtHR 16 February 2000, *Amann v Switzerland* (2000-II)

ECtHR 4 May 2000, *Rotaru v Romania,* (RJD 2000-V)

ECtHR 24 June 2004, *Von Hannover v Germany* (2004-VI)

ECtHR 19 October 2005, *Roche v United Kingdom,* (2005-X)

ECtHR 10 November 2005, *Leyla Sahin v Turkey* (ECLI:CE:ECHR:2005:1110JUD004477498)

ECtHR 14 February 2006, *Turek v Slovakia*, (2006-II)

ECtHR 14 April 2009, *Társaság a Szabadságjogokért v Hungary*, Application No 3734/05

ECtHR 26 May 2009, Kenedi v Hungary, Application no31475/05

ECtHR 12 January 2010, *Gillan and Quinton v the United Kingdom* (ECLI:CE:ECHR: 2010:0112JUD000415805)

ECtHR 14 September 2010, *Sanoma Uitgevers B.V. v the Netherlands* (ECLI:CE:ECHR:2 010:0914JUD003822403)

ECtHR 2 November 2010, *Gillberg v Sweden*

ECtHR 31 March 2016, *Stoyanov etc. v Bulgaria* (ECLI:CE:ECHR:2016:0331JUD005538810)

ECtHR 77 June 2017, *Satakunnan Markkinapörssi Oy and Satamedia Oy v Finland* (ECL I:CE:ECHR:2017:0627JUD000093113)

CONSTITUTIONAL COURTS

PeVL18/2014 vp

Judgement by German Constitutional Court, BVerfGE 65, 1 (15 December 1983).

FINNISH DATA PROTECTION BOARD - TIETOSUOJALAUTAKUNTA

Decision of the Finnish Data Protection Board (tietosuojalautakunta) 4/2007, dnro 6/932/2006.

Decision of the Finnish Data Protection Board (tietosuojalautakunta) 2/2009, dnro 1/933/2008.

Decision of Data Protection Board 1/2010, dnro 2/932/2009.

Decision of the Finnish Data Protection Board (tietosuojalautakunta) 4/2010, dnro 1/933/2010 and 4/932/2010.

ADMINISTRATIVE COURT OF HELSINKI

KHO 2011: Decision of Administrative Court of Helsinki 30.12.2011, dnro 01026/11/1204.

KHO 2014:83

KHO 2009: 82

LEGISLATIVE MATERIAL

EUROPEAN UNION

Code of Conduct Concerning Public Access to Documents to Council and Commission Documents (OJ L 340, 31.12.1993, p. 41–42)

Council Decision of 20 December 1993 on public access to Council documents (OJ L 340, 31.12.1993, p.43–44)

Commission Decision of February 1994 on public access to Commission documents (OJ L 46, 18.2.1994, p. 58–59)

Directive 95/46/EC of the European Parliament and 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 (OJ L 281, 23.11.1995, p. 31–50)

Decision of the Secretary-General of the Council/High Representative for Common Foreign and Security Policy of 25 June 2001 on a code of good administrative behaviour for the General Secretariat of the Council of the European Union and its staff in their professional relations with the public (OJ 5.7.2001 C189/1)

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37–47)

Council Regulation (EC) No 1290/2005 of 21 June 2005 on financing common agricultural policy (OJ L 209, 11.8.2005, p. 1–25)

Charter of Fundamental Rights of the European Union (OJ C 303, 14.12.2007, p. 1–16)

Regulation (EC) No 1367/2006 of the European Parliament and of the Council on the application of the provisions of the Aarhus Convention to Information, Public Participation in Decision-making and Access to Justice in Environmental Matters to Community institutions and bodies (OJ L 264, 25.9.2006, p. 13–19)

Council Regulation (EC) 1437/2007 of 26 November 2007 amending Regulation (EC) No 1290/2005 on the financing of the common agricultural policy (OJ L 322, 7.12.2007, p. 1–5)

The decision (25 March 2009) by the European Chemical Agency on the implementation of Regulation (EC) 1049/2001 of the European Parliament and of the Council regarding public access to documents to European Parliament, Council and Commission documents

Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1–88)

Directive (EU) 2016/680 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 by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free

movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, p. 89–131)

Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union in institutions, bodies, offices and agencies and on the free movement of such data, repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39–98)

NATIONAL LEGISLATIONS

Data Protection Act 1998 (UK)

Laki potilaan asemasta ja oikeuksista 1992/785 (Finland)

Laki viranomaisen toiminnan julkisuudesta 21.5.1999/621 (Finland)

Henkilötietolaki 22.4.1999/523 (Finland)

Tryckfrihetsförordning (1949:105) (Sweden)

Personuppgiftslagen (1998:204) (Sweden)

Brotssbalk (1962:700) (Sweden)

Slovenian Access to Public Information Act, published on 22 March 2003 (Official Gazette of RS. No 24/2003), available on internet < www.ip-rs.si> [last visited 6.8.2017]

OTHER

CoE, Committee of Ministers (1973), Resolution (73) 22 on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector, 26 September 1973

CoE, Committee of Ministers (1974), Resolution (74) 29 on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector, 20 September 1974

OFFICIAL DOCUMENTS

Parliamentary Assembly of Council of Europe, Resolution 1165 (1998); Right to Privacy

Government bill for the Public Access to Document Law HE 30/1998 vp (Finland, laki viranomaisen toiminnan julkisuudesta 21.5.1999/621)

Decision of the European Ombudsman on complaint 713/98/(IJH)/GG against the European Commission

Commission of the European Union, Amended proposal for the Council Directive on the protection of individuals with regard to the processing of personal data and the free movement of such data, COM(92) 422 final – SYN 287, Brussels 15 October 1992

Commission's white paper, Code of Good Administrative Behaviour, Relations with the public, adopted on 1 March 2000 (OJ 20.10.2000 L267)

Commission's white paper, Code of Good Administrative Behaviour, Relations with the public, adopted on 1 March 2000 (OJ 20.10.2000 L267)

The Recommendation 2002(2) of the Committee of Ministers to member states on access to official documents

A letter from the European Ombudsman to the President of the European Commission, 30.9.2002/7411

Decision of the European Central Bank of 4 March 2004 on public access to European Central Bank documents (ECB 2004/3)(2004/258/EC) (OJ 2004 L 80, p. 42)

The European Ombudsman, The European Code of Good Administrative Behaviour, 2005

Communication from the Commission, Follow-up to the Green Paper 'European Transparency Initiative', COM 2007 (127) final

Document 12973/07, Brussels, 19 October 2007, available on the internet < http://data.consilium.europa.eu/doc/document/ST-12973-2007-INIT/en/pdf> [last visited 18.3.2017]

Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data

European Transparency Initiative (ETI), Communication from the Commission of 21 March 2007, Follow-up to the Green Paper 'European Transparency Initiative'[COM 2007 (127) final]

Commission Proposal for a Regulation of the European Parliament and of the Council regarding public access to European Parliament, Council and Commission documents COM(2008) 229 final (30.4.2008)

Pleading of the EDPS in Public Hearing in Case C-28/08P (16 June 2009), available on the internet < http://www.edps.europa.eu/EDPSWEB/ webdav/site/mySite/shared/Documents/Consultation/Court/2009/09-06-16_pleading_C-28-08P_EN.pdf> [last visited 29.9.2011]

Article 29 Data Protection Working Party, Opinion 2/2010 on online behavioural advertising

Communication from the Commission to the European Parliament, The Council, the Economic and

Social Committee and the Committee of Regions, A comprehensive approach on personal data protection in the European Union, COM 2010 (609) final

Document 14549/11, Brussels, 23 September 2011

Commission Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) COM(2012) 11 final (25.1.2012)

Article 29 Data Protection Working Party, Opinion 3/2013 on purpose limitations

Article 29 Data Protection working party, Opinion 6/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 844/14/EN WP 217

European Parliament legislative resolution of 12 March 2014 on the Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)

Council of European Union, 9565/15, Brussels, 11 June 2015

Article 29 Data Protection working party, Opinion 2/2016 on the publication of Personal Data for Transparency purposes in the Public Sector, 1806/16/EN WP 239

The Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision by Article 29 Data Protection Working Party (13.4.2016)

Document 10949/05, Brussels, 23 May 2016, available on the internet < http://data.consilium.europa.eu/doc/document/ST-10949-2005-DCL-1/en/pdf >[last visited 20.2.2017]

Document 8807/16, Brussels, 19 May 2016, available on the internet < http://data.consilium.europa.eu/doc/document/ST-8807-2016-ADD-1/en/pdf > [last visited 20.2.2017]

Document 5961/17, Brussels, 14 February 2017

Document 6224/17, Brussels, 15 February 2017

Commission Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC COM(2017) 8 final (10.1.2017)

Commission Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM(2017) 10 final (10.1.2017)

European Data Protection Supervisor, *Public access to documents containing personal data after the Bavarian Lager ruling*

Convention 108 and Protocol, available on the internet < www.coe.int/en/web/data-protection/convention108-and-protocol > [last visited 15.8.2018]

Security Council Resolutions:

Security Council Resolutions 1511(2003), p.1 (no 2), 1546(2004), para. 3 and 1637(2005), p. 1 (no 4)

Security Council Resolution 1546(2004), p. 1 (no 3) and Resolution 1619 and 1637(2005)

Security Council Resolution 1546(2004), p. 1 (no 10)

Security Council Resolution 1483(2003), para. 22.

REPORTS AND GUIDELINES

OECD original guidelines, OECD Council Recommendation concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (23 September 1980), available on the internet < http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm> [last visited 23.10.2016]

Report "*The Secret State of EU Transparency Reforms*" published March 2010, by Access Info Europe, www.access-info.org

Revised Recommendation adopted by the OECD Council adopted on 11 June 2013, "Privacy Guidelines", available on the internet < ttp://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf> [last visited 23.10.2016]

Report on public access to documents (Rule 116(7) for the years 2014-2015, European Parliament, available on the internet <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A8-2016-0141+0+DOC+PDF+V0//EN> [last visited 23.10.2016]

Report from the Commission on the application in 2015 of Regulation (EC) No 1049/2001 regarding public access to European Parliament, Council and Commission documents COM/2016/ 533 final, Brussels, 24.8.2016, available on the internet < http://eur-lex.europa.eu/resource.html?uri=cellar:3a0be84b-69fd-11e6-9b08-01aa75ed71a1.0003.02/DOC_2&format=PDF > [last visited 5.3.2017]

Report on Public Access to Council documents 2015, available on the internet < http://www.consilium.europa.eu/en/press/press-releases/2016/06/24-council-access-documents/> [last visited 23.10.2016]

Report from the Commission on the application in 2016 of Regulation (EC) No 1049/2001 regarding public access to European Parliament, Council and Commission documents COM/2017/738 final, Brussels 6.12.2017, available on the internet < http://eur-lex.europa.eu/resource.html?uri=cellar:05a0236b-dbf9-11e7-a506-01a> [last visited 29.12.2018]

Report from the Commission on the application in 2017 of Regulation (EC) No 1049/2001 regarding public access to European Parliament, Council and Commission documents COM/2018/663 final, Brussels 3.10.2018, available on the internet < http://ec.europa.eu/ info/sites/info/files/com_2018_663_f1_report_from_commission_en_v3_p1_988979.pdf > [last visited 29.12.2018]

Fifteenth annual report of the Council on the implementation of Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May regarding public access to European Parliament, Council and Commission documents, 7903/17, Brussels 12 May 2017

Sixteenth annual report of the Council on the implementation of Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May regarding public access to European Parliament, Council and Commission documents, 8689/18, Brussels 14 May 2018

Article 29 Data Protection working party, "Guidelines on transparency under Regulation 2016/679" , 17/EN WP 260, 11.4.2018

Henkilötiedot ja paikkatiedot: Miten tietosuojalainsäädäntö vaikuttaa paikkatietojen julkaisemiseen ja luovuttamiseen, Ympäristöministeriö, 21.2.2018

Explanatory Report – CETS 205 – Access to Official Documents, Available on the internet < http://www.coe.int/t/dghl/monitoring/greco/default_en.asp > [last visited 21.2.2017]

EUI working paper, *Report on system effectiveness, efficiency and satisfaction assessment; Data Protection* by Erik Krempel, Fraunhofer IOSB and Dr Coen van Guljik, TU Delft, available on the internet < https://surveille.eui.eu/wp-content/uploads/sites/19/2015/04/D3.3bSystem-Effectiveness-and-Efficiency-Data-Protection.pdf > [last visited 15.5.2017]

MCEL Working Paper series, *Freedom of expression and Artificial Intelligence: on personalisation, disinformation and (lack of) horizontal effect of the Charter* by Maja Brkan (March 17, 2019). Available on the internet < https://ssrn.com/abstract=3354180 or http://dx.doi.org/10.2139/ssrn.3354180 > [last visited 1.5.2019]

PRESS RELEASES

Press release, Danish Ministry of Justice 2.6.2014, *Justitsministeren ophæver reglerne om sessionslogning*, available on the internet < http://justitsministeriet.dk/nyt-og-presse/pressemeddelelser/2014/justitsministeren-oph%C3%A6ver-reglerne-om-sessionslogning> [last visited 3.11.2015]

Press release, Vivane Reding, Vice-President of the European Commission, EU Commissioner for Justice, *Today's Justice Council – A council of Progress*, Luxembourg, 6 June 2014

Press release, the European Commission 29.2.2016, *Restoring trust in transatlantic data flows through strong safeguards: European Commission presents EU-U.S. Privacy Shield* available on the internet < http://europa.eu/rapid/press-release_IP-16-433_en.htm > [last visited 30.8.2016]

Press release (23.5.2018) by Council of the European Union *New rules on data protection for EU institutions agreed* available <http://www.consilium.europa.eu/en/press/press-releases/2018/05/23/new-rules-on-data-protection-for-eu-institutions-agreed/> [last visited 21.7.2018]

ELECTRONIC SOURCES

Tasks of the European Data Protection Supervisor, available on the internet < http://www.edps.europa.eu/EDPSWEB/edps/EDPS?more=moins > [last visited 21.2.2012]

Good Governance Guide, available on the internet < http://www.bioa.org.uk/docs/BIOAGovernanceGuideOct09.pdf > [last visited 21.2.2012]

Commission factsheet on The EU Data Protection Reform and Big Data, March 2016, available on the internet < http://ec.europa.eu/justice/data-protection/files/data-protection-big-data_factsheet_web_en.pdf> [last visited 9.10.2016]

Convention 108 and Protocol, available on the internet < www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=Xn1qwlWa > [last visited 15.8.2018]

Transparency Register, see Transparency and EU, available on the internet < http://ec.europa.eu/transparencyregister/public/homePage.do?locale=en#en> [last visited 23.10.2016]

European Commission, "Digital Single Market, Bringing down barriers to unlock online opportunities", available on the internet < http://ec.europa.eu/priorities/digital-single-market/> [last visited 16.10.2016]

Transparency International, available on the internet <https://www.transparency.org/what-is-corruption/#what-is-transparency> [last visited 21.2.2017]

United Nations Economic and Social Commission for Asia and the Pacific – What is Good Governance , available on the internet <http://www.unescap.org/sites/default/files/good-governance.pdf > [last visited 21.2.2017]

Details of Treaty No.205, Council of Europe Convention on Access to Official Documents, available on the internet < https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/205 > [last visited 21.2.2017]

EU Charter of Fundamental Rights, Why the Charter of Fundamental Rights exists, available on the internet < http://ec.europa.eu/justice/fundamental-rights/charter/index_en.htm> [last visited 20.3.2017]

European Digital Rights, *Key aspects of the proposed General Data Protection Regulation explained: What are they? Why are they important? What are common misconceptions? What can be improved?*, available on the internet < https://edri.org/files/GDPR-key-issues-explained.pdf> [last visited 8.4.2017]

Eric Posner, "Debate about the Right to be Forgotten, 13 March 2015, available on the internet < http://ericposner.com/debate-about-the-right-to-be-forgotten/ > [last visited 9.4.2017]

Anders Chydenius Foundation, What did Chydenius say about freedom of the press, available on the internet <www.chydenius.net/historia/mita_sanoi/e_ilmaisunvapaudesta.asp > [last visited 14.8.2017]

The Risk-Based Approach in the GDPR: Interpretation and Implications by Gabriel Maldoff, available on the internet < https://iapp.org/media/pdf/resource_center/GDPR_Study_Maldoff.pdfxx > [last visited 4.8.018]

SEMINARS AND CONFERENCES

Data Protection Conference organised by European Commission in *Brussels 19-20 May 2009*

National Information Law Conference, Canberra, 23-25 March 2011

Seminar lecture by Sabino Cassese, May 2011, London. Sabino Cassese is a former judge in a constitutional court in Italy and professor of Public Law at the University of Rome

Commentary of the Charter of Fundamental Rights of the European Union, June 2006

SPEECHES

Viviane Reding, Vice-President of the European Commission, EU Justice Commissioner, SPEECH/12/26, *The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age*, available on the internet < http://europa.eu/rapid/press-release_SPEECH-12-26_fi.htm > [last visited 3.7.2017]

Oikeuskansleri Tuomas Pöysti, *Korruptiontorjunnan voitettavat vaikeudet Suomessa*, 11.12.2018, Available on the internet < https://www.okv.fi/fi/tiedotteet-ja-puheenvuorot/494/korruptiontorjunnan-voitettavat-vaikeudet-suomessa/ > [last visisted 22.2.2019]

BLOGS

Privacy & Information Security Law Blog, *Authorities in Austria and Switzerland Rule on Google Street View*, 3 May 2011, available on the internet < https://www.huntonprivacyblog.com/2011/05/03/authorities-in-austria-and-switzerland-rule-on-google-street-view/> [last visited 8.4.2017]

European Law Blog, News and comments on EU law, *European Data Protection and Freedom of Expression After Buivids: An Increasingly Significant Tension*, 21 February 2019, available on the internet < https://europeanlawblog.eu/2019/02/21/

european-data-protection-and-freedom-of-expression-after-buivids-an-increasingly-significant-tension/ > [last visited 23.2.2019]

NEWSPAPER ARTICLES

Helsingin Sanomat, 29.8.2016, A 22

The Guardian, "We need to talk about the right to be forgotten", by David Drummond, available on the internet < https://www.theguardian.com/commentisfree/2014/jul/10/right-to-be-forgotten-european-ruling-google-debate > [last visited 9.4.2017]

Financial Times, *Brussels welcomes Google 'right to be forgotten' measure*, May 30 2014, available on the internet < https://www.ft.com/content/bc116b3e-e810-11e3-9cb3-00144feabdc0?mhq5j=e1> [last visited 3.7.2017]

INTRODUCTION

I believe that by May 2018 there were not too many who could claim they had never heard the letter combination GDPR – the General Data Protection Regulation. When I started with this project several years ago, I was told that data protection was not a good topic for a PhD, because it is such a niche sector of law. I did not agree. It was clear even back then that not too many fields of law cover as comprehensively nearly every sector of life and society. I also had a very strong personal interest in the topic and felt quite privileged when I later entered into the GDPR negotiations.

Data protection has become a very hot topic with the vast reform process that has taken place in the EU. This development was bolstered by a series of data protection scandals including Uber, Cambridge Analytica, Snowden, the Schrems case, and Wikileaks' leaks to name just a few. When triggered by individual persons, like Snowden, Assange or Schrems, certain individual data protection rights have been at the core of the discussion. In the case of Snowden and Assange, the issues addressed equally included freedom of information, or more precisely disclosure of information; information, which also contained personal data.[1]

This thesis will take a specific interest in the relationship between the protection of personal data and a transparent society, with a particular emphasis on the democratic decision-making process. Despite the current data protection reforms, the tension between data protection and public access to documents has not entirely vanished from the European legal scene. The General Data Protection Regulation clearly leaves the space for the Member States to reconcile public access to documents with the protection of personal data, but the General Data Protection Regulation itself does not – nor should it – provide a direct answer to the question of how to reconcile these fundamental rights. At the same time, the reform process for the Data Protection Regulation for the EU institutions themselves, now referred to as the EU Institutions' Data Protection Regulation[2], provided an excellent opportunity to seek a balance between the said fundamental rights at the Union level. Quite delightfully, this opportunity was not wasted.

The amendments adopted in the EU Institutions' Data Protection Regulation were needed. Statistics on public access to EU institutions' documents dating from

1 Some of these breaking news events had a strong influence on European Data Protection Reform. See for example Press release, Vivane Reding, Vice-President of the European Commission, EU Commissioner for Justice, *Today's Justice Council – A council of Progress*, Luxembourg, 6 June 2014.

2 The Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39–98).

the time before the adoption of the said Regulation reveal a concerning tendency. While the general trend shows that public access to documents has steadily increased, the offline trend of the protection of personal data becoming the most applied exception is concerning. The reports of the Commission and the Council on public access to documents reveal clearly this development.[3] This was also the very reason for the decrease in the percentage of the documents released by the Commission in the year 2015.[4] While in 2011 only 8,9% of the refusals were based on a personal data exemption, in 2015 the corresponding figure was 29%.[5] The Council's report on access to documents reveals a similar trend. According to Council statistics, in 2015 the refusal to give full access to documents was justified with the protection of personal data in 29% of cases.[6] This was the most widely applied single exemption for denial of disclosure.

These figures capture in a clear and simple manner why it is essential to work further to find a stable balance between the two fundamental rights.

---

3 Unfortunately, the European Parliament does not provide clear figures on the exemptions which have been applied in its report. For the report of the European Parliament, see Report on public access to documents (Rule 116(7)) for the years 2014–2015 (2015/2287(INI)), available on the internet <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A8-2016-0141+0+DOC+PDF+V0//EN> T. Ojanen, "Privacy Is More Than Just a Seven-Letter Word: The Court of Justice of the European Union Sets Constitutional Limits on Mass Surveillance: Court of Justice of the European Union, Decision of 8 April 2014 in Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others, Participation and Democracy" in *European Law and Polity* 3 (2014), 528–541, For an analysis, see M.-P.Granger & K.Irion, "The Court of Justice and the Data Retention Directive in Digital Rights Ireland: Telling Off the EU Legislator and Teaching a Lesson in Privacy an Data Protection" in *European Law Review* 39 (2014), 835–850. See also the Report from the Commission on the application in 2015 of Regulation (EC) No 1049/2991 regarding public access to European Parliament, Council and Commission documents COM/2016/0533 final, available on the internet < http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2016:533:FIN> [last visited 23.10.2016].

4 See the Report from the Commission on the application in 2015 of Regulation (EC) No 1049/2001 regarding public access to European Parliament, Council and Commission documents COM/2016/0533 final, available on the internet < http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2016:533:FIN> [last visited 23.10.2016]. Similarly, Report from the Commission on the application in 2016 of Regulation (EC) No 1049/2001 regarding public access to European Parliament, Council and Commission documents COM/2017/738 final, available on the internet <

http://eur-lex.europa.eu/resource.html?uri=cellar:05a0236b-dbf9-11e7-a506-01a> [last visited 29.12.2018] and Report from the Commission on the application in 2017 of Regulation (EC) No 1049/2001 regarding public access to European Parliament, Council and Commission documents COM/2018/663 final, available on the internet <

http://ec.europa.eu/info/sites/info/files/com_2018_663_f1_report_from_commission_en_v3_p1_988979.pdf > [last visited 29.12.2018]. By 2018 the percentage had increased to 31,3%.

5 Ibid.

6 Public Access to Council documents: 2015 report, available on the internet < http://www.consilium.europa.eu/en/press/press-releases/2016/06/24-council-access-documents/> [last visited 23.10.2016]. See also Fifteenth annual report of the Council on the implementation of Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May regarding public access to European Parliament, Council and Commission documents, 7903/17, Brussels 12 May 2017. In 2016 there was a decrease in the percentage, 21,2% of the partial refusals were reasoned with the said exemption at the initial stage, however, on the confirmatory stage the refusal was increased to 45,5%. In 2017 the corresponding figures were 16,8% and 3,9% and the most widely applied exception was the protection of institution's decision-making process, see Sixteenth annual report of the Council on the implementation of Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May regarding public access to European Parliament, Council and Commission documents, 8689/18, Brussels 14 May 2018.

1. SUBJECT MATTER AND AIM

This research will examine the interplay between two fundamental rights in the European legal framework and the aim is to reconcile the protection of personal data with the right of public access to documents.

In essence, there is a tension between the requirements arising from the transparency and data protection regimes. The precise legal nature of these two rules, rights or principles is also unclear. Protection of personal data has only very recently been recognized as an independent fundamental right, instead of a sub-element of another fundamental right; namely, the right to privacy and integrity. Similarly, transparency – and more precisely public access to documents – is a newcomer in the field of fundamental rights. The extent to which these two rights should be pursued is also controversial.

The tension between these rights takes place in the form of colliding rules. The problem would be resolved if one of these principles could be seen as superior to the other one. Thus, it is necessary first address the question of whether data protection or transparency can be considered superior to the other or whether they both are considered fundamental rights in the sense of EU law. Only after this initial question is addressed can some more detailed and practical situations where the tension between the two rights is apparent be examined.

When the reconciliation exercise is carried out, it is essential to identify the hard core of the examined rights.[7] Reconciliation is possible only when the essence, or hard core, of the rights remains untouched. When the inviolable core of these rights has been identified, an attempt will be made to balance the underlying principles in order to reconcile the requirements of data protection legislation with the rights provided by the transparency legislation.

1.1 LEGAL AND SOCIETAL CONTEXT OF THE EXAMINED RIGHTS

To understand the significance of the tension between these two rights, they must first and foremost be placed in their legal and societal context.[8] Transparency and the right to public access to documents must be considered in a wider perspective

7 See for example T. Ojanen, "Making the essence of fundamental rights real: the Court of Justice of the European Union clarifies the structure of fundamental rights under the Charter" in *European Constitutional Law Review* 2 (2016); G. Van Der Schyff, Cutting to the Core of the Conflicting Rights: The question of inalienable Cores in Comparative Perspective, in Brems (ed.) *Conflicts between Fundamental Rights*, (Intersentia, 2008), 131–147.

8 On contextual interpretation of the essence of the fundamental rights, see for example T. Ojanen, "Making the essence of fundamental rights real: the Court of Justice of the European Union clarifies the structure of fundamental rights under the Charter" in *European Constitutional Law Review* 2 (2016), 326.

as a part of democratic society and, in particular, the democratic decision-making process.[9] As the core of the democracy is the idea of a nation as the sovereign of political power, it is easy to draw the connection between transparency and democracy. How could a nation form a position on anything if its people are not provided with the necessary information?[10] The connection between transparency and democracy is also clearly underlined in the second recital of the Transparency Regulation[11] which underlines that openness enables citizens to participate more closely in the decision-making process and guarantees that the administration enjoys greater legitimacy and is more effective and more accountable to the citizens in a democratic system. It goes even further, stating that openness contributes to strengthening the principles of democracy and respect for fundamental rights as laid down in Article 6 of the Treaty on European Union and the Charter of Fundamental Rights of the European Union.

Furthermore, an individual's right to privacy and to the protection of personal data must be examined as a part of democratic society and the democratic decision-making process.[12] Data protection will also be assessed in the wider context and in relation to the protection of privacy and integrity. For a long time, the core aim of the protection of personal data was seen as identical to the protection of privacy and integrity. This was clearly illustrated in, for instance, Article 1 of the Data Protection Regulation[13] according to which "*Community institutions or bodies shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data […]*". In this context, data protection could have been seen as a part of protection of privacy and integrity. It has also been suggested that privacy actually forms a part of data protection. It is therefore essential to examine the areas where these two rights overlap. Yet, there

9 The alliance between transparency and democracy has been recognized already in the early case-law. For example, in the case Council of the European Union v Hautala (353/99P), the Advocate General concluded that access to documents is a fundamental right. The ECJ did not confirm this approach, instead it underlined the importance of the public's right of access to documents held by public authorities and its connection with the democratic nature of the institutions. Similarly, in the so called Turco case (Case C-39/05 P and C-52/05 P, Kingdom of Sweden and Maurizio Turco v Council), Advocate General Maduro stated that Regulation 1049/2001 seeks to govern the exercise of a right which has acquired the status of fundamental right. ECJ maintained its neutral approach recalling the connection between public access to institutions' documents and the democratic nature of those institutions.

10 T. Pöysti, *Tehokkuus, informaatio ja eurooppalainen oikeusalue*, (Helsinki, 1999) 481.

11 Regulation (EC) No 1049/2001 of the European Parliament and the Council of 30 May 2001 regarding public access to European Parliament, Council, and Commission documents (OJ L 145, 31.5.2001, p. 43–48).

12 Case T-121/05, *Borax Europe v Commission,* ECLI:EU:T:2009:64; Case T-115/13, Dennekamp v Parliament, ECLI:EU:T:2015:497.

13 Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1–22). The Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39–98) does not contain similar wording.

is still room for the argument that protection of privacy includes the protection of personal data where it follows that the latter should be considered a sub-element to the protection of privacy. Therefore this aspect must be thoroughly examined.

1.2 COLLIDING RULES

Besides the theoretical and contextual setting introduced earlier, the tension between transparency and data protection culminates in a more detailed and concrete manner on the level of colliding rules, which are examples of issues pertaining to the surface level of law.[14] Next, some examples will be introduced where the tension is apparent and will be studied further in this thesis.

The first example is a situation where a person is requesting access to a document containing the applicant's own personal data. The Transparency Regulation does not address this situation any differently from other situations where the requested document contains personal data. However, based on the Data Protection Regulation, one has privileged access to his or her own personal data. Even if the applicant would not be entitled to have access to the document based on the Transparency Regulation, (s)he might have that right under the Data Protection Regulation. Applying the Data Protection Regulation instead of Transparency Regulation would lead to a more transparent approach in this case. The questions of how to deal with these situations, and what role the principle of good administration should have, arise in this context.

The second practical example relates to the applicant's onus to state reasons for the application. The Transparency Regulation aims to provide the widest possible access to the documents and as such, the applicant is not required to justify his or her application. Therefore, from the outset, the reasons for the request cannot have any relevance as such. Contrary to this approach, if the request for the information is based on the Data Protection Regulation, the applicant has to provide reasons for the request. The Court of Justice has taken a stand on this very precise question by stating that full application of both the Transparency Regulation and the Data Protection Regulation should be ensured, and the requirements set by the Data Protection Regulation cannot be set aside.[15] It follows that the applicant must provide some level of reasoning for the application when access to personal data is requested.

---

14 For levels of law, see Kaarlo Tuori, for example K.Tuori, "Law, Power and Critique", in Tuori et al. (ed.), Law and Power, Critical and Socio-Legal Essays, (Deborah Charles Publications, 1997) and K. Tuori, Critical Legal Positivism, (Hants, 2002).

15 See Case C-28/08P, Bavarian Lager, ECLI:EU:C:2010:378, para 56; Case T-115/13, *Dennekamp v Parliament*, ECLI:EU:T:2015:497. For a case comment, see for example O. Lynskey, "Data protection and freedom of information; reconciling the irreconcilable?", in *Cambridge Law Journal* 70 (2011), 37–39.

The entry into force of the EU Institutions' Data Protection Regulation clarifies this situation to a certain extent.

The third example is a recurring situation which relates to further transmission of personal data and the purpose limitation principle. An often repeated argument is that the access to a document cannot be granted as the document contains personal data and releasing it would violate those provisions of the Data Protection Regulation concerning the further transmission of personal data and the purpose limitation principle.[16] If this argument was accepted as such, it would lead to a situation where all requests for access to documents containing personal data could be refused based on this argument alone. Regardless of the nature of the personal data, it would never be released based on the Transparency Regulation and only partial access could be granted to the documents containing personal data.

A fourth example concerns the data subject's right to object the processing of data relating to him or her.[17] At the outset, the data subject's right to object the data processing reflects the value of self-determination and is justified in the data subject's relationship with the controller. In this thesis, however, it must be examined in relation to someone's right to information and as an element that restricts the said right. The scope of the right to object needs to be defined precisely and thereafter be placed in the context of the democratic decision-making process and the public's right to information.

1.3 CONTRIBUTION TO THE CURRENT DISCUSSION

The subject matter of this thesis has not been thoroughly examined previously, even if there are some early studies in this field, such as the dissertation of Herke Kranenborg at the University of Leiden on the relationship between data protection and access to documents. Unfortunately, this study was published in Dutch and, as such, is not accessible to a wider European audience.[18] Also, this dissertation was published in 2007, more than a decade ago. This was before the Court of Justice of the European Union delivered its landmark judgments, and before European data protection reform. That is to say some significant changes have taken place since its publication.

16 See for example Case T-529/09, *In 't Veld v Council*, ECLI:EU:T:2012:215, para 20; Case T36/04, *API v Commission*, ECLI:EU:T:2007:258, paras 54, 94.

17 See for example Case T-412/05, *M. v European Ombudsman*, ECLI:EU:T:2008:397; Case C-553/07, *College van burgemeester en vethounders van Rotterdam v E.E: Rijekeboer*; ECLI:EU:C:2009:293, paras 4, 16, 48, 52, 65.

18 H. Kranenborg, *Toegang tot documenten en bescherming van persoonsgegevens in de Europese Unie – Over de openbaarheid van persoonsgegevens* (Kluwer, 2007).

In Finland, the existing studies have primarily focused on the relationship between the rights of expression and privacy, or alternatively the focus has been in the national context.[19] The questions posed by this thesis have not been addressed by the previous studies. Considering that Finland as an actor in the European Union sets much weight on transparency and actively attempts to guide the EU as a whole towards a more transparent society, this lacuna in the research is regrettable.

Two topical developments emphasize the significance of this research. First, the European Union is currently in a transitional period. Extensive reform of the European data protection regime has just been concluded at the Union level. The Member States very recently finalized the adoption of the necessary measures to meet the requirements set by the General Data Protection Regulation and so-called Law Enforcement Directive.[20] And even more importantly, the interpretation of the new data protection instruments has not yet been settled. Furthermore, Convention 108 has been renegotiated and as an aftermath to the GDPR negotiations, the European Commission published its proposal for the Regulation concerning the processing of personal data in the Union institutions.[21] These negotiations were concluded on 23 May 2018.[22] The negotiations on the Transparency Regulation in turn have not been closed. This is, however, a *status quo*.

Also, the recent events that have taken place in the UK relating to Brexit seem to set heavy demands for the EU to strengthen the transparency in its decision-making structures, as lack of information turns easily into distrust. It is very tempting to draw the parallels between Brexit and the Danish rejection of the Maastricht

19 For example, Päivi Korpisaari (ex. Tiilikka) has a vast list of publications focusing on this question. Korpisaari has also contributed to the discussion related to access to information in the European legal framework; for that, see P. Tiilikka, "Access to Information as a Human Right in the Case Law of the European Court of Human Rights" in *The Journal of Media Law* 5(1) (2013). For Korpisaari see also *Henkilötiedot ja paikkatiedot: Miten tietosuojalainsäädäntö vaikuttaa paikkatietojen julkaisemiseen ja luovuttamiseen*, Ympäristöministeriö, 21.2.2018. See also R. Neuvonen, *Yksityisyyden suoja Suomessa*, (Lakimiesliiton kustannus, 2014) 161–184; H.Kulla & M.Koillinen, *Julkisuus ja henkilötietojen suoja viranomaistoiminnassa* (Turun yliopisto, 2014) and T.Voutilainen, *Oikeus tietoon – Informaatio-oikeuden perusteet* (Edita, 2012). For Nordic approach, see also J.Reichel, "The Swedish right to freedom of speech, EU data protection law and the question of territoriality", in A-S.Lind; J.Reichel & I.Österdahl (eds.), Transparency in the Future – Swedish Openness 250 years (Visby, 2017), 201–224. For the relationship between freedom of expression and protection of personal data in the cloud environment, see MCEL Working Paper series, Freedom of expression and Artificial Intelligence: on personalisation, disinformation and (lack of) horizontal effect of the Charter by Maja Brkan (March 17, 2019). Available on the internet < https://ssrn.com/abstract=3354180 > [last visited 1.5.2019].

20 Directive (EU) 2016/680 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 by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, p. 89–131).

21 Commission Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, COM(2017) 8 final (10.1.2017).

22 See for example Press release (23.5.2018) by Council of the European Union *New rules on data protection for EU institutions agreed* available <http://www.consilium.europa.eu/en/press/press-releases/2018/05/23/new-rules-on-data-protection-for-eu-institutions-agreed/> [last visited 21.7.2018]. The EU Institutions' Data Protection Regulation has now entered into force.

Treaty in 1992. The latter was followed by a flourishing discussion on public access to documents in the European Union.[23] This discussion drew from the discourse relating to the democratic decision-making process in the European Union.[24]

2. LIMITATIONS

The tension between transparency and data protection will be examined in the European legal framework. These rights are examined as fundamental rights and the essence of the said rights is at the core of this study. This limitation is significant in particular regarding the protection of personal data. This limitation excludes the commercial dimension of data protection from the scope of this study. The European Commission has stated that some evaluation has assessed that "*the value of European citizens' personal data has the potential to grow to nearly € 1 trillion annually by 2020*".[25] Thus the economic value of personal data is apparent.

Deriving partly from its economic value, the protection of personal data has several dimensions in the European legal framework. Data protection can be examined as one of the key elements of IT law, or consumer law[26] or contractual law[27] etc. The Data Protection Directive[28] was the first instrument regulating data protection in the European Union. It is of particular importance to note that the legal base for this Directive was Article 95 EC, which lays down the grounds for measures which have as their object the establishment and functioning of the internal market.[29] This aim was also clearly expressed in the Commission's

23 I. Harden, "The Revision of Regulation 1049/2001 on Public Access to Documents", in *European Public Law* 2 (2009), 239–256.

24 Commentary of the Charter of Fundamental Rights of the European Union, June 2006.

25 Commission factsheet on The EU Data Protection Reform and Big Data, March 2016, available on the internet < http://ec.europa.eu/justice/data-protection/files/data-protection-big-data_factsheet_web_en.pdf> [last visited 9.10.2016].

26 The role of data subject as consumer is of particular interest in this respect. For an analysis of the emergence of consumer law and data protection law, see N.Helberger, F.Zuiderveen Borgesius and A. Reyna, "The Perfect Match? A closer look at the relationship between EU consumer law and data protection law" in *Common Market Law Review* 54 (2017), 1427–1466.

27 For example, the contracts between controller and processor have a high significance in cloud environment. See also for example M. Brkan, "Data protection and European private international law: observing a bull in a China shop" in *International Data Privacy Law*, 5 (2015).

28 Directive 95/46/EC of the European Parliament and 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 (OJ L 281, 23.11.1995, p. 31–50).

29 The first paragraph of Article 95 states that "by way of derogation from Article 94 and save where otherwise provided in this Treaty, the following provisions shall apply for the achievement of the objectives set out in article 14. The Council shall, acting in accordance with the procedure referred to in article 251 and after consulting the Economic and Social Committee, adopt the measures for the approximation of the provisions laid down by law, regulation or administrative action in Member States *which have as their object the establishment and functioning of the internal market*. [...]"

explanatory memorandum on the Data Protection Directive, which underlined that the objective of the Directive is to allow personal data to flow freely from one Member State to another.[30] To achieve this aim, a high level of protection of personal data had to be ensured as well as security of data protection. In other words, the protection of one's privacy or personal data was not initially the goal itself. The actual aim was the free flow[31] of personal data and the high level of protection of one's personal data could be described rather as means to attain this goal. A similar approach can be identified when examining the OECD's Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Even if the need to protect privacy has been recognized in these guidelines, the actual interest seems to lie in the need to avoid the development of "unnecessary" hinderances to the free flow of data.[32]

An individual legal base for the protection of personal data was established only in the Treaty of Lisbon.[33] Together with the Charter of Fundamental Rights[34] these evolutions in the European legal framework have created solid bases for data protection to be acknowledged as fundamental right and this is where the focus of this thesis is laid.

Another significant limitation is the exclusion of access to personal data for the purposes of national security. This issue is clearly related to data protection's character as a fundamental right, not its economic value. However, this thesis does not seek the solution on how to balance one's right to protection of personal data with the need to ensure national security. When assessing the requirements drawn from ensuring national security vis-à-vis data subject's rights, the core question is how much a data subject's rights may be restricted for reasons of national security and the balance must be found in a relationship between the state and data subject.

---

30 Commission of the European Communities, Explanatory Memorandum com(92) 422 final.

31 See also for the case-law joined cases C-465/00, C-138/01 and C-139/01 Österreichischer Rundfunk and Others, ECLI:EU:C:2003:294, paras 39–42; case C-101, *Lindqvist*, ECLI:EU:C:2003:596, paras 79–81; Case C-73/07, *Satakunnan Markkinapörrsi and Satamedia*, ECLI:EU:C:2008:727, paras 51–53.

32 See the OECD original guidelines, OECD Council Recommendation concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (23 September 1980), available on the internet < http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm> [last visited 23.10.2016], see also the revised Recommendation adopted by the OECD Council on 11 June 2013, "Privacy Guidelines", available on the internet < ttp://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf> [last visited 23.10.2016].

33 Article 16 TFEU stipulates that "*1. Everyone has the right to the protection of personal data concerning them. 2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.*"

34 Article 8 for Charter of Fundamental Rights states that "*1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority.*"

The focus of this thesis is, however, balancing two fundamental rights. Finding a balanced approach to restrict one's right to protection of personal data is only one side of the coin. The other side of the coin is to find a balanced approach to restrict one's right of access to documents. While there are certainly still many relevant questions in the field of data protection and national security to be examined more profoundly, these highly relevant issues have already inspired quite a wide range of academic literature.[35]

The focus of the thesis is public access to documents containing personal data. Thereby the thesis does elaborate on how to disclose documents by anonymizing personal data. As anonymized personal data is no longer personal data, data protection legislation does not apply to such situations and information could be disclosed solely based on the Transparency Regulation.

Regarding transparency, the focus of this thesis will be on the European access to documents legislation. This excludes some transparency initiatives launched by the European Commission from the scope of this study. For example, the "lobbying register", or transparency register, if you wish.[36] The same applies also to some other developments, such as broadcasting Council meetings. The significance of these steps in paving the way towards a more transparent European Union must however be acknowledged.

The wider European legal framework sets the environment for the assessment of the founding principles for the fundamental rights examined in this thesis. When moving from the more general level into a more detailed assessment of the tension between the rules, the focus will be on the provisions of the EU Institutions' Data Protection Regulation and the Transparency Regulation; in other words, on the instruments applied by the EU institutions. Even if the rules of only these instruments will be examined, the assessment cannot be fully separated from the General Data Protection Regulation and the relevant national legislation regarding data protection and public access to documents. The examined rules reflect the more profound principles of the said rights. These principles are derived from the wider European legal framework, thus the ground from which these principles stem must be thoroughly covered.

35 See for example M.Tzanou, *The Added Value of Data Protection as a Fundamental Right in the EU Legal Order in the Context of Law Enforcement*, (EUI, 2012); A.Dimitrova and M.Brkan, "Balancing National Security and Data Protection: The role of EU and US Policy-Makers and Courts before after the NSA Affair", in *Journal of Common Market Studies* (2017) DOI.10.1111/jcms.12634. For more recent examples, see A.Vedaschi, "Privacy and data protection versus national security in transnational flights: the EU-Canada PNR agreement" in *International Data Privacy Law* 8 (2018) and O. Tambou, "Opinion 1/15 on the EU-Canada Passenger Name Record (PNR) Agreement: PNR Agreement Need to Be Compatible with EU Fundamental Rights", in *European Foreign Affairs Review* 23 (2018). See also O. Lynskey, *The Foundations of EU Data Protection Law*, (Oxford, 2015) 161–173.

36 For the Transparency Register, see Transparency and EU, available on the internet < http://ec.europa.eu/transparencyregister/public/homePage.do?locale=en#en> [last visited 23.10.2016].

3. JURISPRUDENTIAL FRAMEWORK

The research will be conducted in the framework of Constitutional EU and also wider European law. The third field of law framing this research is Information Law, which has slowly become an area of law in its own right.[37] While the collision of the examined rules exists in EU law – and more precisely in the legislation concerning the EU institutions – the solution for the tension is sought from European law in a wider sense. In addition to EU law, wider European law consists of the practice of the European Court of Human Rights and the European Convention on Human Rights and also national law and practice of the European states.

Thus, the study can be placed in the framework of legal positivism when it comes to the analysis of the colliding legal rules. This part of the thesis is a formation of normative legal analysis. However, critical legal positivism considers the examined rules only examples of issues pertaining to the surface level of law.[38] Separation of rules and principles in the line with the legal doctrines developed by gentlemen like Ronald Dworkin and Robert Alexy provides a method for deducting the solution for the collision from Tuori's deeper levels of law.[39] The deeper levels of law must be sought from the wider European regime and this part of the thesis is not limited to legal positivist analysis, but reaches the elements of something more enduring and universal, and therefore provides a twist of natural law as well.[40]

4. METHODOLOGY

The underlying theoretical foundation for this research is in the analysis of the nature of the transparency and data protection as rules, principles or policies.[41] This analysis will be carried out based on doctrines elaborated by such scholars as Ronald Dworkin, Robert Alexy, Konrad Hesse and Kaarlo Tuori. The characteristic elements of these doctrines are, for example, differentiating the rules and principles based on their nature, and rules being applied in an either-or manner, while principles carry

37 For Information Law as an independent area of law, see A.Saarenpää, "Legal Infomatics Today – The View from the University of Lapland", in A. Saarenpää & K. Sztobryn (eds.) *Lawyers in the Media Society, The Leal Challenges of the Media Society*, (Lapin yliopisto, 2016), 13.

38 For Tuori, see for example K.Tuori, "*Law, Power and Critique*", in Tuori et al. (ed.), *Law and Power, Critical and Socio-Legal Essays*, (Deborah Charles Publications, 1997) and K. Tuori, *Critical Legal Positivism*, (Hants, 2002).

39 For the three level of legal order, see K. Tuori, *Critical Legal Positivism*, (Hants, 2002).

40 For providing the means to diminish the unclarity between legal positivism and natural law, see J. Bengoetxea, *The legal Reasoning of the European Court of Justice*, (Oxford, 1993) 21.

41 See for example R. Dworkin, *Taking Rights Seriously* (London, 2009); R. Dworkin, Rights as Trumps, in Waldron (ed.) *Theories of Rights*, (Oxford, 1984); R. Alexy, *A Theory of Constitutional Rights* (Oxford, 2010).

dimension and allow balancing. Furthermore, the inviolable core of the rights, which in turn approaches the "rule-like" effect, will be assessed in order to gather the scope of the principles, which allows for balancing.[42] More profound assessment of the methodology applied in this research together with the setting of the jurisprudential framework will be provided in Chapter I.

The chosen methodology provided an excellent tool for assessing the core question of this thesis. Identifying the hard core, or the essence, of the right[43] did demonstrate that the inter-rights conflict was not total in Zucca's terms[44], but left room for balancing the principles in a manner which allowed the essence of the rights to be preserved.

5. TERMINOLOGY AND KEY DEFINITIONS

The most central concepts of this thesis will be elaborated in more detail in their respective chapters. Such concepts are for example personal data, the processing of personal data, document etc. The terms referring to these concepts are applied as they are established in European law. However, the exact content of these concepts still causes uncertainty and therefore they must be elaborated in detail with the appropriate references to relevant case-law. Furthermore, the content of these key concepts has a central role when balancing the protection of one's personal data with public access to documents. Thus, instead of repeating the definitions of respective laws, it suffices at this stage to note that definition of the terms corresponds to the definitions as they are adopted in the relevant legislation.

Nevertheless, some initial remarks of the applied terminology ought to be made. First, the Regulation 1049/2001 will be referred to in this thesis as the "Transparency Regulation". This might not be the most commonly applied name for the said Regulation; most often it is referred to as "Regulation 1049". While Regulation 1049/2001 covers public access to documents, transparency as a concept covers more widely other areas and instruments strengthening society's openness. Furthermore, it ought to be noted that when entering into the discussion of fundamental rights, it is precisely public access to documents, which has this status, not transparency in

42 See T. Ojanen, "Making the essence of fundamental rights real: the Court of Justice of the European Union clarifies the structure of fundamental rights under the Charter" in *European Constitutional Law Review* 2 (2016), 321–323; G. Van Der Schyff, Cutting to the Core of the Conflicting Rights: The question of inalienable Cores in Comparative Perspective, in Brems (ed.) *Conflicts between Fundamental Rights*, (Intersentia, 2008), 131–147.

43 See T. Ojanen, "Making the essence of fundamental rights real: the Court of Justice of the European Union clarifies the structure of fundamental rights under the Charter" in *European Constitutional Law Review* 2 (2016), 321–323.

44 L. Zucca, Conflicts of Fundamental Rights as Constitutional Dilemmas, in Brems (ed.) *Conflicts between Fundamental Rights*, (Intersentia, 2008), 26–28.

broader terms. However, for the purposes of making the text more reader-friendly, the vocabulary used in this thesis adopts "Transparency Regulation".

Furthermore, to separate Data Protection Regulation 45/2001 from the General Data Protection Regulation, it is referred to as the Data Protection Regulation. For the General Data Protection Regulation, the abbreviation GDPR will be applied. The Data Protection Regulation is applied by the EU institutions where the GDPR is applied by private sector actors and Members States' public sectors.[45] The GDPR sets an obligation for the European Commission to submit legislative proposals when this is needed in order to ensure that the processing of personal data will be uniform and consistent. The obligation to put forward a legislative proposal regarding the processing of personal data by the Union institutions was underlined and the Commission gave its proposal accordingly.[46] The new Data Protection Regulation for the EU institutions will be called the "EU Institutions' Data Protection Regulation".[47] This thesis was initially drafted based on the former Data Protection Regulation, but the text has been aligned with the EU Institutions' Data Protection Regulation. Where there is a difference in the former Data Protection Regulation and the renewed EU Institutions' Data Protection Regulation, this is specifically mentioned. The most significant amendment relates to the provisions on justifying the application. The analysis of the case-law is based on the former data protection regime, as there is no case-law on the interpretation of the EU Institutions' Data Protection Regulation yet. The EU Institutions' Data Protection Regulation does not have an influence on this analysis, but it might confirm certain conclusions drawn in the analysis.

The Data Protection Directive refers to the EU Data Protection Directive 95/46/EC.[48] The GDPR has now replaced the Data Protection Directive. Even though the GDPR entered into force in May 2016, it became applicable only in May 2018. Thus, the Member State legislation which is based on the Data Protection Directive was still in force in May 2018. At the same time as the GDPR, a Directive regarding the processing of personal data in the context of police and judicial cooperation was adopted.[49] The "Law Enforcement Directive" (LED) will not be examined in this

45 The national flexibility provided in the GDPR leaves a wide margin for the member states to adopt more specific data protection legislation in the public sector. See for example Article 6(3) and 23 of GDPR.

46 See Article 98 of GDPR.

47 The Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39–98).

48 Directive 95/46/EC of the European Parliament and 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 (OJ L 281, 23.11.1995, p. 31–50).

49 Directive (EU) 2016/680 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 by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, p. 89–131).

thesis. The Data Protection Directive should also be separated from the so-called ePrivacy Directive.[50] Following the adoption of the GDPR, the European Commission did launch a consultation on the ePrivacy Directive with a view to reviewing it as a part of the Digital Single Market Strategy.[51] The consultation led to Commission's proposal for Regulation on Privacy and Electronic Communications.[52]

The Court of Justice of the European Union will be referred as the CJEU. This abbreviation will be applied also in such cases where the Court delivered its judgment in an era before the structural changes concerning the Court, instead of using the abbreviation commonly applied before these changes (ECJ). Similarly, the established abbreviations for European Court of Human Rights (ECtHR), The Treaty on the European Union (TEU),, Treaty on the Functioning of the European Union (TFEU) and European Convention of Human Rights (ECHR) will be applied in this thesis.

6. SOURCES

The research is mainly based on the legal documents of the European Union and the Council of Europe. The focus will be on the EU's primary legislation and the Charter of Fundamental Rights and the Treaty on the Functioning of the European Union. Secondary EU legislation will also be applied as a source. Thus Directives, Regulations, Council Decisions etc. will be applied as sources. Where publicly available, the preparatory work of secondary legislation has also provided a significant source for the thesis. Furthermore, the case-law of the Court of Justice of the European Union and the European Court of Human Rights will provide significant source for the research. National legislation and national decisions by different bodies will provide further support in relation to certain questions examined in this research. In addition, opinions and statements by such institutions as the European Data Protection Supervisor (EDPS), the Article 29 Working Party (WP29) and its current formation, the European Data Protection Board (EDPB) and European Ombudsman will provide important input to the sources of the thesis. Furthermore, the Council's replies to confirmatory applications will also provide

50 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37–47).

51 The Digital Single Market Strategy is one of the European Commission's priorities. For more, see "Digital Single Market, Bringing down barriers to unlock online opportunities", available on the internet < http://ec.europa.eu/priorities/digital-single-market/> [last visited 16.10.2016].

52 Commission Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM(2017) 10 final (10.1.2017).

an additional source for the thesis. Case-law, academic literature and legislative processes have been followed up to August 2019.

The emphasis on the sources will be on the legal and official documents. As the European data protection regime has recently gone through a vast reform, the academic literature can at this stage provide well-reasoned opinions. No settled case-law or practice by the data protection authorities exist just yet. However, the academic literature provides significant support when individual issues are studied. This is in particular the case with data protection, which itself has stimulated various studies from several different angles. The academic literature on transparency and in particular public access to documents is more scarce, but it does exist. Academic literature applied in this research will contain scientific articles, commentaries, studies, case notes etc.

In the interests of transparency, the author's official post in the Finnish administration should be acknowledged. The author represented the Finnish government in the GDPR negotiations in the DAPIX working party in the Council, participating in the GDPR drafting process. The author has also participated or had the responsibility of numerous other data protection files, including the EU Institutions' Data Protection Regulation. The author was also part of the Finnish delegation in the reform negotiations for the Transparency Regulation. Currently the author holds a post as Deputy Data Protection Ombudsman in Finland.

7. STRUCTURE

This thesis consists of two parts; the General Part and the Case studies. These two parts will be followed by the concluding remarks. The first chapter of the General Part will introduce the theoretical foundations for the research. This will be followed by chapters which will discuss transparency legislation and more precisely the public access to documents regime in the European legal framework, followed by similar analysis of European data protection legislation. These chapters will concentrate on concepts which are relevant when examining the relationship between transparency and the protection of personal data. Once the necessary elements for understanding the background and the context where the examined tension occurs have been clarified, some more concrete situations of tension will be tackled in the fifth and sixth chapters. These situations are not only theoretical, but have also materialized in the case-law of the Court of Justice of the European Union or taken place in the European institutions' practice when assessing whether access to document should be granted. The last section will draw together all of the earlier sections and provide a solution on how to balance transparency together with data protection requirements. Next the content of different chapters of the thesis will be elaborated in more detail.

PART 1, GENERAL PART

Chapter I provides the theoretical foundations for the research. This chapter draws on the writings of Dworkin and Alexy in particular, but also on more recent scholars such as Zucca. The chapter builds also on Kaarlo Tuori (Finland), Konrad Hesse etc.

Chapter II provides a short overview of the developments and "history" of data protection and transparency legislation, and draws together the developments of these rights. As both data protection and access to documents are relatively new concepts, particularly in the field of fundamental rights, this chapter provides useful background information on the context and societal environment where the development of these concepts took place.

Chapter III examines some of the core concepts of European transparency legislation. While these concepts are presented in the general framework of European transparency regulation, the purpose of this chapter is not to provide an exhaustive picture of the said legislative framework. Instead the focus will be on selected key concepts, which are essential to first identify and then elaborate, as these concepts will play a significant role later in this thesis, when the tension between transparency and data protection will be tackled. When the tension between transparency and data protection is elaborated, it is fundamental to understand the dimensions of these concepts as well as how they function.

First, a general overview of transparency regulation in Europe will be provided. The relationship between democracy and transparency together with transparency's nature as a fundamental right is discussed first. This is followed by discussion of some of the most relevant concepts related to this legislation and how they are to be understood in the European legal framework. This will be followed by the identification and elaboration of the core principles of transparency regulation. Without a thorough understanding of these principles, one cannot fully comprehend European transparency regulation.

Chapter IV will provide a similar overview of the data protection concepts to the one provided in Chapter III for transparency. It will first elaborate on data protection as a fundamental right. The data subject's right to self-determination is of particular interest in this section. After data protection as fundamental right and its relation to democracy has been addressed, central data protection concepts and data protection principles, which should be separated from Dworkin's and Alexy's principles, are elaborated. This section covers, for example, the concept of *personal data* and the *purpose limitation principle*. Also, some other data protection elements, which are particularly important in relation to transparency, will be elaborated. These are, for

example, *consent* and the *right of access to personal data*. Lastly, some new data protection elements will be assessed, and a short overview of Europe's new data protection regime will be provided.

PART 2, CASE STUDIES

Once the central concepts and principles of transparency and data protection legislation have been established in the previous chapters, **Chapter V** focuses on the dilemmas caused by competing rules and principles in the given framework. This chapter elaborates on the tension between data protection and transparency in light of the recent case-law of European Courts. It will identify the dilemmas and give indications on possible solutions raised by the case-law. The chapter has three main sections and a conclusion. The first section focuses on the case-law of the Court of Justice of the European Union. It examines four significant judgments of Luxembourg courts, Bavarian Lager, Satakunnan Markkinpörssi, Volker un Markus Schecke GbR and Dennekamp. The second section of this chapter will focus on the case-law of the European Court of Human Rights. While this section gives a broader European perspective on the issues discussed in this thesis, it will also provide some indications on how to solve the dilemmas arising from the simultaneous application of the two Regulations. The third section of this chapter will draw together the different elements of the central issues discussed in the chapter, such as consent of the data subject, stating reasons for the application and professional activities.

Chapter VI will elaborate further on the tension discussed in the previous chapter. While Chapter V focused on the dilemmas that have arisen in the aftermath of recent case-law, this chapter will focus on dilemmas not yet addressed by the courts. Besides completing the previous chapter on the elements causing tension between transparency and data protection, it will also elaborate further on some of the questions covered in Chapter V.

The issues discussed in this chapter include access to one's own personal data, further transmission of personal data, the purpose limitation principle, and the data subject's right to object and stating reasons for the application.

The Concludind Chapter – From simply sharing the cage to living together – will draw together the discussion from the previous chapters. The core dilemmas causing the tension on the surface level of law together with some indications of how to solve these dilemmas and how to deduct the solution by identifying the underlying principles and the essence, or hard core, of the rights were elaborated in the previous chapters. Thus, at this stage, the reader should have the relevant information on the transparency and data protection regimes for

the final discussion. The concluding chapter will focus on resolving the dilemma of competing rules and principles. While the theoretical framework provides the means to deduct an answer for the dilemmas examined in this thesis, an attempt at a more concrete solution will be provided.

PART 1
GENERAL PART

CHAPTER I

THEORETICAL FOUNDATIONS; CLASHING PRINCIPLES

This chapter will provide an overview of the theoretical foundations of this thesis. The objective of this thesis is to provide a structuralized approach to the simultaneous application of the Transparency and the Data Protection Regulations where the essence of both rights is appropriately acknowledged. Instead of addressing this aim by examining solely the underlying objectives of the Regulations, the theoretical framework will provide the means for deeper understanding of the research question by identifying the underlying principles and the essence of the said rights. Even more importantly, it frames and provides the structure for the research and for the sought solution.

When seeking a fair balance between two rights, the theories of clashing principles and rules become interesting. This question has been thoroughly discussed in the legal field, yet it seems like it has not been entirely exhausted.[53] There are numerous participants in this discussion, but the contributions of two scholars are of particular interest in this thesis: Ronald Dworkin and Robert Alexy. While Ronald Dworkin initiated the intense debate over the theory of clashing principles, Robert Alexy is of equal importance, providing the necessary angle for examining these issues from the civil law perspective.[54] These gentlemen share many of the founding ideas of the theories of clashing principles, which will serve as a basis for the discussion in this thesis. It must also be acknowledged that some of the participants in the discussion of clashing principles do not agree, at least not entirely, with all the components of the doctrines developed by the two gentlemen.[55]

As established earlier, this thesis can be placed within the fields of European and Constitutional law. As such, the purpose of the theory of the colliding legal principles and rights is to serve as a tool in this research, not as the purpose itself. However,

53 See for instance J. Raz "Legal Principles and the Limits of Law" in *The Yale Law Journal* 81 (1972), 823–854 and J. Raz, *the Authority of Law, Essays on Law and Morality*, (Oxford, 1979), 53–77; M.Rosenfeld, *Law, Justice, Democracy, and the Clash of Cultures* (Cambridge, 2011) 182–207. In Finland, see also for example A. Aarnio, On Rules and Principle, A Critical Point of View, in Aerschot (ed.) *Juhlakirja, Kaarlo Tuori, 50 vuotta*, (Helsinki, 1998), 83–96.

54 R. Dworkin, *Taking Rights Seriously*, (London, 2009); R. Alexy, *A Theory of Constitutional Rights*, (Oxford, 2010).

55 See for example H.L. Hart.

the importance of this tool is evident. Just consider the statement of Alexy: "*without [the distinction of rules and principles] there can be neither an adequate theory of the limitation of rights, nor an acceptable doctrine of the conflict of rights, nor a sufficient theory of the role of constitutional rights in the legal system*".[56] While acknowledging the significance of the theoretical foundations of clashing principles and rights, this thesis will not elaborate on this aspect in great detail as the theoretical foundations will first and foremost provide an angle and an approach to examine the core question of the thesis. A short overview of the theoretical foundations together with the core concepts of the theories will be provided next. Before entering into the said discussion, the basic elements of limiting fundamental rights in the European legal framework will be covered. This is followed by the discussion of the concepts of principles and rights. Thereafter, the dilemma of clashing principles will be tackled. As a last element of this chapter, democracy will be briefly discussed. The last element of this chapter is necessary in order to give an exhaustive picture of the framework in which the research question is examined. The entire research question must be examined in the context of democratic legitimacy and therefore the different doctrines of democracy contribute to the theoretical framework of the thesis.

1. LIMITING FUNDAMENTAL RIGHTS IN THE EUROPEAN LEGAL FRAMEWORK

When seeking a balanced approach for the simultaneous application of two rights, the question of restricting rights becomes relevant. First, it must be noted that the sole fact of limiting a fundamental right to realize another fundamental right does not necessarily lead to the collision of rights. Fundamental rights can be limited, but restrictions to fundamental rights cannot be arbitrary or disproportionate. The Charter of Fundamental Rights sets clear parameters for limiting the rights recognized by the Charter. The tension examined in this thesis exists in the European Union legal framework. Therefore, the Charter provides the primary frames for assessing how the said rights may be restricted. The practice of the European Court of Human Rights is also relevant in this assessment. Article 52(1) of the Charter states that

> *"Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and essence of those rights and freedoms. Subject to the principle of proportionality, limitations*

56 R. Alexy, *A Theory of Constitutional Rights*, (Oxford, 2010) 44.

> *may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others."*[57]

At least four elements which need to be met when fundamental rights are limited can be distinguished. First, limitations must be provided for by law. Second, the essence of the rights at stake must be preserved. The third and fourth elements emerge in the requirement of proportionality; limitations must be necessary and meet the objectives recognized by the European Union or be required to protect other rights.[58]

1.1 PROVIDED FOR BY LAW

The limitations on fundamental rights must be provided for by law.[59] At the outset, the criteria seem quite clear, however, the question of what law is might arise in some hard cases. The first time the CJEU addressed this question was in the context of the WebMindLicenses case. While referring to the case-law of the European Court of Human Rights, the CJEU set a particular weight in its assessment on the question of whether the legal basis for the measures in the said case was sufficiently *clear* and *precise*. In other words, clearness and preciseness were essential criteria in defining what is law in the sense of Article 52(1). Furthermore, the CJEU emphasized the need to *define the scope of the limitation*. It underlined that this provides a protection against arbitrary interference by the authorities.[60] Thus the CJEU's interpretation was not based on formal requirements, but rather on substantive ones, when defining the criteria to be met when assessing what law is in the meaning of Article 52(1).

The interpretation of the CJEU follows the settled practice of the European Court of Human Rights.[61] In its assessment, the ECtHR first establishes whether

---

57 Article 52(1) of the Charter of Fundamental Rights of European Union. Furthermore, paragraph 3 of the same article clarifies that "*in so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection.*"

58 Article 52(1) of the Charter of Fundamental Rights of European Union.

59 See for example case C-73/16, *Puskar v Financne riaditel'stvo Slovenskej republiky etc*, EU:ECLI:C:2017:725, paras 62–63; Joined cases C-439/14 and C-448/14, *SC Star Storage SA etc*, ECLI:EU:C:2016:688, para 49–50; case C-650/13, *Delvige*, ECLI:EU:C:2015:648, para 46–47.

60 For case-law on the content of the concept of law, see case C-419/14, *WebMindLicenses,* ECLI:EU:C:2015:832, para 81; ECtHR 2 August 1984, *Malone v the United Kingdom,* ECLI:CE:ECHR:1984:0802JUD000869179, para 67; ECtHR 12 January 2010, *Gillan and Quinton v the United Kingdom*, ECLI:CE:ECHR:2010:0112JUD000415805, para 77.

61 See for example ECtHR 14 September 2010, *Sanoma Uitgevers B.V. v the Netherlands*, ECLI:CE:ECHR:2010:0914JUD003822403, paras 83 and ECtHR 10 November 2005, *Leyla Sahin v Turkey*, ECLI:CE:ECHR:2005:1110JUD004477498, paras 88.

there is an interference of a right provided by the Convention on Human Rights. As a second step, it examines if this interference is prescribed by law. The basis for the interference might be laid down in a legislative act, an act of the executive or administrative authorities, a systematic practice or momentary act, etc.[62] In its assessment the ECtHR has set a particular emphasis on the clearness and preciseness of the legal basis. This allows those concerned to act accordingly and seek expert advice when needed. Furthermore, this is also closely linked with the requirement for predictability.[63] Similarly, the CJEU has emphasized that "*the principle of legal certainty requires that Community rules enable those concerned to know precisely the extent of the obligations which are imposed on them. Individuals must be able to ascertain unequivocally what their rights and obligations are…*".[64] Furthermore, the ECtHR has emphasized in its case-law that the legal basis setting the limitations for the rights must also provide sufficient protection against arbitrary measures. It follows that the powers of the competent authorities must have been clearly defined.[65]

To conclude, the case-law of the European courts do not set formal but rather substantive requirements for the law or legal basis when fundamental rights are restricted. This does not, however, prevent the national legislator from setting more formal requirements when it comes to national law.[66]

1.2 THE ESSENCE OF THE RIGHT

The limitations to fundamental rights provided by the Charter may not be limited in a manner which would infringe the essence of the right. The essence might also be referred to as the hard core of the right. The proportionality doctrine has been elaborated in a reasonable amount of detail by the European courts, however, the

62 L. Cariolou, "The search for an equilibrium by the European Court of Human Rights", in Brems (ed.) *Conflicts between Fundamental Rights*, (Intersentia, 2008), 249–251.

63 ECtHR 14 September 2010, *Sanoma Uitgevers B.V. v the Netherlands*, ECLI:CE:ECHR:2010:0914JUD003822403, paras 81–82; ECtHR 31 March 2016, *Stoyanov etc. v Bulgaria*, ECLI:CE:ECHR:2016:0331JUD005538810, paras 124–126.

64 See case C-345/06, *Heinrich*, ECLI:EU:C:2009:140, para 44 and case C-158/06, *ROM-projecten*, ECLI:EU:C:2007:370, para 25.

65 ECtHR 14 September 2010, *Sanoma Uitgevers B.V. v the Netherlands*, ECLI:CE:ECHR:2010:0914JUD003822403, paras 81–82; ECtHR 31 March 2016, *Stoyanov etc. v Bulgaria*, ECLI:CE:ECHR:2016:0331JUD005538810, paras 124–126. See also see case C-419/14, *WebMindLicenses,* ECLI:EU:C:2015:832, paras 81, 84.

66 See also for example recital 41 of the GDPR. Recital 41 states that "*where this Regulation refers to a legal basis or a legislative measure, this does not necessarily require a legislative act adopted by a parliament, without prejudice to requirements pursuant to the constitutional order of the Member State concerned. However, such a legal basis or legislative measure should be clear and precise and its application should be foreseeable to persons subject to it, in accordance with the case-law of the Court of Justice of the European Union and the European Court of Human Rights*".

identification of the essence of the right has not yet provided a similar contribution to legal doctrines.[67]

The CJEU has applied Article 52(1) several times, which includes the requirement of non-violation of the essence of the fundamental right. Yet, it appears that the court is often satisfied by merely noting that the essence of the right has not been violated and rather grounds its argumentation on the proportionality test. For example, the question of the essence of the protection of personal data was touched upon in such cases as Tele2 Sverige, Digital Rights Ireland and Schecke. In its Tele2 Sverige decision the CJEU did state that the data retention in question did not affect the essence of the rights as the content of the communication was not in the scope of the said retention.[68] In its earlier judgment in the Digital Rights Ireland case, the CJEU came to a similar conclusion; the essence of the right was not violated. The CJEU did hold the examined Directive void based on the proportionality test instead.[69] The Court's approach seems very reasonable and also pragmatic. The proportionality test does leave margin for reassessment of the chosen measures in order to, for example, adjust the Union legislation with the requirements set by the Court. To pronounce a violation of the essence would instead lead to a situation wherein there is no future measure available to rectify the situation.

Another question is how clearly the essence of the right can be separated from the proportionality test. The inviolable core and how it is to be identified will be further examined as a part of the balancing test in section 3.2.2.1.

1.3 PROPORTIONALITY

The Charter states that the limitation must be carried out in accordance with the principle of proportionality; limitations may be made only if they are necessary. In other words, Article 52 sets a requirement for the proportionality test when fundamental rights are limited. The third and fourth elements which were established earlier are both present in the said requirement. In other words, limitations must be necessary and meet the objectives recognized by the European Union or needed to protect other rights.

The CJEU has a long lineage when it comes to applying the proportionality test.[70] Even if the proportionality test was initially applied when assessing whether

67 For the essence of the right, see also M. Brkan, "The Concept of Essence of Fundamental Rights in the EU Legal Order: Peeling the Onion to its Core", in *European Constitutional Law Review*, 2(2018), 332–368.

68 Case C-203/15, *Tele2 Sverige*, ECLI:EU:C:2016:970, paras 100–101.

69 See case C-203/15, *Tele2 Sverige*, ECLI:EU:C:2016:970, para 101; Joined cases C-293/12 and C-594/12 *Digital Rights Ireland and Kärtner Landesregierung*, ECLI:EU:C:2014:238, paras 26–30, 65.

70 See for example case C-331/88, *R v Minister Agriculture, Fisheries and Food, ex parte Fedesa etc.*, ECLI:EU:C:1990:391. For the CJEU's case-law on proportionality and the appropriate measures to achieve

the Union measures had exceeded what is necessary to achieve the aims set by the Treaties, the basic elements of the test as formulated in the Fedesa case, are very similar to those applied when the limitations of fundamental rights are stake. These are: 1) The measure must be suitable to achieve a legitimate aim, 2) The measure must be necessary to achieve the said aim, 3) The measure must not have an excessive effect on the applicant's interest.[71]

In the context of fundamental rights, the proportionality test is more recent in the EU's legal framework. Until quite recently, fundamental rights have been established, developed and protected only through the case-law of the CJEU. This changed with the entry into force of the Treaty of Lisbon and the Charter of Fundamental Rights. The Charter is now endowed with the same weight and importance as founding treaties.

When fundamental rights emerged on the scene of the EU regime, they were at first balanced with the economic freedoms.[72] Then the core question was whether a fundamental right could constitute a rightful reason to deviate from the freedoms provided by the founding treaties.[73] Only later was the proportionality test applied in the context of limiting fundamental rights.

When it comes to the European Court of Human Rights, the proportionality test has formed an essential element in the assessment of limitations to rights for longer. The proportionality assessment by the ECtHR culminates in the evaluation of whether an interference is necessary in a democratic society. When assessing whether such a pressing social need exists, which justifies the interference, the ECtHR has paid attention to the relevance of the measures and also sufficient reasoning of the contracting parties.[74]

The first time the CJEU confirmed the Charter's binding nature was when it applied the proportionality test provided by Article 52 while assessing the rightful interference of one's right to protection of personal data and privacy in the Schecke case.[75]

---

the legitimate objectives and on the question of not exceeding what is appropriate and necessary, see case C343/09, *Afton Chemical,* ECLI:EU:C:2010:419, para 45; joined cases C581/10 and C629/10, *Nelson and Others*, ECLI:EU:C:2012:657, para 71; case C283/11, *Sky Österreich*, ECLI:EU:C:2013:28, para 50 and case C101/12, *Schaible*, ECLI:EU:C:2013:661, para 29. For assessing the aims pursued by certain restrictions, see case C-398/15, *Manni*, ECLI:EU:C:2017:197, paras 48–61.

71 Case C-331/88, *R v Minister Agriculture, Fisheries and Food, ex parte Fedesa etc.,* ECLI:EU:C:1990:391.

72 See for example J.H. Jans, "Proportionality Revisited" in *Legal Issues of Economic Integration*, 27(2000).

73 See for example case C-112/00, *Schmidtberger*, ECLI:EU:C:2003:333; case C-341/05, *Laval un Partneri*, ECLI:EU:C:2007:809; case C-438/05, *The International Transport Workers' Federation ja The Finnish Seamen's Union*, ECLI:EU:C:2007:772 and case C-36/02, *Omega*, ECLI:EU:C:2004:614. For balancing fundamental rights with the freedoms provided by the Treaties, see also S.A de Vries, "Balancing Fundamental Rights with Economic Freedoms According to the European Court of Justice", in *Utrecht Law Review* 9(1) (2013), 169–192.

74 See for example ECtHR 25 November 1999, *Nilsen and Johnsen v Norway* (1999–VIII), para 43.

75 Joined cases C-92/09 and C-93/09, *Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen*, ECLI:EU:C:2010:662.

When the proportionality test is applied, Alexy's *law of balancing* and Hesse's doctrine of *practical concordance* become of particular interest. These doctrines will be soon studied in more detail together with the thesis developed by Dworkin. At this stage it suffices to note that the doctrine elaborated by Konrad Hesse is considered a limitation tool, but also a tool for interpretation. When practical concordance is applied, all constitutional rights and values are considered of equal rank. When a tension between two competing rights exist, both rights are considered variable. This enables a context-based assessment and a balanced solution can be sought based on the specific circumstances of the case.[76]

Quite interestingly, practical concordance sets lot of weight on the object and purpose when the proportionality test is carried out.[77] This leads to the following question: how would this relate to Dworkin's separation of principles and policies where policies, which are drawn from the objectives and aims, are always superseded by principles in a case of collision.[78] I see that practical concordance gives a tool to assess how policies are to be taken into consideration in balancing. While Dworkin never denies the role of policies in the balancing[79], Hesse's practical concordance structures how to take them into consideration when balancing two rights; as a part of proportionality test. Thus, these two doctrines seem to complete one another.

Finally, the Charter of Fundamental Rights stresses that limitations must meet the objectives recognized by the Union.[80] In the case-law of the ECtHR, it has been similarly underlined that the limitations to human rights must be necessary in a democratic society.[81] These requirements can be rendered to Hesse's context-based approach. It must be noted that when assessing the objectives of the Union and what is necessary in democratic society, the following remarks can be made. On the one hand, the requirement to meet the objectives recognized by the Union can be considered wider in a sense that it implies that the core freedoms on which the

76 K. Hesse, *Grundzüge des Verfaussungsrechts der Bundesrepublik Deutschland*, (Heidelberg, 1990) 142; T. Marauhn and N.Puppel, Balancing Conflicting Human Rights: Konrad Hesse's notion of "*Praktische Kokordanz*" and the German Federal Constitutional Court, in Brems (ed.) *Conflicts between Fundamental Rights*, (Intersentia, 2008), 279–281, 296.

77 K. Hesse, *Grundzüge des Verfaussungsrechts der Bundesrepublik Deutschland*, (Heidelberg, 1990) 142; T. Marauhn and N.Puppel, Balancing Conflicting Human Rights: Konrad Hesse's notion of "*Praktische Kokordanz*" and the German Federal Constitutional Court, in Brems (ed.) *Conflicts between Fundamental Rights*, (Intersentia, 2008), 281.

78 R. Dworkin, *Taking Rights Seriously,* (London, 1977) 90–122.

79 R. Dworkin, *Taking Rights Seriously*, (London, 2009) 116–117.

80 For example the fight against international terrorism and serious crime have been considered as an objective of general interest in the CJEU's case-law. See for example joined cases C402/05 P and C415/05 P, *Kadi and Al Barakaat International Foundation* v *Council and Commission*, ECLI:EU:C:2008:461, para 363 and joined cases C539/10 P and C550/10 P, *Al-Aqsa* v *Council*, ECLI:EU:C:2012:711, para 130.

81 See Article 52(1) in the Charter of Fundamental Rights of European Union or Articles 8(2) and 10(2) of the European Convention on Human Rights; see also for example R.Gisbert, The Right to Freedom of expression in a democratic Society (Art. 20 ECHR), in Garcia Roca & Santolaya (eds.) *Europe of Rights: A Compendium of the European Convention of Human Rights*, (Leiden, 2012), 371–401.

Union is established must be taken appropriately into account when limiting rights. These are the freedoms creating a basis for the internal market and having therefore strong economic influence. On the other hand, the notion of a democratic society is wider in the sense that it is not limited to the European Union, but contains elements of democracy more widely.

2. PRINCIPLES AND RIGHTS

The short discussion of the basic elements of limiting rights in the European legal framework paved the way for what will follow now; a study of the concepts of principles and rights and, in particular, the discussion of clashing rights and principles which will follow thereafter.

To start with, it should be noted that the number of rights, which are considered fundamental rights, has increased over the past years. Besides classic negative rights, a whole new generation of positive fundamental rights has appeared.[82] The rights examined in this thesis, the right to protection of personal data and the right of access to documents, are relatively new in the field of fundamental rights. These rights have previously been protected through other rights, but they are now considered independent, individual rights.

The proliferation of fundamental rights has also led to questioning whether fundamental rights should be treated differently from other interests and rights.[83] While this question is acknowledged in this thesis, the baseline assumption is that fundamental rights are considered to trump others. Policies, aims and objectives provide significant elements to be taken into consideration when balancing is carried out, but these elements cannot outweigh rights. While these elements are considered relevant in balancing, it must be underlined that democracy is more than just a significant element in balancing. As was established in chapter 1, when the limitation of a fundamental right is necessary in a democratic society, it is justified. In other words, democracy forms an essential element in the balancing test.

2.1 PRINCIPLES

Principles form the basis for the rights and are therefore an important element in legal reasoning. As Dworkin notes in one of his writings, "*legal practice, unlike many*

82 J.H. Gerards, Fundamental rights and other interests: Should it really make a difference, in Brems (ed.) *Conflicts between Fundamental Rights*, (Intersentia, 2008), 655–659.

83 Ibid.; R. Dworkin, Rights as Trumps, in Waldron (ed.) *Theories of Rights*, (Oxford, 1984), 153–167.

other social phenomena, is argumentative. Every actor in the practice understands that what it permits or requires depends on the truth of certain propositions that are given sense only by and within the practice; the practice consists in large part in deploying and arguing about the propositions".[84] Therefore, those with the best information on the propositions describing rights would seem to have an advantage in legal discourse.[85]

Dimension is a characteristic and distinctive element of principle; principles are said to carry a dimension. In other words, principles are not applied in an either-or manner. This is a matter where Dworkin and Alexy seem to very much agree, even if there are some other noteworthy differences in their doctrines.[86] Despite the differences, simultaneous application of their doctrines is indeed feasible. Firstly, Dworkin's interpretation of principles is narrower than Alexy's. Dworkin's more narrow interpretation of principles draws from the difference between individual and collective good. Dworkin links principles with individual good and sees that they create the backbone for the arguments of individual rights; collective rights Dworkin relates with policies.[87] This is a difference, which Alexy does not make. His interpretation of principles is broader and includes collective good as well.[88] Secondly, Alexy sees principles as optimization requirements.[89] As he puts it, "*principles require that something be realized to the greatest extent legally and factually possible*".[90] These differences are not necessarily contradictory, and, as underlined earlier, do not hinder the assessment of principles based on Dworkin and Alexy simultaneously. Furthermore, both of these scholars agree on the distinction between principles and rules.[91] Even if this difference is not the focal point of this study, and the focus of the research is rather on the underlying principles as such, this distinction is significant in order to provide a better understanding and a more comprehensive picture of the functioning of the principles.

84 R. Dworkin, *Law's Empire*, (Oxford, 1998) 13.

85 See for example K. Tuori, Law, Power and Critique, in Tuori et al. (ed.) *Law and Power, Critical and Socio-Legal Essays*, (Deborah Charles Publications, 1997), 7. Tuori notes that *the only power in discourses is that of better argument*.

86 R. Alexy, *A Theory of Constitutional Rights*, (Oxford, 2010) 48–54; R. Dworkin, *Taking Rights Seriously*, (Duckworth, 1977) 22.

87 R. Dworkin, *Taking Rights Seriously*, (London, 2009) 90–100.

88 R. Alexy, *A Theory of Constitutional Rights*, (Oxford, 2010) 62.

89 R. Alexy, *A Theory of Constitutional Rights*, (Oxford, 2010), 48; for more, see also K. Möller, "*Balancing and the structure of constitutional rights*" in Constitutional Law 5 (2007), 453–468.

90 R. Alexy, *A Theory of Constitutional Rights*, (Oxford, 2010) 57; K. Hesse, *Grundzüge des Verfaussungsrechts der Bundesrepublik Deutschland*, (Heidelberg, 1990) 142. For optimization requirement see also Konrad Hesse's practical concordance in T. Marauhn and N. Puppel, Balancing Conflicting Human Rights: Konrad Hesse's notion of "*Praktische Kokordanz*" and the German Federal Constitutional Court, in Brems (ed.) *Conflicts between Fundamental Rights*, (Intersentia, 2008), 279–281.

91 R. Alexy, *A Theory of Constitutional Rights*, (Oxford, 2010) 50–54; R. Dworkin, *Taking Rights Seriously*, (Duckworth, 1977) 27.

The above-mentioned distinction is quite well established in the general framework of legal theory.[92] Both Dworkin and Alexy seem to have a similar basis for their distinction, even if Alexy's approach appears to be more formalistic. Rules are seen as clear statements of law, which must be applied as such, while principles allow more balancing and are more flexible.[93]

Principles differentiate from rules firstly in the manner in which officials take them into consideration.[94] Principle can be considered as legal principle, when officials like judges have to take it into account when relevant for the case. Although an official might be obliged to take a legal principle into a consideration, this does not necessarily mean that the principle will be applied in the case, or if applied, it can be overruled by other principle. Yet, if not applied, this cannot be considered as rendering the principle void and it might well be applied in the next case. This differs from the manner in which rules function, an all-or-nothing-fashion. The second distinctive feature follows from the first one; unlike rules, the principles have dimension. In this context, the dimension reflects the importance and the weight of the principle.[95]

Even if the different nature of rules and principles appears relatively easy to comprehend, it is not always obvious how to distinguish principles from rules. Principles cannot be identified, for example, solely based on the formulation.[96] There might even be similarities in the formulation of rules and principles and some scholars have specifically noted that such texts as fundamental rights in the Constitution or international human rights conventions contain both rule-like and principle-like norms.[97] Nevertheless, Dworkin argues that if one is familiar with the law and legal system, one should recognize principles and be able to separate them from rules.[98] It appears that if a rule is drawn very generally, it is more likely to act as a principle. Principles are typically quite general in their nature[99]. However, for the purposes of this thesis it is not necessary to draw clear guidelines on how to separate rules from principles. It is essential, however, to comprehend how these different elements of legal system serve their purposes. An interesting doctrine in

92 See for instance R. Alexy, *A Theory of Constitutional Rights*, (Oxford, 2010) 44–48; R. Dworkin, *Taking Rights Seriously*, (Duckworth, 1977), 14–31; See also Zucca's approach, L. Zucca, *Constitutional Dilemmas*, (Oxford, 2007) 11.

93 Dworkin, *Taking Rights Seriously*, (Duckworth 1977) 14–31.

94 For more criteria for how to examine the difference between rules and principles, see H. Tolonen, "Rules, Principles and Goals: the interplay between law, morals and politics", in *Scandinavian studies in law* 35(1991), 269–293.

95 Dworkin, *Taking Rights Seriously*, (Duckworth 1977) 14–31.

96 Dworkin, *Taking Rights Seriously*, (Duckworth 1977) 24–28.

97 See for example M. Scheinin, *Ihmisoikeudet Suomen oikeudessa,* (Jyväskylä, 1991) 32–34. For the particular relationship between Constitutional rights and principles, see also See K. Tuori, *Critical Legal Postivism*, (Hants, 2002) 171–172.

98 Dworkin, *Taking Rights Seriously*, (Duckworth 1977) 22–31.

99 M. Scheinin, *Ihmisoikeudet Suomen oikeudessa,* (Jyväskylä, 1991) 34.

this respect is the thesis of rule fragments and so-called *rule influence* and *principle influence* which follows from rule fragments. This doctrine underlines that a rule is not necessarily a singular provision but might be formed from different fragments. It follows that certain provisions in an international human rights Convention, for example, are not necessarily direct rules, but these provisions might have *rule influence* in certain circumstances. This signifies that these provisions are applied as rules together with other elements of the legal order.[100] *Principle influence* on the other hand would lead to a balancing of different elements.[101] It was established that rules can be composed of different fragments, but in the case of principles this is even more clear. Dworkin attacked positivists' theories precisely by arguing that unwritten elements of law, such as principles, do exist.[102] In Tuori's theory of the deep structure of law, principles[103] are drawn from the underlying layers of law. Tuori sees that legal order is formed from several layers of law. On the surface level, there is, for example, current legislation and norms. The deeper levels of law consist of tacit knowledge of the lawyers. The deeper levels are the most stable levels of law.[104] As principles are not necessarily concretely formulated, they must be sought from the deep structure of the jurisprudence.

It was established that the formulation, as such, does not reveal principles, nor distinguish them from rules. Instead the capability to identify principles draws on expert knowledge of the legal system. Here Dworkin offers institutional support as a tool for perceiving principles.[105] Although this gives us some guidance on how to recognize a principle, it does not give a precise formula for reaching the right answer. Such examples of institutional support as *travaux préparatoires* or established social practice are given in the legal literature.[106] However, there is no unequivocal answer to, for example, which institutional acts should have references to the principle. Furthermore, there is no simple or clearly direct relation between the institutional acts and the principles they support. This is also the reason why institutional support cannot be considered as the rule of recognition[107] for principles, argues Dworkin.[108]

100 For rule-like effect of the hard core see T. Ojanen, "Making the essence of fundamental rights real: the Court of Justice of the European Union clarifies the structure of fundamental rights under the Charter" in *European Constitutional Law Review* 2 (2016).

101 See M. Scheinin, *Ihmisoikeudet Suomen oikeudessa,* (Jyväskylä, 1991) 31–38.

102 For common grounds of law, R. Dworkin, *Law's Empire*, (Oxford, 1998) 44.

103 Tuori distinguishes two types of principles. First, principles as legal norms, which exist on the surface level of law. Second, principles as sources of law, these principles must be derived from the deeper level of law. See K. Tuori, *Critical Legal Postivism*, (Hants, 2002) 179. The focus in this study is in the latter.

104 K. Tuori, *Critical Legal Positivism*, (Hants, 2002) 147–196.

105 Dworkin, *Taking Rights Seriously*, (Duckworth 1977) 39–45, 64–68.

106 H. Tolonen, "Rules, Principles and Goals: the interplay between law, morals and politics", in *Scandinavian studies in law* 35(1991), 276.

107 For rule of recognition see H.L.A Hart, *Concept of Law*, (Oxford, 1961) 72–107.

108 R. Dworkin, *Taking Rights Seriously*, (Duckworth 1977) 39–45.

Before examining the existence of institutional support, substantive significance reveals whether the legal instrument at stake is actually a principle.[109]

As a concluding remark, it could be noted that even if the different nature of rules and principles seems quite clear, it is far from clear how to draw clear lines between them. In the end, the core question seems to culminate in the validity of the weaker element of law. Furthermore, even if the concepts of rule influence and principle influence will not be adopted in this thesis, this is mostly for the sake of clarity of the text, and the underlying idea of these concepts is accepted. This doctrine specifies the difference at stake and it would indeed be more accurate to talk about principle influence instead of simply principles in this thesis as well.

2.2 RIGHTS

When Dworkin's or Alexy's principles collide, the actual collision takes place on the surface level of law in the form of colliding rights. Principles can be seen as propositions which describe rights; "*arguments of principle are arguments intended to establish an individual right*"[110]. Principles are balanced on the basis of their dimension and courts often seek the balance between different rights through doctrines of proportionality.[111] When the relationship between principles and rights is seen in the Dworkinian way, it appears that the correct proportionality considerations are drawn from the dimensions of different principles.

Dworkin separates abstract rights from concrete rights and argues that this difference is crucial for all adequate theories of rights. Following from the difference between abstract and concrete rights, the principles establishing these rights can also be characterized either abstract or concrete. Abstract rights are general political aims, aiming at collective good. While generality can be considered characteristic for abstract rights, concrete rights are instead more definite and more precise. Furthermore, contrary to an abstract right, a concrete right is aimed at individual good. Abstract rights do not collide or carry different dimension of weight like concrete rights do. However, abstract rights are an important element of concrete rights as they support them, and, even more importantly, concrete rights are derived from abstract rights.[112] Because abstract rights never collide in the Dworkinian world,

109 H. Tolonen, "Rules, Principles and Goals: the interplay between law, morals and politics", in *Scandinavian studies in law* 35(1991), 275–277.

110 R. Dworkin, *Taking Rights Seriously,* (Duckworth 1977) 90–91.

111 P. Ducoulombier, Conflicts between Fundamental Rights and the European Court of Human Rights: An Overview, in Brems (ed.) *Conflicts between Fundamental Rights*, (Intersentia, 2008), 234.

112 R. Dworkin, *Taking Rights Seriously,* (London, 1977) 90–122.

it is the concrete rights which are either confirmed or denied in the so-called hard cases.[113]

The focus of this thesis is on colliding rights and as such, concrete rights are of primary interest here. However, when seeking the fair balance between two rights, it might require assessment of abstract rights to form a more comprehensive picture of the context. The final outcome of balancing might take place on the level of concrete rights, but it is essential even for Dworkin's Hercules[114] judge to take abstract rights duly into consideration.[115]

Thus, the objectives and aims of the legislation forming the basis for the rights examined in this thesis will be analyzed in the concluding chapter when the balance between the colliding principles will be sought.

Fundamental rights are often considered trumps. It follows that the trump would surmount other rights in a situation of conflict.[116] In Dworkinian theory, rights based on policies could never create a basis for trumps. This could be done only by rights based on principles and, as such, for individual rights.[117] When rights are considered trumps and prevail over other rights, the question of two fundamental rights colliding and how to solve such a collision arises. Thus, to identify a collision of rights, the colliding rights must be fundamental. It is of interest to note though, that in the recent literature, it has been proposed that fundamental rights should not automatically be considered superior to other interests and rights. This would be in particular the case when peripheral interests are at stake.[118] As earlier established, fundamental rights are often formulated in a very general manner. This leaves relatively wide discretion for judges to evaluate how wide the scope of each fundamental right actually is.[119]

3. CLASHING RIGHTS AND PRINCIPLES

The clash of rights might take several forms, but the collision is of most interest when two constitutional rights are clashing. This is for several reasons. Firstly, constitutions

113 R. Dworkin, *Taking Rights Seriously,* (London, 1977) 100–101.

114 Hercules is a superhuman lawyer, a judge who is able to solve all conflicts as they should be solved with his superhuman skills, see for example R. Dworkin, *Taking Rights Seriously*, (London, 1977) 105–106.

115 R. Dworkin, *Taking Rights Seriously*, (London, 2009) 116–117.

116 R. Dworkin, Rights as Trumps, in Waldron (ed.) *Theories of Rights*, (Oxford, 1984), 153–167.

117 See for example L. Zucca, *Constitutional Dilemmas, conflicts of fundamental legal rights in Europe and the USA*, (Oxford, 2007) 50–51.

118 J.H. Gerards, Fundamental rights and other interests: Should it really make a difference, in Brems (ed.) *Conflicts between Fundamental Rights*, (Intersentia, 2008), 686–690.

119 This has also caused some criticism that because judges are not chosen democratically, i.e. by vote, they should not create law. See E. Maes, Constitutional Democracy, Constitutional Interpretation and Conflicting Rights, in Brems (ed.) *Conflicts between Fundamental Rights*, (Intersentia, 2008), 70.

hardly ever set one fundamental right above other fundamental rights.[120] Even if fundamental rights can be considered absolute or qualified based on their nature, this distinction does not necessarily dictate the outcome of the conflict between such rights.[121] Like Ojanen underlines, the inviolable core of the right does exist despite of the nature of the fundamental right.[122] Secondly, fundamental rights are often defined in a very general manner. When a legislator regulates fundamental issues, the result is likely to be a set of very general propositions. These propositions should maintain their effect and weight even when circumstances change.[123] This leaves a wide scope for collision, which might take place on a level of rules.

For a comprehensive picture of clashing rights and underlying principles, they should be mirrored against clashing rules. As Zucca notes, both Alexy and Dworkin see the conflict of rules very much alike. When rules are conflicting, only one of them becomes applicable rendering the other one void.[124] These conflicts could be solved for instance based on principles like *lex specialis* or *lex posterior* i.e. constructions of jurisprudence familiar to most lawyers. So, Dworkin and Alexy have a similar approach regarding clashing rules that the collision can be solved in a very clear-cut manner; the rule is either applicable or it is not. It also appears that once the clash of rules has been solved, the same pattern would apply in subsequent cases.[125] Thus, when assessing the conflict between rules, consistency and foreseeability play an important role.

Besides some relatively easily applied principles like *lex specialis* which give guidance on how to solve the situations of colliding rules, Dworkin draws the answer for solving the case of clashing rules from the underlying principles supporting the rules.[126] Similarly Alexy sets weight on balancing principles.[127] Alexy has adopted a very structural approach for balancing and underlines that "*the key question is [...] under what conditions does which principle take precedence over the other*".[128] Although this might seem to blur the lines between rules and principles,

120 E. Maes, Constitutional Democracy, Constitutional Interpretation and Conflicting Rights, in Brems (ed.) *Conflicts between Fundamental Rights*, (Intersentia, 2008), 69–71.

121 ECtHR Grand Chamber, 8 July 1999, Sürek and Ödzemir v Turkey. See also P. Ducoulombier, Conflicts between Fundamental Rights and the European Court of Human Rights: An Overview, in Brems (ed.) *Conflicts between Fundamental Rights*, (Intersentia, 2008), 238.

122 T. Ojanen, "Making the essence of fundamental rights real: the Court of Justice of the European Union clarifies the structure of fundamental rights under the Charter" in *European Constitutional Law Review* 2 (2016), 326.

123 E. Maes, Constitutional Democracy, Constitutional Interpretation and Conflicting Rights, in Brems (ed.) *Conflicts between Fundamental Rights*, (Intersentia, 2008), 69–71.

124 L. Zucca, *Constitutional Dilemmas*, (Oxford, 2007) 11; R. Alexy, *A Theory of Constitutional Rights*, (Oxford, 2010) 50–54; R. Dworkin, *Taking Rights Seriously*, (Duckworth, 1977) 27.

125 Ibid.

126 R.Dworkin, *Taking Rights Seriously*, (Duckworth 1977) 14–31

127 R. Alexy, *A Theory of Constitutional Rights*, (Oxford, 2010) 50–54.

128 Ibid.

the distinctive feature still remains; the non-applicable rule becomes void while the weaker principle does not vanish.

The core difference between clashing principles and clashing rules draws from the weight or dimension that the principles carry. As previously noted, dimension is a characteristic feature of principles and the disjunctive factor vis-à-vis rules. The dimension of principle is weighted in a situation where principles clash. Consequently, unlike a rule, a principle does not become void when colliding with another principle. Weighting the dimension of the principle might seem to lead to case-by-case evaluation when solving hard cases by drawing an answer from the deeper level of law, however, both Alexy and Dworkin deny that the outcome would be somehow arbitrary or irrational. Dworkin relies on the "one-right-answer" thesis while Alexy's approach is more structured and underlines the circumstances of the case.[129]

Even if Dworkin sees principles leaving a margin for finding the correct answer in their application, he still presumes that the correct answer exists. Once the judge has found the right answer, he or she is bound by it. Sometimes, it might happen, however, that a single judge makes a mistake and comes up with wrong solution.[130] Dworkin underlines that judges are not arbitrarily coming up with answers to what law is in the absence of law, but once they have formulated what the law actually is, they follow the law in their decision. Therefore, it is not a question for political discretion.[131]

Alexy sees that balancing might lead to different outcomes on a case-by-case basis, but underlines that, regardless, balancing is a rational process.[132] For balancing to be rational, it is essential, however, that the statements leading to a preferential statement are rationally defined.[133] Alexy argues that "*the circumstances under which one principle takes precedence over another constitute the conditions of a rule which has the same legal consequences as the principle taking precedence*".[134] According to Alexy, these statements leading to a preferential statement include "*the intention of the constitution makers, the negative consequences of an alternative statement of preference, doctrinal consensus and earlier decisions*".[135] It can be

129 See for example R. Dworkin, *Matter of Principle*, (London, 1985) 119–145; R. Alexy, *A Theory of Constitutional Rights*, (Oxford, 2010) 54, 100–107.

130 Ibid.

131 Ibid.

132 R. Alexy, *A Theory of Constitutional Rights*, (Oxford, 2010) 100–101.

133 R. Alexy, *A Theory of Constitutional Rights*, (Oxford, 2010) 101.

134 R. Alexy, *A Theory of Constitutional Rights*, (Oxford, 2010) 54.

135 R. Alexy, *A Theory of Constitutional Rights*, (Oxford, 2010) 100–101; K. Hesse, *Grundzüge des Verfaussungsrechts der Bundesrepublik Deutschland*, (Heidelberg, 1990) 142. For the contextual-based assessment and circumstances, see also Konrad Hesse's *practical concordance* in T. Marauhn and N.Puppel, Balancing Conflicting Human Rights: Konrad Hesse's notion of "*Praktische Kokordanz*" and the German Federal Constitutional Court, in Brems (ed.) *Conflicts between Fundamental Rights*, (Intersentia, 2008), 280.

argued that Alexy's circumstances are approaching Dworkin's institutional support to certain extent.[136] Thus the assessment of the dimension of principles can be drawn from a very similar basis on Alexy's and Dworkin's terms.

Alexy has formulated a "Law of Balancing", which he sees as an answer to a question of what should be rationally justified. According to the Law of Balancing "*the greater the degree of non-satisfaction of, or detriment to, one principle, the greater must be the importance of satisfying the other*".[137] Some authors have criticized courts' wide margin of appreciation and balancing and suggested that the use of this margin should be minimalized and based on strict criteria. The criteria suggested were based on questions of *what, who, how* and *why*, and it was suggested that applying these criteria could lead to a hierarchical order between different rights.[138] However, it seems like these criteria could be rendered back to Alexy's circumstances, which dictate the conditions for balancing. To suggest that this would lead to a hierarchical order between rights would seem rather bold, and the underlying dilemma would mostly seem to relate to the definition of the hierarchy itself.

Hesse's "practical concordance" is also of particular interest when it comes to balancing. First, and very much in line with Alexy, Hesse sees that deriving from the constitution's consistency, optimization must be applied.[139] Secondly, and still in line with Alexy, Hesse sees that optimization must take place in specific circumstances. Hesse also underlines that limitations may not exceed what is necessary to attain the aim of the limitation. According to Hesse "*conflicting rights and interest must be subject to limitations, so that each one attains its optimal effect. Consequently, limitations have to be proportionate in the light of specific circumstances. They must not be broader than required to establish concordance of conflicting constitutional values*".[140] This very much concretizes the content of the necessity element established by Article 52 of the Charter.

Some scholars have opposed the idea of rules being either applicable or void. It has been suggested that "*it is clearly not the case that every time rules conflict, one is valid and other invalid. Sometimes one rule will be considered an exception to the other*".[141] This argument doesn't seem to hold. When applying a rule which

136 For institutional support, see for example Dworkin, *Taking Rights Seriously*, (Duckworth 1977) 39–45.

137 R. Alexy, *A Theory of Constitutional Rights*, (Oxford, 2010) 102–107.

138 P. Ducoulombier, Conflicts between Fundamental Rights and the European Court of Human Rights: An Overview, in Brems (ed.) *Conflicts between Fundamental Rights*, (Intersentia, 2008), 238–247.

139 K. Hesse, *Grundzüge des Verfaussungsrechts der Bundesrepublik Deutschland*, (Heidelberg, 1990) 142; T.Marauhn and N.Puppel, Balancing Conflicting Human Rights: Konrad Hesse's notion of "*Praktische Kokordanz*" and the German Federal Constitutional Court, in Brems (ed.) *Conflicts between Fundamental Rights*, (Intersentia, 2008), 279–281.

140 Ibid.

141 L.Zucca, *Constitutional Dilemmas, conflicts of fundamental legal rights in Europe and the USA*, (Oxford, 2007) 11–12.

contains an exception, the judge is still applying a certain rule and bound by it. He or she has some margin of discretion when deciding whether the exception is applicable in the said case. Regardless of the outcome of his or her decision, the said rule would not become void, because the exception is part of the rule. The exception would simply be either applicable or not in the said case.[142] However, when a margin of discretion has been used in order to decide whether an exception becomes applicable, the underlying principles of the different rights might need to be balanced.

Furthermore, Zucca counters strongly Dworkin's presumption of the existence of one right answer in balancing principles. He argues that if this was accepted, there would not be any genuine conflicts of fundamental rights.[143] The "one right answer" thesis does seem to imply the existence of a harmonious universe of rights. However, conflicts between rights do exist when two equally important fundamental rights are at stake and the case cannot be solved without one interfering with the essence of the other. Before coming to this conclusion, a serious attempt to reconcile the rights should be made. The conclusion that a real conflict of rights exists should not be drawn too hastily. As Zucca underlines, it is important to distinguish genuine conflicts from the spurious ones and this narrows down the scope of genuine constitutional conflicts. Once the spurious conflicts have been separated from the genuine ones, the conflicts solved by rational arguments must also be distinguished from the genuine conflicts.[144]

3.1 TOTAL AND PARTIAL CONFLICTS

When narrowing down the scope of genuine constitutional conflicts, total conflicts can be distinguished from partial ones.[145] Based on this fundamental distinction, Zucca divides conflicts into four different lots. Firstly, conflicts can be total and arise in so-called intra-relations situations. When this is the case, there is the same right at stake, but two different right-holders. Realizing the right of one holder will inevitably render the right of the other holder void. Zucca uses the separation of conjoined twins as an example. There are also intra-rights conflicts that are partial. As in the previous case, there are two right-holders and they are sharing an interest in the same right. However, in this case, the problem can be solved without

142 Both Alexy and Dworkin do recognize the existence of exceptions. For Dworkin, see for example Dworkin, *Taking Rights Seriously*, (Duckworth 1977), 24–27.

143 L.Zucca, *Constitutional Dilemmas, conflicts of fundamental legal rights in Europe and the USA*, (Oxford, 2007) 11–12.

144 L. Zucca, Conflicts of Fundamental Rights as Constitutional Dilemmas, in Brems (ed.) *Conflicts between Fundamental Rights*, (Intersentia, 2008), 3–126.

145 H.Kelsen, *General Theory of Norms*, (Oxford, 1991) 123–127.

interfering with the core of that right. Here the given example is two different groups wanting to demonstrate at the same time in the same place of the city and reconciling this dilemma requires some logistics, but the core of the right would still remain untouchable.[146]

Secondly, total and partial conflicts can arise in inter-rights relations according to Zucca. In these cases, two different rights are colliding, both having the equal status of fundamental right. As an example of total conflict in inter-rights relations, Zucca looks at assisted suicide. It can be argued that decisional privacy and right to life cannot be realized simultaneously. Regarding partial inter-rights conflicts, the conflict between the right to free speech and informational privacy is given as an example. When this type of conflict occurs, it can be solved by case-by-case regulation.[147] The focus in this thesis is on inter-rights relations. The aim is to find a solution for how to execute one's right to the protection of personal data simultaneously with another person's right of access to documents without violating the essence of the said rights.

While partial conflicts can be solved by balancing, Zucca sees that total conflicts cannot be solved at all; or more correctly, cannot be solved without setting one right aside. There are two main manners of balancing conflicting rights: structured balancing and loose balancing. For the purpose of this research, the former is of more interest. The characteristic features for structured balancing are the assessment of the scope of the rights and rights' strengths.[148] The assessment of the scope of the right requires formulation of the hard core of the said right. Ojanen notes the hard core of a fundamental right can generate a rule and as a consequence require an either-or application.[149]

Furthermore, Zucca argues that balancing is often used to explain the conflicts away. He sees that, instead, the genuine conflicts should be recognized and dealt with.[150] I agree to some extent. For example, defining the scope of the right very narrowly can create an illusion of harmonious coexistence of different rights; the core of each right remains untouchable. However, this might not solve the conflicts on a practical level, only on a theoretical one. Regardless, the harmonious coexistence of

146 L. Zucca, Conflicts of Fundamental Rights as Constitutional Dilemmas, in Brems (ed.) *Conflicts between Fundamental Rights*, (Intersentia, 2008), 26–28.

147 L. Zucca, Conflicts of Fundamental Rights as Constitutional Dilemmas, in Brems (ed.) *Conflicts between Fundamental Rights*, (Intersentia, 2008), 26–28.

148 L. Zucca, Conflicts of Fundamental Rights as Constitutional Dilemmas, in Brems (ed.) *Conflicts between Fundamental Rights*, (Intersentia, 2008), 28–37.

149 See T. Ojanen, "Making the essence of fundamental rights real: the Court of Justice of the European Union clarifies the structure of fundamental rights under the Charter" in *European Constitutional Law Review* 2 (2016), 321–323.

150 L. Zucca, Conflicts of Fundamental Rights as Constitutional Dilemmas, in Brems (ed.) *Conflicts between Fundamental Rights*, (Intersentia, 2008), 28–37.

fundamental rights should be taken as premise[151] while at the same time recognizing the possibility of genuine conflicts of rights.

3.2 THE ESSENCE OF THE FUNDAMENTAL RIGHT

To distinguish genuine conflicts of principles from the partial ones, the essence or the hard core of the related rights must be identified. When a collision occurs in inter-rights relations, the conflict is genuine only when the hard core of the said rights cannot be put into effect simultaneously. The question of what constitutes the hard core of the rights which are in focus in this research, i.e. the right to protection of personal data and the right to public access to documents will be examined in the concluding chapter.

3.2.1 RELATIVE AND ABSOLUTE APPROACH

Alexy distinguishes the absolute and relative approach when defining the inalienable core.[152] The relative approach leaves more margin for discretion. With the relative approach, the hard core, the essence of the right, can be identified after it is clear what is left of the said principle when balanced with other principle. The hard core must remain inviolable, but this approach allows broad margin for balancing as far as the proportionality principle is taken appropriately into account.[153] It seems that a genuine collision of rights could never occur when this doctrine is applied.

When the absolute approach is adopted, the founding idea is that certain conditions create an essence of the right, which cannot be violated. Thus, certain conditions would set the circumstances where the essence of the right would be preserved.[154] Alexy sees that "*the absolute theory goes too far in saying that there are legal positions such that no possible legal reason can restrict them*".[155] This observation seems to underline the need to take the circumstances of the case duly into account. Alexy also notes that "*the extent of 'absolute' protection depends*

151 Also Zucca underlines that the existence of genuine conflicts of rights is rare, see for example Conflicts of Fundamental Rights as Constitutional Dilemmas, in Brems (ed.) *Conflicts between Fundamental Rights*, (Intersentia, 2008), 19–37.

152 R. Alexy, *A Theory of Constitutional Rights*, (Oxford, 2010) 192–196; For absolute and relative approaches, see also G. Van Der Schyff, Cutting to the Core of Confidential Rights: The Question of inalienable Cores in Comparative Perspective, in Brems (ed.) *Conflicts between Fundamental Rights*, (Intersentia, 2008), 133–135.

153 Ibid.

154 Ibid.

155 R. Alexy, *A Theory of Constitutional Rights*, (Oxford, 2010) 195.

on the balance of principles".[156] This leads to a context-based assessment, where the rights, which are balanced, might lead to a different definition of the essence depending on the balanced principles.[157]

Thus, both the relative and absolute approach allow taking into consideration the circumstances of the case, but the relative approach would define the essence of the right based on what is left after the balancing of the principles, while the absolute approach sets the conditions under which the essence of the right cannot be breached. This research examines the relationship between data protection and public access to documents and therefore the circumstances of the examined case are settled to certain extent. Thus, the differentiating circumstances will be examined in the concluding chapter only to provide an exhaustive picture of the context in which these rights are interacting.

3.2.2 IDENTIFYING THE INVIOLABLE CORE

In line with Alexy's doctrine, Ojanen stresses that when identifying the hard core of the fundamental right, the normative elements of the right together with particular characteristics of each case must be recognized appropriately. Ojanen distinguishes three more general elements for the assessment of the essence of the right. These elements relate to textual formulation, the amount of the elements forming the hard core and the nature of rights.[158]

The first element of the essence of the right is ultimately based on the more general remark of the normative elements of the fundamental right and specific characteristics of the case. Being faithful to Alexy, Ojanen namely stresses that the essence of the fundamental right cannot be identified solely based on the textual formulation of the right. Instead the assessment requires appropriate evaluation of the context.[159] This approach reflects Alexy's doctrine, which underlines the circumstances of the case.[160] Thus the essence of the right cannot be identified in a vacuum. Instead, it requires balancing of the underlying principles.

Ojanen's second general remark relates to the hard core itself. The hard core does not necessarily constitute of only one element but may contain several different

156 Ibid.

157 See also T. Ojanen, "Making the essence of fundamental rights real: the Court of Justice of the European Union clarifies the structure of fundamental rights under the Charter" in *European Constitutional Law Review* 2 (2016), 321–323.

158 See T. Ojanen, "Making the essence of fundamental rights real: the Court of Justice of the European Union clarifies the structure of fundamental rights under the Charter" in *European Constitutional Law Review* 2 (2016), 321–323.

159 Ibid.

160 R. Alexy, *A Theory of Constitutional Rights*, (Oxford, 2010) 54, 100–107.

elements. In other words, several elements might form the hard core of a right. These elements would then generate the rule-like effect.[161] As a third element, Ojanen brings up that rights other than absolute rights have a hard core. This doctrine separates the inviolable core of the right from the other elements of the right. It could be said that even non-absolute rights contain the non-violable hard core, which is absolute.[162]

The "one-right-answer" thesis by Dworkin breaches the elements of natural law.[163] Alexy and Ojanen in turn underline the circumstances of the case and contextual, case-to-case interpretation. These scholars, however, seek the answer from the deeper levels of law. While the contextual-based interpretation might approximate Hart's positivist approach which underlines discretion, it does not exclude the Dworkinian "one-right-answer"thesis.[164] The doctrine of similar circumstances leading to similar outcomes allows the essence of the right to remain the same. Despite the intriguing dimensions of this question, it will not be further elaborated on in this thesis. For the purposes of this research it suffices to note that the hard cores of rights are seen as absolute and, as such, having the rule-like effect. Furthermore, in identifying the hard core of the right, the answer must be sought from the deeper levels of law and this calls for the balancing of principles in Alexy's sense.

3.3 SOME CRITICS OF BALANCING OF RIGHTS

It is quite common understanding that when two fundamental rights must be applied simultaneously, it often requires balancing. Some scholars have, however, criticized balancing and considered it an incomplete method. Reasons for such criticism vary. Some have claimed that balancing, which the court's decisions are based on, is quite opaque. Furthermore, it has been claimed that balancing is irrational and arbitrary. Also, balancing has been claimed too narrow when excluding collective goals and policies from the considerations.[165]

161 See T. Ojanen, "Making the essence of fundamental rights real: the Court of Justice of the European Union clarifies the structure of fundamental rights under the Charter" in *European Constitutional Law Review* 2 (2016), 321–323; see also for example M. Scheinin, *Ihmisoikeudet Suomen oikeudessa,* (Jyväskylä, 1991) 32.

162 See T. Ojanen, "Making the essence of fundamental rights real: the Court of Justice of the European Union clarifies the structure of fundamental rights under the Charter" in *European Constitutional Law Review* 2 (2016), 321–323.

163 See for example R. Dworkin, No Right Answer?, in P.M.S. Hacker & J. Raz (ed.) *Law, Morality, and Society: Essays in Honor of HLA Hart*, (Oxford 1977), 58–84; R. Dworkin, *Taking Rights Seriously*, (Duckworth 1977) 14–31, 44, 159–60, 340–42, 334, 360; R. Dworkin, *Matter of Principle*, (London, 1985) 119–145.

164 For Hart's positivist approach, see H.L.A Hart, *Concept of Law*, (Oxford, 1961). For "one-right-answer" thesis, see R. Dworkin, No Right Answer?, in P.M.S. Hacker & J. Raz (ed.) *Law, Morality, and Society: Essays in Honor of HLA Hart*, (Oxford 1977), 58–84; R.Dworkin, *Taking Rights Seriously*, (Duckworth 1977) 14–31, 44, 159–60, 340–42, 334, 360; R. Dworkin, *Matter of Principle*, (London, 1985) 119–145.

165 See for example S. Greer, "'Balancing' and the European Court of Human Rights: a Contribution to the Habermas-Alexy debate" in *The Cambridge Law Journal* 63 (2004) 412–413.

These concerns are justified to a certain extent. However, Alexy's doctrine does seem to provide an answer to these concerns. Firstly, Alexy does not separate rights based on the differing aims. Therefore, both individual rights and collective rights are considered equal. Secondly, Alexy's balancing process is rational and logical. The circumstances of the case are the elements for measuring the dimensions of different principles. Similar circumstances would lead to similar outcomes.[166] Identifying Alexy's circumstances and formulating them in precise conditions leading to a certain outcome in similar cases would create a rational formulation for balancing in each case. For the third point of criticism, namely the lack of transparency in the decision-making process, identifying Alexy's circumstances would provide a tool for the court to formulate their reasoning in a more precise and, as such, also more transparent way.

4. DEMOCRACY

This section will briefly introduce the core components of democracy and also some of the key concepts related to democracy. While acknowledging how fascinating and multilayered the concept of democracy is, it is beyond the scope of this research to explore this concept thoroughly. However, a brief overview is provided to facilitate the further examination of the relationship between transparency, privacy and democracy at a later stage. As it will be argued later in this thesis, if transparency is not to be considered a fundamental right, it ought to be considered a right with equivalent importance. This argument draws from the relationship between public access to documents and democracy. In Nordic countries, public access to documents is seen as an essential component of democratic society, as the current Chancellor of Justice in Finland, Tuomas Pöysti, puts it, "*Rational political, ethical and legal debate requires reliable and publicly available information. Thereby access to information and participation in public discourse are essential democratic values*".[167]

Some scholars consider that democracy itself is a right and that there is a general right to democracy.[168] This right would belong to people[169] and in line with Dworkin's thesis would therefore be based on policies. As such, it would always be overrun by principles, which are aimed at individual good.[170] However, without getting

166 R. Alexy, *A Theory of Constitutional Rights*, (Oxford, 2010) 54, 100–107.

167 T. Pöysti, Scandinavian Idea of Informational Fairness in Law – Encounters of Scandinavian and European Freedom of Information and Copyright Law, in *Scandinavian Studies in Law* 65(2007), 225.

168 E. Maes, Constitutional Democracy, Constitutional Interpretation and Conflicting Rights, in Brems (ed.) *Conflicts between Fundamental Rights*, (Intersentia, 2008), 70.

169 Ibid.

170 R. Dworkin, *Taking Rights Seriously*, (London, 2009) 90–100.

deeper in the rights discussion at this point and while setting Alexy's differing approach of collective and individual rights aside, democracy is not considered a right in the sense that rights are defined in this thesis.[171] However, democracy is an essential building block when balancing fundamental rights. This is because limiting fundamental rights is acceptable to a certain extent, when this is necessary in a democratic society.[172]

The roots of democracy are deep in Western society. The origins of democracy are often associated with Ancient Greece, but according to some, the first versions of democracy can actually be traced all the way to the Mycenaeans.[173] Democracy is said to be the first form of governance by the people. In other words, people were not governed by nature or by one sole authority, such as a king. Even if the existence of deities was apparent in the democracy of Ancient Greece, the core idea was that humans could actually rule and govern themselves. And when doing this, they were equals. Equality in this context meant that the ancient Greeks had equal rights before the law and they had equal rights to speak.[174] The democracy in Ancient Greece was a very pure form of direct democracy and the idea of representative democracy has its roots in a much later era, in the 16th to 18th centuries.[175] Here, attention should be drawn to the core element of democracy. That is equality between people when governing themselves. For this to happen, it is naturally essential that those participating in governing are provided with equal information. Quite interestingly, it appears that public record-keeping existed already in Athens and, even if there was no single constitution, the laws were displayed publicly[176]. Thus, it could be argued that access to information already played a role in the first forms of democracy.

4.1 KEY ELEMENTS OF DEMOCRACY

The concept of democracy can be approached from different angles. One way to address democracy is to examine the conditions which a sovereign state should meet to be considered a democracy. Three elements defined by the late professor Thomas Franck can be used as a starting point in this assessment. Franck argues that essential elements for democracy are self-determination, freedom of expression

171 Democracy is not defined as a right for example in the European Convention on Human Rights or in the Charter of Fundamental Rights of European Union.

172 See for example Article 52(1) in the Charter of Fundamental Rights of European Union or Articles 8(2) and 10(2) of the European Convention on Human Rights.

173 For more, see J. Keane, *The Life and Death of Democracy*, (London, 2009) xi.

174 Naturally, this did not apply to slaves or women at the time.

175 J. Keane, *The Life and Death of Democracy*, (London, 2009) xiv, xviii, 38.

176 J. Keane, *The Life and Death of Democracy*, (London, 2009) 37.

and electoral rights.[177] While the three aspects of democracy defined by Franck can without a doubt be considered main elements of democracy, they alone might not be enough to build a well-functioning democracy.

Sabino Cassese[178] has elaborated Franck's three elements into more detailed requirements. Cassese first underlines the importance of free elections and in this context he also stresses the significance of a multi-party system. Besides these two points, he also underlines the importance of separation of powers. As a second element, he brings up freedom of information and public access to official documents. Lastly, he returns to the core values of democracy in Ancient Greece and lists equality as one of the components on which democracy is built. These two sets of criteria are rather compact and partly overlapping. They seem to complete each other nicely. It is also possible to define the core elements of democracy in a much wider way. For example, the United Nations Security Council has taken a rather wide approach to democracy. This approach has taken place in the context of United States' invasion of Iraq. In several resolutions, the Security Council concluded that the following elements are part of democracy: right to determine own political future and control own natural resources, right to independence, sovereignty, unity and territorial integrity; the rule of law, and democracy, including free and fair elections and an internationally recognized, representative government of Iraq.[179] As can be seen, these elements defining democracy are quite comprehensive.

It is beyond the scope of this thesis to draw conclusions about the precise elements on which democracy is built. While all of the aforementioned criteria can be distinguished, Dworkin draws the punch line of effective democracy quite nicely, when elaborating the core requirements for achieving a democratic society. As he puts it, "*people do not govern themselves if they are deprived of the information they need to make an intelligent decision or cheated of the criticism they need in order effectively to judge the record of their officials*".[180] While recognizing the people as sovereign regardless of the actual form the democracy, Dworkin places heavy emphasis on gaining access to information in order to govern oneself.[181] Putting this in the context of Franck's and Cassese's criteria, it can be concluded that free elections and other political institutions related to them, are unquestionably the core elements of democracy. However, they would have little value if people

177 Franck T.M., "The Emerging Right to Democratic Governance", in *The American Journal of International Law* 86 (1992), 52.

178 Seminar lecture by Sabino Cassese, May 2011, London. Sabino Cassese is a former judge in a constitutional court in Italy and professor of Public Law at the University of Rome.

179 Security Council Resolutions 1511(2003), p.1 (no 2), 1546(2004), para 3 and 1637(2005), p. 1 (no 4); Security Council Resolution 1546(2004), p. 1 (no 3) and Resolution 1619 and 1637(2005); Security Council Resolution 1546(2004), p. 1 (no 10); Security Council Resolution 1483(2003), para 22.

180 For the particular relationship between Constitutional rights and principles, see also See K. Tuori, *Critical Legal Postivism*, (Hants, 2002) 171–172.

181 R. Dworkin, *Is Democracy Possible here?*, (Princeton, 2006) 154.

were deprived of accurate information. Furthermore, people could not be equal if not provided with equal information. Even if Dworkin draws his conclusion when elaborating on the importance of freedom of speech in a democratic society, this doctrine can be extended to the freedom of information and access to documents. Freedom of speech would have little use without accurate information.

4.2 DIFFERENT FORMS OF DEMOCRACY

Even if several different types of democracy can be distinguished, they all share the core idea of the people as sovereign and citizens' equal rights to participate in the decision-making process.[182] The difference in different types of democracy comes mainly from the extent to which, and manner in which, the people are able materialize their rights.

The purest form of direct democracy[183] probably existed in Ancient Greece.[184] While in Greece all citizens participated in the decision-making, direct democracy exists today mainly as a component in society, which is mainly based on representative democracy. For example, in Switzerland citizens are able to vote when the proposals concern constitutional amendments and the outcome of the referendum binds the government.[185] Also in many of the EU Member States referendums took place before the ratification of the Lisbon Treaty.[186] In a representative democracy, the members of the parliament get the justification for decision-making from the sovereign, i.e. the people, which has authorized parliament through free elections.[187] Another form of democracy is participatory democracy, in which citizens are able participate in the decision-making process in one form or another.[188] Examples of such participation

182 G. Smith, *Democratic Innovations*, (Cambridge, 2009) 22.

183 In some contexts direct democracy is used as a partner to indirect democracy in the sense that in direct democracy refers to institutions where the representatives have been elected with direct vote and indirect democracy refers to the institutions where the representatives have been chosen from a lot, which has been elected with a direct vote in the original country. For that, see A. Rosas & L. Armati, *EU Constitutional Law*, (Oxford, 2010) 112–115.

184 See for example E. Maes, Constitutional Democracy, Constitutional Interpretation and Conflicting Rights, in Brems (ed.) *Conflicts between Fundamental Rights*, (Intersentia, 2008), 71–72.

185 G. Smith, *Democratic Innovations*, (Cambridge, 2009) 111–113.

186 For more about direct democracy and the relevance of access to correct information in the direct democracy, see for example A.Lupia and J.G.Matsusaka, "Direct Democracy: New Approaches to Old Questions" in *The Annual Review of the Political Science* 7 (2004), 463–482.

187 See for example P. Avril, "The democratic institutions of the European countries", in Rieu & Duprat (ed.) *European democratic culture*, (London, 1995), 215–216.

188 For participatory governance, see also E. Korkea-aho & P. Leino, "Who owns the information held by EU agencies? Weed killers, commercially sensitive information and transparent and participatory governance" in *Common Market Law Review* 4 (2017), 1059–1092.

are the right to complain to the European Ombudsman and open initiatives to the European Commission.[189]

Features of both above-mentioned types of democracy are combined in the concept of deliberative democracy. While representative democracy gets its authorization from free elections and voting, deliberative democracy draws it from citizens' participation in the process of drafting the law through free, public debate.[190] It has been noted that possibility to participate in public debate does not yet imply that the views expressed would dictate the outcome of the law drafting process.[191] [192] Although this is naturally correct, the benefits of public debate are still obvious. Even if the outcome might differ from some of the views expressed during the process, these views cannot simply be disregarded. To justify the final outcome, dissenting opinions should be taken into consideration and "reasoned away". Even if it might be too much to ask to provide reasoning that would convince the opposite side, they should at least convince a "reasonable man". This obviously contributes to the final outcome of law drafting processes and should lead to better law-making.

Graham Smith points to the deficit of citizens' control over the decision-making process as a common problem for all of the variations of democracy.[193] He suggests that transparency could be part of the solution. He separates transparency in relation to participants and transparency in relation to wider public.[194] For the purposes of this research, the latter is of more interest. The sovereign – the people in this case – should have the right to know, regardless of the adopted form of democracy.[195]

189 A. Rosas & L.Armati, *EU Constitutional Law*, (Oxford, 2010) 124: Article 24 of the Treaty on the Functioning of the European Union.

190 A. Ieven, Privacy Rights in Conflict: In Search of the Theoretical Framework behind the European Court of Human Rights' balancing of private life against other rights, in E. Brems (ed.) *Conflicts between Fundamental Rights*, (Intersentia, 2008), 61–63; see also See E. Maes, Constitutional Democracy, Constitutional Interpretation and Conflicting Rights, in Brems (ed.) *Conflicts between Fundamental Rights*, (Intersentia, 2008), 74–79.

191 A. Ieven, Privacy Rights in Conflict: In Search of the Theoretical Framework behind the European Court of Human Rights' balancing of private life against other rights, in E. Brems (ed.) *Conflicts between Fundamental Rights*, (Intersentia, 2008), 64.

192 For an analysis of current topical issues in light of deliberative democracy see S. Ecran, "Democratizing Identity Politics: a Deliberative approach to the Politics of Recognition", in D. Gozdecka and M.Kmak (ed.) *Europe at the Edge of Pluralism*, (Intersentia, 2015), 13–26.

193 G. Smith, *Democratic Innovations*, (Cambridge, 2009) 22.

194 G. Smith, *Democratic Innovations*, (Cambridge, 2009) 25–26.

195 For the use of term *right to know*, see for example A.Saarenpää, "Legal Infomatics Today – The View from the University of Lapland", in A. Saarenpää & K. Sztobryn (eds.) *Lawyers in the Media Society, The Leal Challenges of the Media Society*, (Lapin yliopisto, 2016), 11.

4.3 THE DEFINITION OF DEMOCRACY IN THE PRACTICE OF THE EUROPEAN COURT OF HUMAN RIGHTS

The European Court of Human Rights has referred to democratic society in several cases relating to the right to freedom of speech.[196] Nevertheless, the Court of Human Rights has been criticized for not having given a clear and unambiguous definition of democracy.[197] It has been claimed that the Court of Human Rights has concentrated on the functioning of democratic institutions and the processes related to them rather than giving guidelines on how to interpret the concept of democracy itself. Moreover, it has been considered problematic that when the Court of Human Rights refers to the characteristic values[198] of democracy in its case-law, these values have not been elaborated further.[199]

Besides the above-mentioned criticism, the Court of Human Rights has been urged to take a clearer position regarding the relationship between democracy and human rights. It has been noted that democracy and human rights do not always go hand in hand. It often appears that democratic decisions are majority decisions and therefore could also discriminate against minorities.[200] However they also share the underlying value of human autonomy.[201]

Democracy might not be clearly defined by the ECtHR and there might be some deficits in the formulation of the relationship between human rights and democracy, however, in the big picture it does seem that human rights are protected by the Convention in the context of democratic society rather than the other way around.[202]

---

196 See for example ECtHR 24 June 2004, *Von Hannover v Germany* (2004–VI) and ECtHR 77 June 2017, *Satakunnan Markkinapörssi Oy and Satamedia Oy v Finland* (ECLI:CE:ECHR:2017:0627JUD000093113). For an analysis, see for example R. Gisbert, The Right to Freedom of expression in a democratic Society (Art. 20 ECHR), in Garcia Roca & Santolaya (ed.) *Europe of Rights: A Compendium of the European Convention of Human Rights*, (Leiden, 2012), 371–401.

197 A. Ieven, Privacy Rights in Conflict: In Search of the Theoretical Framework behind the European Court of Human Rights' balancing of private life against other rights, in E. Brems (ed.) *Conflicts between Fundamental Rights*, (Intersentia, 2008), 57.

198 Pluralism, tolerance, broadmindedness.

199 R. O'Connell, "Realising political equality: the European Court of Human Rights and positive obligations in a democracy", in *Northern Ireland Legal Quarterly* 3 (2010), 263–79.

200 For an analysis of hate speech and democracy in light of the case-law of the European Court of Human Rights, see J. Cernic, "Democracy as a Trump Card? Combating Hate Speech in Pluralistic Societies", in D. Gozdecka and M. Kmak (ed.) *Europe at the Edge of Pluralism*, (Intersentia, 2015), 163–175.

201 A. Ieven, Privacy Rights in Conflict: In Search of the Theoretical Framework behind the European Court of Human Rights' balancing of private life against other rights, in E. Brems (ed.), *Conflicts between Fundamental Rights* (Intersentia, 2008), 61.

202 S. Greer, "'Balancing' and the European Court of Human Rights: a Contribution to the Habermas-Alexy debate" in *The Cambridge Law Journal* 63 (2004) 416–417.

4.4 DEMOCRACY IN THE EU

Democracy is one of the founding values of the European Union and this is also clearly expressed in Article 2 of the TEU.[203] Despite this, the European Union has long been blamed for the deficit of democracy. These claims and the reasons provoking them have been vastly explored by various scholars and other stakeholders. For example, Rosas and Armati identify three different reasons causing these allegations. First, the EU as a whole is seen undemocratic, because it is run by non-elected officials.[204] Second, the European Parliament has been accused of having an undemocratic foundation. Third, the lack of transparency in Union decision-making is commonly raised as the main problem causing the accusations of the undemocratic Union. Both legislative and executive processes are seen opaque. As a more fundamental problem, Rosas and Armati identify the lack of a sense of community.[205] It is quite easy to concur with this; the lack of unity among the nations was quite apparent for example during the eurozone crisis.

The European Union has worked to respond to these allegations. The democratic foundations of the European Parliament have constantly been increased and the Parliament's role in the legislative process has been strengthened.[206] Also, starting from the Treaty of Maastricht, the role of transparency has gained more weight in the EU institutions decision-making.[207] At any rate, as Rosas and Armati note, the democratic nature of the Union must be placed in right context. The European Union is not a federal state and even less a national state. The discussion on the lack of democracy should therefore be put in this context.[208]

Thus, the settled theories and opinions on how democracy should work might not be directly applicable in the European Union. The unique nature of the Union might require new solutions. As an example, equality between the Union members might not be best achieved in a one-man-one-vote manner but might require some more sophisticated practices in order to accomplish the most democratic mode in which to function.

---

203 The Treaty on the European Union (OJ C 115, 9.5.2008, p. 13–45).

204 A. Rosas & L. Armati, *EU Constitutional Law*, (Oxford, 2010) 111–112.

205 A. Rosas & L. Armati, *EU Constitutional Law*, (Oxford, 2010) 111–112.

206 A. Rosas & L. Armati, *EU Constitutional Law*, (Oxford, 2010) 111–123.

207 See for example I. Harden, "The Revision of Regulation 1049/2001 on Public Access to Documents" in *European Public Law* 2 (2009), 239–240.

208 A. Rosas & L. Armati, *EU Constitutional Law*, (Oxford, 2010) 112.

CHAPTER II

AN OVERVIEW OF THE DEVELOPMENT OF TRANSPARENCY AND DATA PROTECTION REGIMES IN EUROPE

This chapter will focus on the development of the transparency and data protection regimes in Europe, starting with an overview from the very early stages of development. This overview should provide grounds for understanding how the Nordic approach on transparency has developed, and how different the development process of the two examined rights has been on the European scene. Yet, the progress of these concepts has led to the same culmination point in the recent breakthrough, giving recognition as a fundamental right to protection of personal data and the right of access to documents. This culmination point will be assessed in more detail later in the context of the said rights. This section will provide a more general picture of the developments.

In chronological order, this chapter will first focus on the development of the transparency regime and, more precisely, the right of access to documents. First, the background and the context in which the principle of public access was grown is examined. This is followed by an overview of the development of the legislative framework on access to documents in the European Union. Thereafter, its character as a fundamental right will be briefly covered. The second part of this section concentrates on developments regarding data protection. For a long time, it has been seen essentially as an element of privacy and it will be approached from this angle. Thus, the discussion will touch upon the developments of the protection of privacy, as such, but the emphasis will be on the evolution of the protection of one's personal data itself. Data protection rights are a more recent phenomenon than transparency. The need to protect personal data draws strongly from the progress which has taken place in automatic data processing. Its roots are approximately 60 years long.

The concluding part will focus on the most significant differences and similarities between the development of the two fundamental rights under examination; data protection and access to documents.

1. THE GENESIS OF THE RIGHT OF ACCESS TO DOCUMENTS AND ITS EMERGENCE IN THE EUROPEAN LEGAL FRAMEWORK

1.1 FIRST DEVELOPMENTS LEADING TOWARDS A RIGHT OF ACCESS TO DOCUMENTS

The history of the European transparency regime can be tracked down all the way to 18th century. In 1766, the first freedom of press law was adopted in Sweden. This law contained the fundamental principle of access to official documents.[209] It is considered the first law, which contained the general principle of access to documents in Europe and also more generally in the world.[210] The law was enacted as a constitutional law whereupon nearly all official documents became public. This made critical discussion of the legislation and policies adopted by the government possible. This was not the case with religion, which still remained under censorship.[211] The law contained, for example, provisions on access to documents relating to court proceedings. Furthermore, the law covered both documents received by the public authorities and documents processed by them. The documents covered by this law were accessible to the public and freely publishable, however, some exceptions to the general principle did exist already at this very early stage. Access to official documents was attained either by viewing and copying the document at the public authorities' premises orby receiving a duplicate of the document.[212]

The father of Swedish freedom of information law was Anders Chydenius, who is considered the father of the right of access to documents also in more general terms.[213] Anders Chydenius was a Swedo-Finn, liberal priest and politician. Chydenius saw that societal changes required the awareness of the wider public and freedom of press would provide the answer for this. Chydenius was a member of the Freedom of Press committee in the Swedish Parliament and even if the majority of the members of this committee were rather conservative, members treasuring the idea of freedom of press were able to prepare the proposal for the above-mentioned

209 P. Hyttinen, *Anders Chydenius, Defender of Freedom and Democracy*, (Kokkola, 1994) 34–35. See also J. Hirschfeldt, "Free access to public documents – a heritage from 1766", in A-S.Lind; J.Reichel & I.Österdahl (eds.), *Transparency in the Future – Swedish Openness 250 years* (Visby, 2017), 21–28.

210 A.Bohlin, *Offentlighets principen*, (Stockholm, 2001) 18–21; C. Malmström, "Sveriges agerande i Öppenhetsmål inför EG-domstolen – politik och juridik hand in hand" in *Europarättslig tidskrift*, 10 (2008), 11–20.

211 P. Hyttinen, *Anders Chydenius, Defender of Freedom and Democracy*, (Kokkola, 1994) 34–35.

212 A.Bohlin, *Offentlighets principen*, (Stockholm, 2001) 18–21.

213 C. Malmström, "Sveriges agerande i Öppenhetsmål inför EG-domstolen – politik och juridik hand in hand" in *Europarättslig tidskrift*, 10 (2008), 11–20.

law without heavy constraints. This was mainly due to the inactive participation of the more conservative members in committee meetings. The Freedom of Press committee submitted their final proposal to the Estates in the spring of 1766. The proposal included abolition of censorship with the exception of writings related to religion. Access to all official documents, as well as memorandums drafted in the parliamentary sessions and protocols from the session, was incorporated in the proposal.[214] Chydenius worked hard to push the law through the Parliament. In his autobiography Chydenius notes that he did not work for any other cause as hard as he did for the freedom of the press.[215] Chydenius also believes that the absence of certain members during the decision-making process were crucial for his law to pass in the Parliament. These members were rather conservative and would most likely have voted against the Freedom of Press Act.[216] Even though freedom of press law has been one of Chydenius' great achievements – and Chydenius himself considered it his most important achievement –, quite interestingly, he might be even better known as a defender of freedom of trade and industry.[217]

Chydenius treasured democracy, human rights and equality. Already, back in 1766, Chydenius stated that

> *"No proof should be necessary that a modicum of freedom for writing and printing is one of the strongest Pillars of support for free Government, for in the absence of such, the Estates would not dispose of sufficient knowledge to make good Laws, nor Practitioners of Law have control in their vocation, nor Subjects knowledge of the requirements laid down in Law, the limits of Authority and their own duties. Learning and good manners would be suppressed, coarseness*

214 P. Virrankoski, *Anders Chydenius, Demokratisk politiker I upplysningens tid*, (Jyväskylä, 1995) 86–93, 174–196.

215 E.G.Palmen, *Anders Chydenius*, (Helsingfors, 1903) 109–150; A.Chydenius, Antti Chydeniuksen omatekoinen elämänkerta, in Kare (ed.) *Anders Chydenius, Suuri Suomalainen valituskirjailija*, (Alea-Kirja, 1986), 434–438. To quote Chydenius,"*Ingenting arbetade jag vid denna riksdag så tränget uti som skrif- och tryckerifriheten. Nordencrantz'skrifter hade redan så öppnat mig ögonen, att jag ansåg den för ögonstenen i ett fritt rike.*" Furthermore, Chydenius noted that "*om skrif- och tryckfriheten blifver en frihetens grundpelare i alla regeringar, där den skyddas; on de flesta Sveriges olyckor i de nästförflutna tider leda sin upprinnelse ifrån mörker och villfarelse, så är det värdt för eftervärlden att känna de som tillfälligheter, hvarigenom den hos oss liksom genom ett lyckskott af försynenblifvit skänkt åt Svea innebyggare, - anekdoter, som annars aldrig kunde hinna i våra häfdatecknares händer*", E.G.Palmen, *Anders Chydenius*, (Helsingfors, 1903) 109–110.

216 Ibid.

217 P-L. Kastari, *Antti Chydenius ja painovapauden aate*, (Tampereen yliopisto, 1981) 1; L. Harmaja, *Antti Chydenius kansantaloudellisena kirjailijana*, (Helsinki, 1929); see also *The National Gain*" by Anders Chydenius, translated from the Swedish original published in 1765 with an introduction by Georg Schauman (London, 1931); C.Uhr, *Antti Chydenius 1729–1803, Adam Smithin Suomalainen edelläkävijä*, (Helsinki, 1965).

> *in thought, speech and customs would flourish, and a sinister gloom would within a few years darken our entire Sky of Freedom."*
>
> *Memorandum on the Freedom of the Press, 1765.*[218]

These words, expressed more than 250 years ago, show the triangle between freedom of press and transparency, good administration and democracy. Only freedom of press is directly mentioned in the text, but the idea of good administration together with democracy, are clearly visible in these lines. Regarding the explicitly-mentioned freedom of writing, the requirement of access to official documents is tacit, as access is a prerequisite for distribution of information.

The principle of access to documents has long traditions in Northern Europe. However, its emergence in other European countries has taken place only very recently. It seems that the real breakthrough took place only in the 1990s when transparency legislation was passed in the recently-born democracies in Eastern and Central European countries. The older and more mature democracies in Europe also adopted new legislation on transparency during this period.[219] This was more than 200 years after Chydenius had expressed the above ideas on the need for greater transparency.

1.2 LEGISLATIVE DEVELOPMENTS IN THE EU

The first step towards transparency regulation in the European Union was the adoption of the Declaration of the Treaty of Maastricht on the right of access to information. As it was still just a Declaration, it did indicate political willingness to move in that direction, but it was not legally binding. The legal basis for regulation regarding public access to documents was introduced by the Amsterdam Treaty in 1997. The new Article 255 EC[220] provided the right of access to documents to any citizen of the Union and any natural or legal person residing or having its registered office in a Member State. This was, however, subject to secondary legislation, which was to be adopted within two years after the Treaty entered into force.[221]

---

218 P. Hyttinen, *Anders Chydenius, Defender of Freedom and Democracy*, (Kokkola, 1994) 34–35. See also Anders Chydenius Foundation, What did Chydenius say about freedom of the press, available on the internet < www.chydenius.net/historia/mita_sanoi/e_ilmaisunvapaudesta.asp > [last visited 14.8.2017].

219 Explanatory report of the Council of Europe Convention on Access to Official Documents, *Explanatory Report – CETS 205 – Access to Official Documents*; See also for example P.Birkinshaw, *Freedom of information The Law, the Practice and the Ideal*, (Cambridge, 2010) 29; P. Birkinshaw, "Review of V. Deckmyn and I. Thompson (eds.), Openness and Transparency in the European Union" in *European Public Law* 4 (1998), 614–615..

220 Currently article 15 of TFEU.

221 See also A. Alamanno, "Unpacking the Principle of Openness in EU Law: Transparency, Participation and Democracy" in *European Law Review* 39 (2014), 72–90; P.Birkinshaw, "Review of V. Deckmyn and I. Thompson (eds.), Openness and Transparency in the European Union" in *European Public Law* 4 (1998), 613–622; H. Ragnemalm, "The Community Courts and Openness Within the European Union" in *Cambridge Yearbook of European Legal Studies* 2 (1999), 19–30.

According to Cecilia Malmström, who later became the European Commissioner responsible for home affairs, the negotiations that eventually led to the adoption of Article 255 EC were quite complicated. Resistance towards greater transparency came not only from some Member States, which lacked long traditions in access to official documents, but also from some parts of the EU institutions. These institutions were unaccustomed to the idea of public access to their documents.[222]

After the initial struggle of creating a functional legal basis for secondary legislation, it became possible to set the parameters for more detailed regulation of public access to documents in the EU context. It was during the Swedish Presidency in the spring of 2001 when this process culminated in the adoption of the Transparency Regulation.[223]

The Transparency Regulation governs the disclosure of the EU institutions' documents to the public. Its predecessor was the Code of Conduct[224] adopted by the Commission and the Council. The Commission and Council had both also adopted the decisions[225] specifying the rules on the access to these institutions' documents.[226] This adoption of these instruments took place in the beginning of 1990s. In comparison with the Transparency Regulation, one of the most significant differences is that the before-mentioned rules governed only the documents drawn up by these institutions. The current Transparency Regulation applies to all documents held by the institutions regardless of the original source. This can be considered one of the core principles of the Transparency Regulation.

The Transparency Regulation was adopted on the 30 May 2001 and this was considered as a triumph for transparency. Some authors have noted that the Regulation was the result of a long negotiation process and that its adoption was possibly due to the transparency-friendly political climate at the time.[227] Besides the appropriate climate facilitating this change, it did also require the efforts of the transparency-oriented Member States.[228]

---

222 C. Malmström, "Sveriges agerande i Öppenhetsmål inför EG-domstolen – politik och juridik hand in hand" in *Europarättslig tidskrift*, 10 (2008), 11–20.

223 I. Harden, "The Revision of Regulation 1049/2001 on Public Access to Documents" in *European Public Law* 2 (2009), 239–256.

224 Code of Conduct Concerning Public Access to Documents to Council and Commission Documents (OJ L 340, 31.12.1993, p. 41–42).

225 Council Decision of 20 December 1993 on public access to Council documents (OJ L 340, 31.12.1993, p.43–44); Commission Decision of February 1994 on public access to Commission documents (OJ L 46, 18.2.1994, p. 58–59).

226 See also for example S. Kadelbach, "Case Law A. Court of Justice", in *Common Market Law Review* 38 (2001), 179–180.

227 I. Harden, "The Revision of Regulation 1049/2001 on Public Access to Documents" in *European Public Law* 2 (2009), 239–256.

228 See for instance C. Malmström, "Sveriges agerande i Öppenhetsmål inför EG-domstolen – politik och juridik hand in hand" in *Europarättslig tidskrift*, 10 (2008), 11–20.

The right of public access to documents reached its culmination point in the European Union legal framework when the Charter of Fundamental Rights of the European Union ("the Charter") was adopted and later given the same status as the founding treaties. The Charter clearly recognizes public access to documents as a fundamental right. Article 42 of the Charter stipulates that any citizen of the Union has a right of access to European Parliament, Council and Commission documents.[229] This approach reflects the Nordic thinking of public access principle; the right of public access is a fundamental right – or constitutional right – in Nordic countries.[230]

Setting this development in an international context and looking at the international instruments in this area, the United Nations Convention on Access to Information, Public Participation in Decision-Making and Access to Justice in Environmental Matters[231] ought to be mentioned. The European Union has also ratified this so-called Aarhus Convention. However, this Convention covers only issues relating to environmental matters. The Aarhus Convention has now celebrated its 20th birthday, having been adopted in 1998.

Besides the before-mentioned legislation, the first binding international instrument regarding access to official documents was negotiated approximately 15 years ago. The Convention of the Council of Europe on Access to Official Documents (Convention 205) was opened for signatures in June 2008. As was the case regarding the protection of personal data, there were some pre-existing instruments guiding the contracting parties of the Council of Europe towards a more transparent society. The Committee of Ministers had adopted earlier both a Recommendation and Declaration regarding public access to documents. The Recommendation 2002(2) adopted in 2002 created basis for the Convention 205. At the moment, 14 contracting parties have signed the Convention and nine out these 14 have also ratified it, Norway being the first, followed by Hungary. Besides the Northern European countries, many new members of the Council of Europe, such as Montenegro, Serbia, North Macedonia and Slovenia have signed the Convention. The Convention will enter into force after ten parties have ratified it.

229 Charter of Fundamental Rights of the European Union (OJ C 303, 14.12.2007, p. 1–16).

230 See for example for Finland Perustuslaki 12 §.

231 13. Convention on Access to Information, Public Participation in Decision-Making and Access to Justice in Environmental Matters, Aarhus, Denmark, 25 June 1998.

2. THE EMERGENCE OF DATA PROTECTION IN THE EUROPEAN LEGAL FRAMEWORK

2.1 DEVELOPMENTS LEADING TOWARDS DATA PROTECTION REGULATION

The evolution of data protection legislation closely follows technological developments. In essence, the driving force behind the development of data protection regulation was the fear of the potential effects of uncontrolled use of new information technologies. The new technologies enabled gathering vast amounts of information in extensive data banks. Not only did it become possible to process large amounts of data, but the possibilities to interlink personal data also reached a new level. Information from two different data banks became easily connectable based on as little as one common element.[232] On the one hand, the new technologies were seen as a threat to privacy and on the other hand the new possibilities they offered for controlling and supervising people were considered dubious.[233] This progress can be placed in the 1960s.[234]

Initially, automatic data processing was only used for different functions of calculation. Only at a later stage did the new technologies become suitable for other types of usage on a larger scale, such as information saving, processing and combining. The technical development in this area can be considered very significant. The first computers were physically very large; their actual size was easily tens of metres.[235] Today, an effective computer fits in our purse and even pockets. Not only has it become easier to carry and place the computers and information technologies, but they have also become affordable for the wider public. Against this background, it is quite obvious why the fear of Orwell's "Big Brother" reached new proportions in the 1960s.

When looking at the progress taking place in the 1960s, it can be argued that a similar transition period is taking place today. Quite often the significance of contemporary developments is overestimated. However, the consequences of the current progress can hardly be overestimated: the rapid growth in the number of street cameras, drones, mobile phones with cameras, efficient means for data

232 A-R. Wallin & P. Nurmi, *Tietosuojalainsäädäntö,* (Lakimiesliiton kustannus, 1990) 1–7.

233 Ibid.

234 See for example Privacy International, What is Data Protection, available on the internet < https://privacyinternational.org/node/44 > [last visited 14.8.2017]. For the developments in Europe, see also De Hert, P. & V. Papakonstantinou, "The rich UK contribution to the field of EU data protection: Let's not go for "third country" status after Brexit" in *Computer Law & Security Review* 33 (2017), 355–356.

235 A-R. Wallin & P. Nurmi, *Tietosuojalainsäädäntö,* (Lakimiesliiton kustannus, 1990) 3–5.

transfers and expanded use of social networks etc. New technologies are providing possibilities to record everyday life, combined with the ability to transfer and distribute this data rapidly and very efficiently. This progress has culminated into a present state where it is said that we live in a network society.[236]

When the main development in the 1960s was the extent and ease of data collection and the possibility to combine data from different sources, while the key issue today seems to relate to the nature of the data, which new technologies enable us to collect, save and distribute. Recording your schoolteacher lecturing the class differs significantly from information about, for example, the books she has borrowed or bought on any particular day. Furthermore, new technologies not only allow you to monitor what books you have bought, but even more precisely to have information on which articles caught your attention in today's online paper, etc. The data subject themselves might not even know the conclusion drawn from the personal information his or her online behaviour reveals to a data controller.[237]

2.2 LEGISLATIVE DEVELOPMENTS IN THE EU

As was mentioned, the protection of personal data and data files is a rather new phenomenon.[238] The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) was the first European legal framework for the protection of personal data.[239] This Convention was also the first international legally binding instrument in the field of data protection and some non-European countries have also accessed Convention 108. When contextualising this progress, it should not be forgotten that Convention 108 was opened for signatures only in January 1981.[240] Achieving this goal took four years of negotiating.

At this stage, 51 contracting parties have ratified the Convention, with the latest ratifying party being Tunisia, which ratified the Convention in July 2017.[241] Even though the first international instrument regulating data protection is 37 years old,

236 A. Saarenpää, "Legal Infomatics Today – The View from the University of Lapland", in A. Saarenpää & K. Sztobryn (eds.) *Lawyers in the Media Society, The Leal Challenges of the Media Society*, (Lapin yliopisto, 2016), 10–16.

237 For profiling, see M. Hildebrandt, "Who is profiling who? Invisible Visibility", in S. Gutwith; Y. Poullet; P. De Hert; C. de Terwangne & S. Nouwt, *Reinventing Data Protection* (Springen, 2009).

238 L.A.Bygrave, *Data Protection Law, Approaching Its Rationale, Logic and Limits* (Kluwer Law International, 2002) 2.

239 Convention 108 and Protocol, available on the internet < www.coe.int/en/web/data-protection/convention108-and-protocol > [last visited 15.8.2018].

240 Convention 108 and Protocol, available on the internet < www.coe.int/en/web/data-protection/convention108-and-protocol > [last visited 15.8.2018].

241 Convention 108 and Protocol, available on the internet < www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=Xn1qwlWa > [last visited 15.8.2018].

the first national laws protecting personal data were drafted in Europe in the 1970s; that is ten years earlier. For example in Germany, a first data protection law was passed in the region of Hesse in 1970.[242] In Sweden, a national law on the protection of personal data was passed in 1973, with Sweden being the first country to enact a national data protection law.[243] In other Nordic countries, data protection laws were adopted at the end of the 1970s and the beginning of the 1980s.[244] In France, the *Loi relative à l'informatique, aux fichiers et aux libertés* entered into force in 1978.[245]

Already before the conclusion of Convention 108, there had been some attempts in Europe to find common ground on data protection principles, both in the private and public sectors. For example, the Council of Europe adopted two Resolutions relating to this topic at the beginning of the 1970s.[246]

The European data protection regime is under an extensive transition period at the moment. The first instrument regulating data protection in the European Union was Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.[247] Many of the solutions adopted earlier in the French legislation (*Loi relative à l'informatique, aux fichiers et aux libertés*) formed guidelines for the Data Protection Directive.[248] The Data Protection Directive has not been applicable from 25 May 2018 when the application of the General Data Protection Regulation began.[249]

The Data Protection Directive provided a general legal framework up until May 2018 for the processing of personal data in the European Union.[250] An interesting detail in the process towards said Data Protection Directive is the fact that the Commission amended its proposal as regards the formal distinction between the

242 See for example Privacy International, What is Data Protection, available on the internet < https://privacyinternational.org/node/44 > [last visited 14.8.2017].

243 P. Seipel, "Sweden", in Blume (ed.) *Nordic Data Protection*, (Kauppakaari, 2001), 116.

244 P. Blume, "Denmark", in Blume (ed.) *Nordic Data Protection*, (Kauppakaari, 2001), 11; A .Saarenpää, "Finland", in Blume (ed.) *Nordic Data Protection*, (Kauppakaari, 2001), 42; D.W. Schartum, "Norway", in Blume (ed.) *Nordic Data Protection*, (Kauppakaari, 2001), 78.

245 See for example L.A. Bygrave, *Data Protection Law, Approaching Its Rationale, Logic and Limits* (Kluwer Law International, 2002); For the recent developments in the EU, see B. Custers, F. Dechesne, A.M. Sears, T. Tani & S. van der Hof, "A comparison of data protection legislation and policies across the EU" in *Computer Law & Security Review* 34 (2018), 234–243.

246 CoE, Committee of Ministers (1973), Resolution (73) 22 on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector, 26 September 1973; CoE, Committee of Ministers (1974), Resolution (74) 29 on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector, 20 September 1974.

247 The ongoing reform process regarding data protection legislation in the European Union will be discussed in more detail in Chapters IV and VII.

248 Bygrave, *Data Protection Law, Approaching Its Rationale, Logic and Limits* (Kluwer Law International. The Hague, 2002) 5.

249 For an academic analysis of the GDPR negotiations, see A. Rossi, "How the Snowden Revelations Saved the EU General Data Protection Regulation" in *The International Spectator Italian Journal of International Affairs* 53(2018), 95–111.

250 From May 2018 onwards the processing of personal must be carried out in accordance with the General Data Protection Regulation.

rules applying to the public and private sectors. This was done at the Parliament's request.[251]

Besides the general legal framework there are several specific regimes for data protection and also sectoral legislation. An example of the sectoral legislation is EU Institutions' Data Protection Regulation (and its predecessor, Data Protection Regulation), which regulates the processing of personal data by the Union institutions. The former Data Protection Regulation followed the solutions adopted in the Data Protection Directive. This Regulation was also renewed in the course of the recent data protection reform.

The European legal framework, which is briefly covered in this section, illustrates that EU-level regulation of data protection is comprehensive. It follows that data protection legislation has, or at least should have, similar features in all Member States. Based on Convention 108, the similarities should be detectable in the legislation of other European states.

As was the case with the right of access to documents, the culmination point for the development of data protection has been its recognition as a fundamental right. At the latest, this took place when the Charter of Fundamental Rights of the European Union entered into force. The Charter clearly stipulates that everyone has the right to protection of personal data. Before this culmination point, the protection of personal data was seen as an element of privacy. Privacy, in turn, has enjoyed a rather unchallenged position as a fundamental right for a long time. For example, Article 8 of the European Convention on Human Rights provides everyone with the right to respect for their private and family life, home and correspondence. Privacy has long been recognised as one of the corner-stones of modern Western society.[252] Quite interestingly, the right to privacy can also be linked with developments leading society towards a more individualistic culture.[253] The scope and the limits of privacy are under constant debate and the further we are from the hard core of privacy, the more complex the questions become. The first attempts to define privacy can be placed in the United States, where this happened in close connection with the growing power of the press and the increasing influence of journalists.[254]

251 Commission of the European Communities, Explanatory Memorandum com(92) 422 final, p. 2.

252 A-R. Wallin & P. Nurmi, *Tietosuojalainsäädäntö,* (Lakimiesliiton kustannus, 1990) 1–7. For the global dimension of the development, see Benediek, A and M. Römer, "*Externalizing Europe: the global effects of European data protection*" in Digital Policy, Regulation and Governance 21 (2019), 32–43.

253 C. Bennet & C. Raab, *The Governance of Privacy - Policy instruments in global perspective*, (Ashgate Publishing Limited, 2003) 14–15.

254 A-R. Wallin & P. Nurmi, *Tietosuojalainsäädäntö,* (Lakimiesliiton kustannus, 1990) 4.

3. CONCLUDING REMARKS ON THE DEVELOPMENT OF THE RIGHTS EXAMINED IN THIS THESIS

This chapter has examined and explained some of the developments and different phases in the evolution of the transparency and data protection regimes in the European context. Next, the concluding section will examine some of the most significant similarities and differences in the evolution of these two rights.

Looking at the right of access to documents, it is easy to identify certain phases in its evolution, with the first phase covering the time from its emergence to the 1990s. This rather long period is characterised by relative silence of this right, despite the birth and existence of it, still lacking a more general breakthrough in the wider European context. While quietly and firmly strengthening its place in the Nordic countries, it did not have wider recognition in Europe. The second phase is characterised by the relatively rapid breakthrough in European countries and in the European Union institutions. It can be argued that at the moment we are living the third phase of the evolution; access to documents has not only become recognized as a right more extensively in Europe, but it is also firmly approaching its status as a fundamental right on more general level.

The evolutionary process of the right to protection of personal data is slightly different. It is not characterized by clearly separable phases. Its development has a close and logical connection with the progress of related technologies. Therefore, it also seems quite natural that its emergence throughout Europe has taken place approximately at the same time, starting from the 1970s.

From a legal point of view, it is possible to distinguish the periods when data protection was considered a part of privacy from the current situation marked by the acceptance of protection of personal data as an individual fundamental right. Despite the differences in the development processes, the culmination point of both access to documents and data protection is the same; fundamental right status. However, it seems like the concept of data protection will keep evolving further while the public access principle seems more stable. This is due to the constantly evolving technological environment. As an example of the further fragmentation of the concept of the protection of personal data, the "right to be forgotten" can be mentioned. Without elaborating this further, it suffices to note that certain elements of the protection of personal data are gradually gaining increasingly attention as independent elements.[255]

255 As a recent example of this fragmentation, see for example W. Li, "A tale of two rights: exploring the potential conflict between two rights to data portability and right to be forgotten under the General Data Protection Regulation" in *International Data Privacy Law* 8 (2018) and J.C. Buitelaar, "Child's best interest and informational self-determination: what the GDPR can learn from children's rights" in *International Data Privacy Law* 8 (2018).

Besides the differences in the evolutionary process itself, another clear difference between these two rights is that the protection of personal data has a longer common European history, while access to documents is actually an older concept, but was originally recognized only in a very limited number of European countries. When comparing the development of data protection and transparency, one of the most significant and apparent differences derives from the way they have been rooted in the European ground. While data protection has a relatively long history in European countries, access to documents is a newcomer. Naturally, both data protection and access to documents are rather "new kids on the block" when examining fundamental rights from a more general and wider perspective.

This chapter has differentiated the developments of these two rights and provided some explanations for it. However, it does seem that, in essence, the emergence of both of these rights has been launched by technological changes. While this is quite clear regarding data protection, we can also find a technological innovation behind the genesis of transparency legislation; namely printing. This observation sets an excellent ground to question why data protection development took place relatively simultaneously in different European countries when this was not the case regarding the right of access to documents.[256] The answer can be sought from a number of factors. One of the most apparent explanations relates to globalization. In a sense, Europe has become "smaller" when compared with the situation in 1776. One of the main questions in the early phases of protection of personal data was precisely the free flow of data between different European states as transborder data flows had become quite ordinary. Access to documents did not face similar issues in its early stages and, due to the different nature of this right, corresponding questions have not arisen in its later developments either.

However, we can seek another and even more interesting explanation from cultural and societal reasons. Developing technologies created pressure to protect one's privacy including personal data, as explained earlier in section 2.1. When this happened, privacy was already considered as a right requiring protection and it also needed to be protected in the changing environment. However, the technological inventions behind the laws regulating the freedom of press did not create pressure to open official files to the public. Printing did, however, enable the birth of mass media. Freedom of press can of course be realized without access to official documents, even if it can be argued that some of the core functions of this right are left incomplete without access to relevant public sector information. However, the urge to have access to official documents did not follow from the existing societal setting, but it had to arise *from* society. Thus, it can be argued that the pressure leading towards

256 See for example C.Uhr, Antti Chydenius 1729–1803, Adam Smithin Suomalainen edelläkävijä, (Helsinki, 1965). Uhr argues that Chydenius and his thoughts would have become better recognized and received if the scene had been Paris or London instead Sweden.

regulation regarding access to documents is rather based on cultural and societal changes, and the relatively slow expansion of this right can be explained by cultural and societal differences in different European states.

CHAPTER III

TRANSPARENCY

This chapter will examine some of the core concepts of European transparency legislation. While these concepts are presented in the general framework of the European transparency regime, the purpose of this chapter is not to give an exhaustive picture of the regulatory framework. Instead the focus will be on selected concepts. These concepts will play a significant role later in this thesis, when the tension between transparency and data protection will be tackled. At that stage, it will be fundamental to understand the dimensions of these concepts as well as how they function in the European legal framework. Therefore these concepts must first be identified and thereafter elaborated.

First, a general overview of the foundations of European transparency regulation will be provided. The basis to consider the right of access to documents as a fundamental right will be examined. Also, the relationship between transparency and democracy will be touched upon. More detailed analysis of this relationship will be provided in the concluding chapter. The latter part of this chapter will cover some of the most significant concepts of transparency legislation and examine how they are to be understood in the European legal framework. First, the definition of a document will be studied and this will be followed by the identification and elaboration of the core principles of transparency regulation. These principles are the soul of the legislation; not always apparent, but always present. Without a thorough understanding of these principles, one cannot fully comprehend European transparency regulation. A significant part of the content of these concepts is drawn from the case-law of the Court of Justice of the European Union and the preparatory work of the transparency legislation. The structure of this chapter and the manner which the key concepts are presented in this thesis serve mainly for the purposes of this thesis.[257]

Before engaging to this discussion further, it must be underlined that the European Union does not have the competence to harmonize legislation on access to documents in Member States.[258] European Union transparency legislation therefore

257 For comprehensive presentation of the Transparency Regulation, see B. Driessen, *Transparency in EU Institutional Law: A Practitioner's Handbook*, (Kluwer 2012). This presentation reflects, however, the personal views of the writer and approaches transparency in a rather restrictive manner.

258 See Article 5 TEU; Article 15 TFEU. See also for example Article 29 Data Protection working party, "Opinion 2/2016 on the publication of Personal Data for Transparency purposes in the Public Sector", 1806/16/EN WP 239, p. 2. WP29 clearly takes the approach that the said opinion on transparency in the public sector does

applies only to the Union institutions. It follows that Union should not regulate how personal data is disclosed based on public access to documents legislation in Member States either.[259] Transparent administration is a relatively new phenomenon in the EU context. Transparency and open governance do not have a long tradition in the European Union institutions and for a long time the presumption was rather secrecy and non-disclosure of information. Some relics of this thinking still exist.[260]

1. TRANSPARENCY IN THE EUROPEAN LEGAL FRAMEWORK – A FUNDAMENTAL RIGHT OR AN ESSENTIAL ELEMENT OF DEMOCRACY

This thesis examines the right of public access to documents as a fundamental right. Its status as a fundamental right in the European Union was controversial still some years ago and its final emergence in the field of fundamental rights has taken place only very recently. While the angle of this thesis builds on the tension between the two fundamental rights, an alternative approach would have been to examine the right of public access documents as an essential element of democratic society. This section will first elaborate the right of public access to documents as a fundamental right. Thereafter a brief overview of the relationship between transparency and democracy will be given. More detailed analysis of democracy as one the Transparency Regulation's aims will be conducted in the concluding chapter.

1.1 TRANSPARENCY AS A FUNDAMENTAL RIGHT

The nature of the right of access to documents was widely debated before the Charter of Fundamental Rights entered into force. There was not a solid understanding that the right of access to documents was fundamental right. Even though many of the Member States recognized it in their constitutions as a right, it was not unanimously accepted as fundamental right in the European Union.[261] Some dissenting opinions

not address the question of which information should be available based on national legislation in Member States. For the scope of Union law, see also case C-207/16, *Ministerio Fiscal*, ECLI:EU:C:2018:788.

259 For a different approach, see M. Koillinen, "Oikeudesta anonyymiin julkisen vallan käyttöön", in *Lakimies* 1 (2016), 26–53.

260 See for instance A. Bicarregui "Rights of Access under European Union Law" in Coppel (ed.) *Information Rights, Law and Practice*, (Oxford, 2010), 93; see also B. Driessen, "The Council of the European Union and access to documents" in *European Law Review* 30 (2005), 679–696.

261 In a survey conducted in 2005, it was discovered that 10 out of 24 Member States' constitutions acknowledged access to documents as a right. In four other Member States' constitutions, it was formulated as a duty for authorities to release information.

might still exist. However, with the entry into force of the Charter of Fundamental Rights, there is no longer room for a real dispute over the nature of the right of public access. It is a fundamental right. However, the Charter recognizes public access to documents as fundamental right only in relation to the EU institutions. Hence, those Member States which do not recognize public access to documents as a fundamental right may preserve their approach. In other words, public access to documents might still not be recognized as a fundamental right in the European Union on the level of all Members States, but the angle of the variance has twisted; its' nature cannot be denied when the focus is on the EU institutions.

Even if public access to documents is not recognized as a fundamental right in all European legal systems, this does not imply that it would be unknown in such cases. The right of access to public documents indeed has institutionalized status in most of the Member States. It is considered a legal principle in many of the European Union Member States. Sometimes it might be formulated as a responsibility on authorities to actively disclose information or it might be explicitly formulated as one's right of access to documents. In both cases, it establishes the right to know for the public.[262]

1.1.1 LEGAL BASIS

Before the Charter of Fundamental Rights entered into force, the right of access was explained as a fundamental right partly based on its legal basis, which was set in EU primary legislation. The legal basis for public access to documents is briefly examined next.

The legal basis for public access to the EU institutions' documents was laid down in the Treaty on the Functioning of the European Union. However, the current Transparency Regulation was drafted while the Treaty of Amsterdam was still in force and its legal basis is therefore drawn from the Amsterdam Treaty. An attempt to reform the Transparency Regulation has taken place and the negotiations for the recast process of the Transparency Regulation was launched in 2008.[263] Unfortunately, the negotiations have not advanced for years and it seems unlikely that this would change in the near future. Even the so-called "lisbonisation" of the Transparency Regulation has not been carried through, and therefore the legal basis for the Transparency Regulation is still drawn from the Treaty of Amsterdam.

262 H. Kranenborg and W. Woermans *Access to Information in the European Union – a Comparative Analysis of EC and Member State Legislation* (Europa Law Publishing, 2005), 10. See also for example T. De Freitas, "Administrative Transparency in Portugal", in *European Public Law* 2(2016), 667–688.

263 Commission Proposal for a Regulation of the European Parliament and of the Council regarding public access to European Parliament, Council and Commission documents COM(2008) 229 final (30.4.2008).

The legal basis for public access to documents has stimulated some commentaries on the nature of said right. It has been suggested that the right to information is not a *universal right*. The precise meaning of this statement is unclear, but this argument has been justified with the formulation of Article 255 of the Treaty of Amsterdam.[264] According to the Treaty of Amsterdam, the right of access to documents can be limited on the grounds of private and public interests. However, these limits have to be defined in law.[265] The Treaty on the Functioning of the European Union contains a similar provision.[266]

In other words, the legal basis clearly entitles the Council, together with the European Parliament, determine the limits for the right of access. This must be done in a legislative procedure. This might seem to limit the right of access to documents, but actually, it underlines the nature of the said right as a fundamental right. Stemming from the common European heritage, and even more importantly, from the Charter of Fundamental Rights, the restrictions to fundamental rights must be laid down by law.[267] It is acknowledged that sometimes there might be a need to balance two fundamental rights and restrict the scope of one or the other – or maybe even both – in order to apply them simultaneously, while the essence of both rights should be preserved.[268]

It therefore seems that the requirement to define the limitations in law legislated in ordinary legislative procedure actually emphasizes the fundamental nature of the right of public access. It implies that the institution cannot diverge from the Transparency Regulation by enlarging, for example, the scope of the exceptions in their internal rules of procedure. This seems even more clear after the entry into force of the Lisbon Treaty, which specifically articulates that the institutions' internal rules of procedure are to be in accordance with access to document regulation.[269] Thus the sole fact that there can be limitations to the right of access to documents cannot be considered to decrease the status of the said right.

---

264 See for instance V. Deckmyn, *Guide to European Union Information*, (European Institute of Public Administration, 2003), 5.

265 According to Article 255(2) "*General principles and limits on the grounds of public or private interest governing this right of access to documents shall be determined by the Council, acting in accordance with the procedure referred to in Article 251 within two years of the entry into force of the Treaty of Amsterdam*".

266 According to Article 15(3) of the Treaty of the Functioning of the European Union "*[…] General principles and limits on grounds of public or private interest governing this right of access to documents shall be determined by the European Parliament and the Council, by means of regulations, acting in accordance with the ordinary legislative procedure. Each institution, body, office or agency shall ensure that its proceedings are transparent and shall elaborate in its own Rules of Procedure specific provisions regarding access to its documents, in accordance with the regulations referred to in the second subparagraph*".

267 Article 52(1) of the Charter of Fundamental Rights.

268 See Chapter I.

269 Art. 15 of the TFEU stipulates that "*each institution, body, office or agency shall ensure that its proceedings are transparent and shall elaborate in its own Rules of Procedure specific provisions regarding access to its documents, in accordance with the regulations referred to in the second subparagraph*".

And lastly, if the intention with the *universal right* was to indicate that there is no such thing as unlimited access to all documents, this is true. And it is equally true that such a right would not be feasible. The advantages of transparent administration are recognized in the legislation, and good administration derives partly from the transparency. But this does not equal an all-encompassing transparency. It is equally important to protect certain interests and protecting these interests might in some cases require non-disclosure of some parts of the document. Such interests could relate, for example, to international relations or military matters. In some cases, the protection of personal data could be such an interest. When the exceptions to public access to documents are based on such interests and are first clearly defined and thereafter narrowly applied, the exceptions rather serve the core idea of transparency than diminish its purpose.

1.1.2 CHARTER OF FUNDAMENTAL RIGHTS

If the right of access to documents was earlier explained as a fundamental right based on its legal basis, the necessary institutional support for the full recognition was gained at the highest possible level when the Charter of Fundamental Rights entered into force.[270] After the entry into force of the Treaty of Lisbon[271], the Charter of Fundamental Rights became equally binding and valued with the founding treaties.

Article 42 of the Charter guarantees that "*any citizen of the Union, and any natural or legal person residing or having registered office in a Member State, has a right of access to European Parliament, Council and Commission documents*". The right of access covers the documents held by institutions, bodies, offices and agencies of the Union despite their medium. Thus, public access to documents is to be considered a fundamental right in the administrative context of the European Union. However, this approach cannot necessarily be extended to the Member States of European Union, which all have different administrative traditions.

To conclude, in the wider European context, the status of the right to information is still somewhat of a blur.[272] Not all of the Member States recognize the right to information as a fundamental right. This is the case for example in Germany and in Slovenia. However, this does not necessarily imply that the weight placed on

270 For institutional support, see Chapter I section 1.1 and in particular Dworkin, *Taking Rights Seriously*, (Duckworth 1977) 39–45, 64–68.

271 The Treaty of Lisbon entered into force 1 December 2010.

272 For wider European approach, see also ECtHR 14 April 2009, Tárásag a Szabadságjogokért v Hungary, Application No 3734/05 and ECtHR 26 May, Kenedi v Hungary, Application no31475/05. The case-law of the European Court of Human Rights suggests that Article 10 of the European Convention on Human Rights contains an element of right of access to documents held by authorities or public institutions.

transparency in a democratic society is overlooked in such cases. In Slovenia, for example, transparency is highly valued in the national legislation.[273]

1.2 TRANSPARENCY AS A PREREQUISITE FOR A WELL-FUNCTIONING DEMOCRACY

While data protection legislation has emerged simultaneously in European states, regulation relating to public access to documents has developed with very different paces in different parts of Europe. The first pan-European instrument (Convention 205) was opened for signatures only in June 2009 and it will enter into force once ten signatory parties ratify the Convention. This has not yet happened.[274]

It is not therefore surprising that the nature of public access to documents as a fundamental right might still raise some question marks in the wider European context. However, the connection between well-functioning democracy and transparency is explicitly acknowledged.[275] Besides the clear references in legislative acts on how transparency strengthens democracy, and surveys carried out in this topic, the Court of Justice of the European Union has emphasized how transparency contributes to the democratic structures of society. Furthermore, the CJEU has so far solved some hard cases by elaborating the relationship between transparency and democracy rather than the nature of public access as a fundamental right.[276] It must be noted though, that the core question in these benchmark cases has not been the collision of two fundamental rights. Instead the focus has been on the application of some of the exceptions laid down in the Transparency Regulation. These exceptions do not necessarily protect interests related to other fundamental rights. The interest protected by the exception might relate, for example, to legal advice[277] or the institutions' decision-making -process, or so-called "space to think"[278].

273 See for example Slovenian Access to Public Information Act, published on 22 March 2003 (Official Gazette of RS. No 24/2003), available on internet < www.ip-rs.si> [last visited 6.8.2017].

274 See Details of Treaty No.205, Council of Europe Convention on Access to Official Documents, available on the internet <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/205> [last visited 21.2.2017].

275 H. Kranenborg and W. Woermans *Access to Information in the European Union – a Comparative Analysis of EC and Member State Legislation* (Europa Law Publishing, 2005) 10.

276 See for example an Opinion of AG Maduro in joined cases C-39/05 P and C-52/05 P *Sweden and Turco/ Council*, ECLI:EU:C:2007:721, delivered 29 November 2007, para 32 and Joined cases C-39/05 P and C-52/05 P *Sweden and Turco/ Council*, ECLI:EU:C:2008:374. See also for example D. Ritleng, "Does the European Court of Justice take democracy seriously? Some thoughts about the *Macro-Financial Assistance* case" in *Common Market Law Review* 53 (2016), 11–34.

277 See for example, Joined cases C-39/05 P and C-52/05 P *Sweden and Turco/ Council*, ECLI:EU:C:2008:374; See also Opinion of AG Bobek in case C-213/15 P *Commission v Breyer*, ECLI:EU:C:2016:994.

278 See for example, Case C-280/11 P *Council v Access Info Europe*, ECLI:EU:C:2013.

At this stage, it is enough to note that transparency is an essential element of democratic society. The relationship between transparency and democracy will be elaborated in more detail when the aims and objectives of Transparency Regulation are examined in the concluding chapter.

2. THE CONCEPT OF DOCUMENT (VS INFORMATION)

When colliding rules of data protection and public access to documents legislation are assessed, one of the central issues to consider is how the material scope of the data protection legislation and public access to documents legislation overlaps. The Transparency Regulation applies to all documents held by an institution.[279] It is therefore essential to elaborate the concept of document in detail. For the purposes of this thesis, it is of a particular interest to assess how document differs from information, and how it relates to data banks. This will be assessed later in the concluding chapter together with the material scope of data protection legislation and, in particular, with the concept of personal data.

European public access to documents legislation provides the public with access to documents, not to information as in some Member States.[280] The difference between document and information might seem significant. Information is considered a wider concept and it can be argued that it covers more different types of data than a simple document does. However, the wide definition of document together with the case-law of the Court of Justice of the European Union has rendered the difference a minor one.[281]

The Transparency Regulation defines document as "*any content whatever its medium (written on paper or stored in electronic form a sound, visual or audiovisual recording) concerning a matter relating to the policies, activities and decisions falling within the institution's sphere of responsibility*".[282] Roughly, three

279 Regulation (EC) No 1049/2001 of the European Parliament and the Council of 30 May 2001 regarding public access to European Parliament, Council, and Commission documents (OJ L 145, 31.5.2001, p. 43–48), article 2(3).

280 H. Kranenborg and W. Woermans, *Access to Information in the European Union – a Comparative Analysis of EC and Member State Legislation* (Europa Law Publishing, 2005); See also for example P.Birkinshaw, *Freedom of information The Law, the Practice and the Ideal*, (Cambridge, 2010) 29, 118–120.

281 For case-law, see for example Case T-436/09, *Julien Dufour v European Central Bank*, ECLI:EU:T:2011:634 and Case C-353/99 P *Council of the European Union v Heidi Hautala*, ECLI:EU:C:2001:661. Also, it should be noted that according to Aarhus Regulation (1367/2006), the objective of the Regulation is to guarantee the right of public access to environmental *information* received or produced [...] Thus the vocabulary adopted in the Aarhus Regulation differs from the Transparency Regulation.

282 Regulation (EC) No 1049/2001 of the European Parliament and the Council of 30 May 2001 regarding public access to European Parliament, Council, and Commission documents (OJ L 145, 31.5.2001, p. 43–48), Article 3(1).

elements can be identified; first, the content, second, the medium and third, the matter. While the content and the matter are quite multilateral elements and they need to be examined in more detail, the third element, namely medium, seems more clear. Therefore, this section will first elaborate the notion of medium and thereafter the two other elements of document; concept and matter.

2.1 MEDIUM

It is quite clearly spelled out in Article 3 of the Transparency Regulation that the medium is not be considered when assessing whether some data forms a document. Regardless of this rather clear provision, the question has also been tried before the Court of Justice of the European Union. And the Court has confirmed that medium is insignificant when assessing whether data can be a document.[283]

However, this question is twofold. On the one hand, the medium can be considered the data itself and on the other hand, it can be seen as the base that the information is saved on. These elements might share some features, but they should be considered separately to draw the line between the information and the base it is attached to. As for the first point, the Court of Justice has clarified that for example audiotapes are documents.[284] Furthermore, the General Court has specified that the definition covers also CDs, videotapes etc.[285] Besides moving pictures and voice, the General Court has confirmed that information in a database is also a document. However, the General Court did not reflect on the question whether the database as such could be considered a document.[286]

2.2 CONTENT

Once it has been established that the right of access covers the information in the documents regardless of the medium, the next step is to assess whether all information should be considered a document. While it is relatively easy to state that medium is indifferent when assessing whether the requested data forms a document, the question of content is more challenging.

How to define what constitutes the content of a document is a fundamental question from many perspectives. If all information were to be considered a

283 See for example Case T-121/05, *Borax Europe v Commission,* ECLI:EU:T:2009:64; Case T-166/05, *Borax Europe Ltd. v Commission*, ECLI:EU:T:2009:65.

284 Case T-121/05, *Borax Europe v Commission,* ECLI:EU:T:2009:64; Case T-166/05, *Borax Europe Ltd. v Commission*, ECLI:EU:T:2009:65.

285 Case T-436/09, *Julien Dufour v European Central Bank*, ECLI:EU:T:2011:634, para 90.

286 Ibid., paras 125, 164.

document, the applicant could request, for example, some information from a databank, like a series of numbers or personal data based on his or her right of access to documents. This is a highly relevant question, in particular regarding the relation of personal data and access to documents. So far, the tension between access to document and data protection legislation has concretized in situations where the applicant has requested a document containing personal data, or certain personal data which has been a part of a document, not purely personal data which could, for example, be retrieved from databanks.

The right of partial access to documents which stems from the Hautala[287] case, and was later incorporated into the Union legislation, renders the difference between the concepts of information and document nearly insignificant.[288] It has been argued, however, that information should form a understandable entity, or be understandable to be considered a document.[289] The interpretation of the highest authority, the Court of Justice of the European Union, is still missing. However, the General Court did assess and elaborate this question in the Dufour case. The General Court elaborated the elements for defining document in a context where access had been requested to European Central Bank documents.[290]

The General Court adopted a very broad approach regarding the definition of a document. It first concluded "*that a document* […] *may be a book of several hundred pages or a 'piece of paper' (to borrow the term used by the ECB in an argument summarised in paragraph 70 above) containing a single word or figure, such as a name or telephone number. Similarly, a document may consist not only of text, as in the case of a letter or memorandum, but also a picture, catalogue or list, such as a telephone directory, a price list or a list of spare parts*". The General Court went further by stating that "*as has already been noted* […], *the terms used in that definition necessarily imply that even content of minuscule proportions, such as a single word or figure, is, if it is stored (for example, if it is written on a piece of paper), sufficient to constitute a document*". And even more importantly, it stated "*it is clear* […] *that a literal interpretation of the definition of the term*

287 Case C-353/99 P *Council of the European Union v Heidi Hautala*, ECLI:EU:C:2001:661.

288 The case T-264/04 World Wildlife Fund EEP v EU Council has been interpreted by some as General Court taking a stand of the definition of document [A. Bicarregui "Rights of Access under European Union Law" in Coppel (ed.) *Information Rights, Law and Practice*, (Oxford, 2010), 102]. However, it seems like this reference to the General Court holding that the Regulation "*applies to information generally and not only simply to documents*" is incorrectly interpreted as the Court's statement when it actually was the conclusion of parties' arguments. Also, the case relates the relationship of Aarhus Regulation and Regulation 1049/2001 and as earlier noted, the Aarhus Regulation governs access to information when Regulation 1049/2001 covers access to documents.

289 Case T-436/09, *Julien Dufour v European Central Bank*, ECLI:EU:T:2011:634, paras 112, 114, 115–117.

290 Decision of the European Central Bank of 4 March 2004 on public access to European Central Bank documents (ECB 2004/3)(2004/258/EC) (OJ 2004 L 80, p. 42). The definition of a document is similar with the Transparency Regulation and the recitals of the said decision refer to the Transparency Regulation. See in particular case T-436/09, *Julien Dufour v European Central Bank*, ECLI:EU:T:2011:634, paras 54–55, 66, 68, 80, 106, 119, 121, 123, 157–159, 162, 164, 166.

'document' [...] *leads to the conclusion that the entirety of the data contained in a database constitutes a document within the meaning of that provision and that no considerations of a practical nature, and none of the various documents to which the parties refer, can call that conclusion into question*".[291] In other words, all information in the databanks is to be considered a document. The General Court did not take the view that, for example, the entity which the information forms could be of relevance when assessing what constitutes a document.[292] The approach adopted by the General Court follows the direction established by earlier case-law and Union legislation, drawing strong parallels between information and document. The General Court concluded that separate words, lists, catalogues or for example figures can be considered a document. The General Court underlined that, for example, length cannot be considered relevant when assessing whether the information at hand is to be considered a document.[293] Consequently one name or a set of names could be considered a document in the meaning of the Transparency Regulation.

Another interesting and relevant point, which the General Court considered in its judgment was how to assess whether the applicant had requested information where its disclosure would require the institution to create a *new* document. This is an interesting point, particularly because it has often been argued – and also confirmed by the General Court – that an institution does not have an obligation to create a new document for the applicant.[294] The General Court first clarified that such information, which is not saved on any base, does not constitute a document. An example of such information would be discussions in a meeting, which all the participants would indeed remember but which has not been recorded. In other words, the civil servants would not be obliged to present this information as a document.[295] Secondly, the General Court set out the rather evident point that a document which is removed or deleted from the database is not to be considered a document in the meaning of the Transparency Regulation.[296] This is the case even when those documents could somehow be retrieved from the database.[297]

---

291 Ibid., paras 94, 108, 125, 164.

292 Case T-436/09, *Julien Dufour v European Central Bank*, ECLI:EU:T:2011:634, paras 94, 108, 164. For the coherence of the information see for example Government bill for the Public Access to Document Law HE 30/1998 vp, p. 19,53,73 and 82 (Finland, laki viranomaisen toiminnan julkisuudesta 21.5.1999/621).

293 Ibid., paras 91, 93, 94.

294 See for example Case T-436/09, *Julien Dufour v European Central Bank*, ECLI:EU:T:2011:634, paras 73, 149. See also case C-491/15 P, *Typke v European Commission*, ECLI:EU:C:2017:5, para 37.

295 Case T-436/09, *Julien Dufour v European Central Bank*, ECLI:EU:T:2011:634, paras 88–89, 126–127.

296 The reference was to the Decision of the European Central Bank of 4 March 2004 on public access to European Central Bank documents (ECB 2004/3)(2004/258/EC) (OJ 2004 L 80, p. 42). See what has been said earlier of the similar interpretation of this decision and Transparency Regulation.

297 Case T-436/09, *Julien Dufour v European Central Bank*, ECLI:EU:T:2011:634, paras 128–130.

In other words, the applicant cannot expect that an institution takes up the aforesaid measures. Thus, an institution cannot be expected to create a new document which corresponds to the needs of an applicant. However, the institution has certain level of responsibility to assist the applicant.[298] As the Republic of Finland submitted in the Dufour case, the term document "*also includes any combination of data in a database that can be produced using the tools for that database. The fact that such a search, although possible, is not carried out by the institution in question as part of its day-to-day activities is, in that regard, irrelevant*".[299] The Kingdom of Denmark took a similar approach and the General Court confirmed this view in its decision.[300]

The aforementioned measures could be described as gathering information. Thus, the institution is not required to create a new document, but simply put together the information it already has. This would be the case, for example, when an institution has the information an applicant is requesting, but it was dispersed in different registers and data banks. If the information could be retrieved from the data banks by using normal search functions, the current "non-existence" of a document should not be accepted as grounds for non-disclosure of the information.

Another interesting element, which the General Court clarified in its judgment was that the permanent nature of the information is insignificant. Thus, the constantly changing content of a database would not be an obstacle to consider the information a document. The content of the database should be assessed according to the date of the request.[301]

The General Court's approach is justified. First, even if it might at first seem quite far-reaching to consider all information a document regardless of size or coherence, the institution that examines the application cannot know what might be relevant information for the applicant. Thus, if none of the exceptions would be applicable in the said case, access should not be refused based on irrelevance of the information.[302] Second, the requirement set for the institution to gather information which already exists seems more than reasonable. Data filing systems are constantly developing. If fragmented information was to be excluded from the scope of the Transparency Regulation, it could lead to a situation where a vast amount of information was dispersed in different databanks and therefore unreachable in the meaning of the Transparency Regulation. The General Court found a fair balance between the applicant's right to receive information and the institution's administrative burden.

298 See for example Regulation (EC) No 1049/2001 of the European Parliament and the Council of 30 May 2001 regarding public access to European Parliament, Council, and Commission documents (OJ L 145, 31.5.2001, p. 43–48), Article 6(2)–(3).

299 Case T-436/09, *Julien Dufour v European Central Bank*, ECLI:EU:T:2011:634, para 63.

300 Ibid., paras 59 and 153.

301 Case T-436/09, *Julien Dufour v European Central Bank*, ECLI:EU:T:2011:634, para 130.

302 See also Case T-436/09, *Julien Dufour v European Central Bank*, ECLI:EU:T:2011:634, paras 111, 112, 115.

2.3 MATTER

The two first components of the document were medium and content. The third element is closely related to content, but instead of the form of the content, the third element draws from the substance of the content.

The third element in Article 3 limits the scope of a document to those matters which concern *the policies, activities and decisions falling within the institution's sphere of responsibility*.[303] This would basically exclude the personal communication of civil servants from the scope. However, it would not automatically exclude, for example, all e-mails exchanged between civil servants. Provided that these e-mails relate to policies etc. falling within the institution's sphere of responsibility, they would indeed be documents in the meaning of Article 3 of the Transparency Regulation.

3. REQUESTS FOR DOCUMENTS

This section will address two main elements of requests for public access to documents. The first element relates to the notion of an applicant, in other words the question of who can file an application for public access to documents. The elaboration of this notion will be followed by the question of whether an applicant should state reasons for the request. The latter topic is particularly important in the context of data protection.

3.1 APPLICANT

Any citizen of the Union and any natural or legal person residing in a Member State is entitled to access to documents of the institutions. This follows from the Charter of the Fundamental Rights and is also clearly stipulated in the Transparency Regulation.[304] Even if the Charter limits the access right to Union citizen and to those who are permanently staying in the Union, the institutions have adopted a wider approach.[305] The wider approach derives at least partly from the possibility to make

303 Regulation (EC) No 1049/2001 of the European Parliament and the Council of 30 May 2001 regarding public access to European Parliament, Council, and Commission documents (OJ L 145, 31.5.2001, p. 43–48), article 3.

304 Article 42 of the Charter of Fundamental Rights; Article 2(1) of Regulation 1049/2001.

305 See for example Report from the Commission on the application in 2015 of Regulation (EC) No 1049/2001 regarding public access to European Parliament, Council and Commission documents, ANNEX 1, Brussels,

an application for access to documents anonymously.[306] When access to documents is applied for anonymously, the identity of the applicant cannot be verified. Hence, it has been a very practical approach to waive the narrow interpretation of Article 2(1) of the Regulation and broaden the scope of applicants. Also, this seems to be entirely in line with the underlying principle of the Transparency Regulation aiming to guarantee the widest possible access to documents.

The Commission has proposed enlarging the scope of beneficiaries to any natural or legal person in its proposal for the Regulation on access to documents.[307] This proposal broadening transparency vis-à-vis current legislation might be prejudiced by the inadequate legal basis.[308] Even if the current practice allows wider access to documents than required by the secondary legislation, the primary legislation limits the beneficiaries to the citizen of the Union, and to any natural or legal person residing, or having its registered office in, a Member State.[309]

If the strict interpretation is adopted, the applicant should have some connection to the European Union, be it either citizenship or permanent residence in the European Union. Thus, non-citizens residing outside of the European Union would not have the right of access to documents. For example, an Australian living in the United States would not be entitled to information held by the EU institutions.

3.2 STATING REASONS FOR THE APPLICATION

One of the core elements of public access to documents legislation in the European Union legal framework has been the equal treatment of applications regardless of the origin of the application. This feature follows from the idea of *public* access to documents. The situation is slightly different in the other main European institution, namely in the Council of Europe. The case-law of the European Court of Human Rights indicates that access is granted to official documents and for individual

24.8.2016, COM(2016) 533 final, p. 7, available on the internet < http://eur-lex.europa.eu/resource.html?uri=cellar:3a0be84b-69fd-11e6-9b08-01aa75ed71a1.0003.02/DOC_2&format=PDF > [last visited 5.3.2017].

306 See article 6(1) of the Regulation (EC) No 1049/2001 of the European Parliament and the Council of 30 May 2001 regarding public access to European Parliament, Council, and Commission documents (OJ L 145, 31.5.2001, p. 43–48).

307 Commission Proposal for a Regulation of the European Parliament and of the Council regarding public access to European Parliament, Council and Commission documents COM(2008) 229 final (30.4.2008).

308 The settled case-law of the Court of Justice does allow though that secondary measures are adopted based on the primary legal basis of an act, or when necessary, see Case C-211/01, *Commission v Council*, ECLI:EU:C:2003:452, paras 38–40 and case C-178/03, *Commission v Parliament and Council*, ECLI:EU:C:2006:4, para 43.

309 During the past years, the EU body has asked the requester's postal address in some cases. See for example AsktheEU.org, available on the internet <https://www.asktheeu.org/en/help/privacy> [last visited 19.8.2018].

applicants rather than public access to documents.[310] The Convention negotiated in the framework of the Council of Europe sets as a principle access to public documents.[311]

At first sight, this difference might seem minor. However, it leads to significant differences in the application of the rules. When access is granted to the public, the information of the applicant becomes irrelevant. As previously noted, the documents can be requested anonymously. That is, the identity of the applicant does not play a role when assessing whether the document should be disclosed. Also, the settled practice of the Council is indeed to disclose all documents on the internet, if access has been granted to one applicant.[312]

Quite interestingly, when placing this feature of European access to document legislation into the Dworkinian theory of rights and principles, the separation of individual aims and collective aims seems to play a role.[313] When application can be filed anonymously and even more importantly, the identity of an applicant is insignificant, the right of an individual seems to approach the features of collective right. Furthermore, the right of access to documents is precisely defined as the public's right.[314] Now, if the right was considered collective instead of individual, it would be based on policies instead of principles and in a Dworkinian world could not collide with rights based on principles.[315] Policies always weigh less and as such, principles trump policies regardless of the circumstances of the case.[316] Regardless of the rather abstract features of the right of access, it does take the form of an individual right, in other words as concrete right. The one exercising the right of access to documents is always a natural person, or legal person. It follows that the right of access to documents is concretized in the form of an individual right in each case. It differs in this respect from democracy, for example. The difference between aims and objectives and principles will be further developed and examined in the concluding chapter. At this stage it suffices to say that regardless of the described characteristics, the right of access to documents is considered a right based on principles in this thesis.

---

310 See for example ECtHR 2 November 2010, *Gillberg v Sweden;* ECtHR 7 July 1989, *Gaskin v the United Kingdom*;

ECtHR 14 February 2006, *Turek v Slovakia*, (2006–II); ECtHR 19 February 1998, *Guerra and Others v Italy*.

311 Council of Europe Convention on Access to Official Documents, (ETS No 205).

312 For Council's *erga omnes* practice, see B. Driessen, *Transparency in EU Institutional Law: A Practitioner's Handbook*, (Kluwer 2012) 44.

313 For individual and collective rights, see R. Dworkin, *Taking Rights Seriously*, (London, 2009) 90–100.

314 On freedom to receive information, see for example R. Gisbert, The Right to Freedom of expression in a democratic Society, in Roca & Santolaya (ed.) *Europe of Rights: A Compendium of the European Convention of Human Rights*, (Leiden, 2012) 386.

315 See Chapter I section1.2. See in particular R. Dworkin, *Taking Rights Seriously,* (London, 1977) 90–122; R. Dworkin, Rights as Trumps, in Waldron (ed.) *Theories of Rights*, (Oxford, 1984), 153–167.

316 Ibid.

The question of the applicant's identity becomes interesting when it is assessed in the context of stating reasons for an application – or to be more precise, in the context of not being obliged to state reasons for an application. Article 6 of the Transparency Regulation stipulates that the applicant is not obliged to state reasons for the application.[317]

The Council legal service's interpretation of the said provision together with the element of *public* access to documents has been that the Council must abstain from taking into consideration individual reasons presented by the applicant. This is the case when, for example, an academic has filed a request for documents. The personal interests of the applicant have not been considered.[318] Still in 2009, this approach seemed justified based on the case-law together with the existing legislation. At that stage there did not seem to be reasons to adopt a different approach.

At this stage it is important to note that the specific interest of the applicant does not necessarily equal the reasoning of an application. Application can, of course, also be justified in more general terms. This would be the case if the information was necessary for example for the protection of the environment. This question is also linked with the question of the existence of an overriding public interest, which will be examined later in this chapter.[319]

While the right to file a request for a document anonymously is an important element of the Transparency Regulation, it does not necessarily belong at the hard core of the said right. While the legal framework created in the Council of Europe also sets weight on the right not to state reasons, the European Court of Human Rights has often assessed the right of access to documents precisely through some specific interest the applicant has in the case.[320]

Public access to documents in the European Union should rather be understood as wide access to official documents instead of party access to these documents. Party access would always relate to a certain situation and circumstances while simple

317 Regulation (EC) No 1049/2001 of the European Parliament and the Council of 30 May 2001 regarding public access to European Parliament, Council, and Commission documents (OJ L 145, 31.5.2001, p. 43–48).

318 Case C-266/05 P, *Sison v Council*, ECLI:EU:C:2007:75, para 43; B. Driessen, *Transparency in EU Institutional Law: A Practitioner's Handbook*, (Kluwer 2012) 45,70; B. Driessen, "The Council of the European Union and access to documents" in *European Law Review* 30 (2005), 690.

319 For reasoning on general terms, see Case T-115/13, *Dennekamp v Parliament*, ECLI:EU:T:2015:497, para 68.

320 Council of Europe Convention on Access to Official Documents lays down following conditions for requesting the access in its Article 4:

1. An applicant for an official document shall not be obliged to give reasons for having access to the official document.

2. Parties may give applicants the right to remain anonymous except when disclosure of identity is essential in order to process the request.

3. Formalities for requests shall not exceed what is essential in order to process the request.

For the case-law, see ECtHR 2 November 2010, *Gillberg v Sweden;* ECtHR 7 July 1989, *Gaskin v the United Kingdom*;

ECtHR 14 February 2006, *Turek v Slovakia*, (2006–II); ECtHR 19 February 1998, *Guerra and Others v Italy*.

access to documents could relate to a wider range of situations, even if the specific interests of the applicant are taken into account. Thus, when assessing whether to disclose documents, the weight should rather be in granting the widest possible access to information, not in disclosing the documents to the public as a whole. This should be the approach in particular in such cases, where the interpretation of *public* access to documents would actually limit access to documents.

4. UNDERLYING PRINCIPLES

At the outset, the administration should be transparent. As it will be argued later in this thesis, transparent administration leads to less corruption and more open decision-making strengthens the democratic framework of society. It follows that disclosure of documents and information should rather be the presumption than an exception.[321] This seems obvious when formulated like this. However, when taking this approach to a more practical level, it suddenly turns into a more challenging question. Instead of asking why a piece of information cannot be disclosed, the commonly rising question seems to be whether it could be disclosed.[322] At first sight the difference might seem insignificant, and naturally both questions might lead to a similar outcome, i.e. disclosure of the same amount of information. However, it does reveal how the one posing the question addresses transparency; the presumption of disclosure is stressed differently. The first questioner presumes that the information will be disclosed unless there are particular reasons not to. The second questioner's starting point is not to release the information unless there are particular reasons speaking in favour of the disclosure. The underlying principles in the European transparency framework strengthen the approach of the first questioner.

This section will examine the founding principles and some of the rules stemming from these principles in the public access regime in the European legal framework. In some cases, the principles are fairly easy to identify. But in some cases, they are more implicit and need to be recognized or found.[323] However, in both cases they illustrate the spirit of the European transparency regime. And even more importantly, they form the basis for the interpretation of law in situations where a potential tension between rules arises.

Many of the principles have been developed in the practice of the Court of Justice of the European Union and, in some cases, later incorporated into Union

321 See for instance Bailey S.H., *Administrative Law,* (London, 2005) 42–44; see also Case T-395/13, *Samuli Miettinen*, ECLI:EU:T:2015:648, para 21.

322 For example in *National Information Law Conference,* Canberra, 23–25 March 2011.

323 For more see Chapter I.

legislation. Often the examined principles and rules share the same fundamental object of granting the widest possible access to information and therefore might be partly overlapping.

4.1 WIDEST POSSIBLE ACCESS

The principle of widest possible access had already existed and was apparent in the European Union legal framework when it was finally clearly formulated in the recitals of the Transparency Regulation in 2001. The fourth recital of the Regulation states that "*the purpose of this Regulation is to give the fullest possible effect to the right of public access to documents*". The actual impetus to this principle was given earlier in the Hautala case.[324] The Hautala case can certainly be considered one of the breakthrough cases in European access to documents case-law. The principle of partial access was formulated in this case, but even more importantly, the Court based the *partial access* rule on the principle of widest possible access. The principle was sought from Declaration No. 17 of the Maastricht Treaty and Code of Conduct.[325] Thus the Court held that the possibility of disclosing the document partially had to be examined even if such a rule did not exist in the Council Decision on public access to documents.[326] The Court's ruling was based on the principle of the widest possible access, which was sought from the regulatory framework. The formulation of the widest possible access principle seems to be a classical example of how principles are recognized in Dworkin's and Alexy's terms, with the principle of widest possible access also gaining the necessary institutional support.[327] First, it was recognized by the Court of Justice and later incorporated into the legislative act itself.

After its initial appearance, the principle of the widest possible access has been confirmed repeatedly in the Union's case-law.[328] Withholding information has been argued on several different grounds, however, it seems that this fundamental principle has not yet been challenged. Thus, it can be argued that widest possible

324 Case C-353/99 P, *Council of the European Union v Heidi Hautala*, ECLI:EU:C:2001:661, paras 80–83. See also D. Curtin, "Citizens' fundamental right of access to EU information: an evolving digital *passepartout?*" in *Common Market Law Review* 37 (2000), 16–18.

325 Ibid.

326 Council decision on public access to Council documents, 20 December 1993.

327 For institutional support, see for example R. Dworkin, *Taking Rights Seriously*, (Duckworth 1977) 39–45.

328 See for example C-135/11P, *IFAW Internationaler Tierschutz-Fonds v Commission*, 21 June 2012 (not yet published), para 49; Case C-506/08 P, *Sweden v MyTravel and Commission*, ECLI:EU:C:2011:496, para 75; Case C-266/05 P, *Sison v Council*, ECLI:EU:C:2007:75, para 63; Joined cases C-39/05 P and C-52/05 P *Sweden and Turco/ Council*, ECLI:EU:C:2008:374, para 36; Joined cases C-514/07 P, C-528/07 P and C-532/07 P *Sweden and Others v API and Commission*, ECLI:EU:C:2010:541, para 73; Case T-395/13, *Samuli Miettinen*, ECLI:EU:T:2015:648, para 17.

access has obtained a status as one of the core principles of public access to documents legislation.

The principle of widest possible access lays underneath most of the other core concepts and rules of the Transparency Regulation. For example, the wide definition of a document can be seen as an expression of this principle, and the narrow interpretation of the exceptions stems partly from the principle of the widest possible access. The overlapping characteristics of the elements introduced in this section are partially explained by this.

4.2 PARTIAL ACCESS

The principle of widest possible access emerges for example in the form of partial access to documents. This rule was first established in the case-law of the Court of Justice of the European Union. A Member of the European Parliament, Heidi Hautala, had requested a document containing information on arms export rules. Even if the applicable rules did not contain provisions setting requirements for partial access, the said rules did not disallow such interpretation either. Thus, the Court of Justice concluded that it was not in line with the principle of proportionality to refuse partial disclosure of the document.[329] This case-law was later incorporated into the legislation in Article 4(6) of the Transparency Regulation.[330]

The partial access rule was first developed or found in the early 2000s in the regulatory framework of the European Union. Also, most of the European Union Member States have provisions in their transparency legislation, which secure partial access to a document in cases where the document cannot be released entirely.[331] As previously explained, this approach has rendered the difference between access to documents and access to information a minor one.[332]

In more practical terms, this rule sets the duty for the institutions to assess whether the document can be released partially when it is not entirely covered by the exception applied. It follows that those parts of the document which could be released without undermining the interests protected by the exceptions have to be disclosed. Quite rarely the requested documents would be entirely covered by one or more exceptions. In most cases some parts of the document can be released. An example of this is In 't Veld case, where a Dutch Member of the European Parliament

329 Case C-353/99 P, *Council of the European Union v Heidi Hautala*, ECLI:EU:C:2001:661, paras 27–31; Council decision on public access to Council documents, 20 December 1993.

330 According to Article 4(6) of the Regulation 1049/2001 if only parts of the requested document are covered by any of the exceptions, the remaining parts shall be released.

331 H. Kranenborg and W. Woermans *Access to Information in the European Union – a Comparative Analysis of EC and Member State Legislation* (Europa Law Publishing, 2005), 18–19.

332 See Chapter IV section 2.

had requested access to legal advice given by the Council's legal service. The General Court itself examined the content of the said document and concluded that while it did include parts covered by some of the exceptions, there were indeed some parts which could have been disclosed.[333]

The partial access rule is also very closely linked to the institutions' duty to examine the documents individually and to make decisions about disclosure based on the content. Only individual examination enables partial disclosure of the documents.

4.3 NARROW INTERPRETATION OF EXCEPTIONS

The exceptions to the right of access to documents must be interpreted narrowly. This is another well-established element in the CJEU's case-law.[334] It is an element which clearly reflects the more general principle of the widest possible access to documents.[335] This also reflects a more general approach in EU law; that the exceptions from the main rule should be interpreted restrictively. Hence this approach does not differ from general EU law.

The Court has given more concrete content for the principle of narrow interpretation by underlining the following elements. Firstly, the Court has been very precise that the institutions have the duty to ensure that the requested document actually contains the type of information which is protected by the exception applied.[336] It follows that it does not suffice that the document is for example named "legal advice", if it does not in reality contain any legal advice. Consequently, withholding certain information requires that the institution verifies that the information is actually the type of information that is protected by the applied exception.

A second element of the narrow interpretation is the necessity to evaluate whether the interest protected by the exception would actually be endangered if the information was disclosed. Thus it does not suffice to ensure that the document actually contains information protected by the exception, but also that the actual disclosure of the information should somehow undermine the protection of that

333 Case T-529/09, *In 't Veld v Council*, ECLI:EU:T:2012:215, paras 106, 112. See also case T-350/12P, *In 't Veld*, ECLI:EU:C:2014:2039.

334 See for example Case T-395/13, *Samuli Miettinen*, ECLI:EU:T:2015:648, paras 58, 67; Case C-266/05 P, *Sison v Council*, ECLI:EU:C:2007:75, para 63; Joined cases C-39/05 P and C-52/05 P *Sweden and Turco/ Council*, ECLI:EU:C:2008:374, para 36; Joined cases C-514/07 P, C-528/07 P and C-532/07 P *Sweden and Others v API and Commission*, ECLI:EU:C:2010:541, para 73; Case C-506/08 P, *Sweden v MyTravel and Commission*, ECLI:EU:C:2011:496, para 75.

335 See for example Case T-529/09, *In 't Veld v Council*, ECLI:EU:T:2012:215, paras 17–18.

336 Case T-395/13, *Samuli Miettinen*, ECLI:EU:T:2015:648, para 25.

interest.[337] It follows that an assessment of the consequences of the disclosure is required when the exceptions are applied.[338]

Furthermore, the CJEU has on several occasions underlined on a more general level that all exceptions to the right of access must be interpreted narrowly.[339] Hence it can be argued that the well-established principle of narrow interpretation requires that the scope of the exception cannot be extended by the interpretation. Thus, the scope of the said exception is strictly limited to the wording of the Transparency Regulation.

4.4 NO BLOCK EXEMPTIONS

One of the founding elements of European access to document regulation is that it covers all documents held by the EU institutions. In other words, no information is excluded from the scope of the Transparency Regulation solely based on the nature of the information or based on the origin of the document. This follows directly from the Transparency Regulation.[340] Furthermore, based on well-established case-law, the assessment of the disclosure of the document must be based on the content of the document.[341] These are the elements which form the basis for the underlying idea of "no block exemptions".

The principle of no block exemptions is not explicitly formulated in the regulatory framework of transparency legislation and is therefore controversial to some degree. Also, the recent case-law has tried heavily the limits of this principle.[342] Nevertheless, its weight cannot be overlooked. Firstly, it has long roots in European thinking. The first indications of such thinking in the European Union can be traced all the way to pre-Amsterdam era and the regulatory framework of that time. In some early access to documents cases, the General Court refused to confirm the arguments which

337 See for example joined cases C-39/05 P and C-52/05 P *Sweden and Turco/ Council*, ECLI:EU:C:2008:374, para 49; joined cases T-424/14 and T-435/15, *ClientEarth v Commission*, ECLI:EU:T:2015:848, para 59.

338 See for example, Case C-280/11 P, *Council v Access Info Europe*, ECLI:EU:C:2013:671, para 31.

339 See for example joined cases T-424/14 and T-435/15, *ClientEarth v Commission*, ECLI:EU:T:2015:848, para 58; Case C-266/05 P, *Sison v Council*, ECLI:EU:C:2007:75, para 63; example joined cases C-39/05 P and C-52/05 P, *Sweden and Turco/ Council*, ECLI:EU:C:2008:374, para 36; Case C-280/11 P *Council v Access Info Europe*, ECLI:EU:C:2013:671, para 30.

340 Regulation 1049/2001, article 1(4).

341 See for example joined cases C-39/05 P and C-52/05 P, *Sweden and Turco/ Council*, ECLI:EU:C:2008:374, paras 38–40. See also P. Birkinshaw, "Review of V. Deckmyn and I. Thompson (eds.), Openness and Transparency in the European Union" in *European Public Law* 4 (1998), 614.

342 See for example joined cases T-424/14 and T-435/15, *ClientEarth v Commission*, ECLI:EU:T:2015:848, paras 64–65; case C-562/14 P, *Sweden and Spirlea v European Commission*, ECLI:EU:2017:356 and case C-271/15 P, *Sea Handling SpA, in liquidation, formerly Sea Handling SpA v commission*, ECLI:EU:C:2016:557. However, see also case C-331/15 P, *French Republic v Carl Schlyter*, ECLI:EU:C:2017:639. For the presumption of non-disclosure, see D. Curtin & P. Leino, "In search of transparency for EU law-making: Trilogues on the cusp of dawn" in *Common Market Law Review* 6 (2017), 1078–1079.

suggested that in certain cases whole policy areas were to be excluded from the scope of the access rules.[343] Further, when no common legal ground can be found in the wider European context, the profound elements of transparency legislation should be sought from Member States where it has stabilized position in the general legal framework. In such settings, the non-existence of block exemptions is considered one of the core principles of the said legislation.[344] Finally, the underlying principle of no block exemptions is apparent in the rules laid down in the Transparency Regulation. The rules reflecting this principle relate to the origin of the document, exceptions and classified documents.

Adopting other types of approach could narrow down public access to documents. As a civil servant, I do understand the beauty of the idea of block exemptions in terms of minimizing administrative work. However, this could easily lead to situation where certain information is not disclosed even when there is no reasonably foreseeable danger of harming interests protected by the exemptions. Taking particularly into account how the case-law and the CJEU's approach has enhanced public access to the EU institutions' documents in comparison to general practice applied by the institutions, this risk is not purely hypothetical.[345]

5. OTHER CHARACTERISTIC ELEMENTS OF THE TRANSPARENCY REGULATION

The previous section discussed the underlying principles of European transparency legislation. This section will examine some of the most essential rules of European transparency legislation. The rules examined in this section are of particular importance when tackling the relationship between transparency and data protection. This section will first address the overriding public interest and this will be followed by Member State and third party documents.

343 See for example Case T-194/94, *Carvel and Guardian Newspapers v Council*, ECLI:EU:T:1996:156; Case T-174/95, *Svenska Journalistförbundet v Counci*l, ECLI:EU:T:1998:127; D. Curtin, "Citizens' fundamental right of access to EU information: an evolving digital *passepartout?*" in *Common Market Law Review* 37 (2000), 35–36.

344 See for example A. Bohlin, *Offentlighets principen*, (Stockholm, 2001) 160. Secrecy exemptions can be applied only after harm test has been carried out, i.e. not solely based on the nature of the information.

345 See for example joined cases C-39/05 P and C-52/05 P, *Sweden and Turco/ Council*, ECLI:EU:C:2008:374, paras 38–40, case T-233/09, *Access Info Europe / Council of the European Union*, ECLI:EU:T:2011:105, Case C-280/11 P *Council v Access Info Europe*, ECLI:EU:C:2013:671, Case T-540/15 *De Capitani v Parliament*, ECLI:EU:T:2018:167.

5.1 OVERRIDING PUBLIC INTEREST

"Public interest" is a challenging concept, yet it appears in various different contexts.[346] As there is not a lucid definition for public interest[347], it leaves a wide margin for appreciation. In the context of European transparency legislation, the legislator has added an extra layer to it; the public interest has to be overriding.[348] An explanation can be sought from the role given to the public interest in this context. When an overriding public interest appears, access to information should be given even if such access would undermine the interests protected by the exceptions laid down in the Transparency Regulation.[349]

The exceptions laid down in the Transparency Regulation can be divided into two categories based on the overriding public interest test. The exceptions laid down in Article 4(1) do not contain the overriding public interest test when exceptions laid down in Articles 4(2) and 4(3) necessitate assessing whether an overriding public interest exists. The exceptions subject to the overriding public interest test relate to protection of commercial interests of a natural or legal person, including intellectual property, court proceedings and legal advice, the purpose of inspections, investigations and audits and also matters where the internal decision-making -process is still ongoing. In some exceptional cases, it also covers the time post decision-making. As mentioned in the beginning of this section, when an interest protected by an exception is subject to the overriding public interest test, the document has to be disclosed when such an interest exists even if the disclosure undermines the interests protected by the said exceptions.[350]

The legislator has not given a clear indication as to how to assess the existence of an overriding public interest and the Court has also been quite prudent not to open the Pandora's box in relation to the overriding public interest. Despite the scarce guidance, two different conditions for assessing whether there is an overriding public interest can be drawn from the legal framework. The Court of Justice of the European Union has also provided procedural guidance for assessing the existence of the overriding public interest.[351]

346 See for example Regulation (EC) No 679/2016 of the European Parliament and 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 (OJ L 119, 4.5.2016, p. 1–88).

347 See for example Case T36/04, *API v Commission*, ECLI:EU:T:2007:258, para 94.

348 Regulation (EC) No 1049/2001 of the European Parliament and the Council of 30 May 2001 regarding public access to European Parliament, Council, and Commission documents (OJ L 145, 31.5.2001, p. 43–48), Article 4.

349 Joined cases C-39/05 P and C-52/05 P *Sweden and Turco/ Council*, ECLI:EU:C:2008:374, para 44.

350 Ibid.; see also for instance Birkinshaw P. *Government & Information – the Law Relating to Access, Disclosure & their Regulation*, (Tottel Publishing, 2005), 196–202.

351 See joined cases C-39/05 P and C-52/05 P *Sweden and Turco/ Council*, ECLI:EU:C:2008:374, paras 28, 40, 44.

The first indication in the Union case-law for assessing when the criteria of the overriding public interest test are met was delivered in the Turco case.[352] The CJEU held that legal advice given by the Council's legal service in the course of legislative procedure should, in principle, be disclosed to the public. In its reasoning, the Court quite firmly stated that it is in the public interest to know what the legislation is based on, and as such also have access to legal advice given during such a process. Furthermore, when setting the three steps for assessing whether the legislative documents should be disclosed, the CJEU stated that even if the interests protected by the said exception would be undermined by the disclosure, the disclosure is justified when the public interest to know relates to the legislative process.[353] Support for the adopted approach can be drawn from Recital 6 of the Transparency Regulation. It states that wider access to documents should be granted when the institution is acting in its legislative capacity.[354]

The second indication for assessing whether the circumstances of the case form an overriding public interest can be drawn from the Aarhus Regulation.[355] The Aarhus Regulation governs access to environmental information received or produced by the Union institutions. Some presumptions regarding the overriding public interest are laid down in Article 6 of the Aarhus Regulation. With certain restrictions, the overriding public interest is deemed to exist when the information requested relates to emissions into the environment. The Article also stipulates more generally that it should be taken into consideration if the information requested relates to emissions into the environment.[356]

Thus, two different occasions where an overriding public interest is presumed can be identified. First, the legal advice given in the course of the legislative process and secondly, information relating to emissions into the environment. The overriding public interest is a rather powerful provision as it contains the idea of allowing some degree of harm for the protected interests when disclosing the document and the consequences of stating something as an overriding public interest are quite far reaching. It is therefore understandable that the Court of Justice refers to it sparingly.

In the context of the Turco case, the Court of Justice of the European Union also provided guidelines for assessing whether the circumstances of the case create

352 Joined cases C-39/05 P and C-52/05 P *Sweden and Turco/ Council*, ECLI:EU:C:2008:374.

353 Joined cases C-39/05 P and C-52/05 P *Sweden and Turco/ Council*, ECLI:EU:C:2008:374, paras 38, 40, 44, 45–50, 59–60, 67–68. For disclosing information in the course of legislative procedure, see also case T-540/15, *De Capitani v Parliament*, ECLI:EU:T:2018:167.

354 Regulation (EC) No 1049/2001 of the European Parliament and the Council of 30 May 2001 regarding public access to European Parliament, Council, and Commission documents (OJ L 145, 31.5.2001, p. 43–48), recital 6.

355 Regulation (EC) No 1367/2006 of the European Parliament and of the Council on the application of the provisions of the Aarhus Convention to Information, Public Participation in Decision-making and Access to Justice in Environmental Matters to Community institutions and bodies (OJ L 264, 25.9.2006, p. 13–19).

356 Ibid.

an overriding public interest.[357] Furthermore, it has given a clear indication of who should conduct the overriding public interest test. The Court has seen that the institution has the best opportunity to assess whether an overriding public interest exists.[358] Hence, the duty to examine whether the qualifications for an overriding public interest are met is for the institution. Naturally, it might advance the applicant's cause to draw the institution's attention to such circumstances as might form the basis for an overriding public interest. However, even when such remarks have not expressly been put forward, the institution should assess on its own initiative whether the qualifications for the overriding public interest are met. This is a logical approach; the applicant is not in a position to know the detailed content of the requested document and it would therefore be disproportionate to set an onus on the applicant. As the institution is in a better position to conduct the overriding public interest test, having a clear picture of the content of the document, it is logical to set the obligation on the institution. However, it appears that so far, the institutions have not released documents based on the overriding public interest test. In the aftermath of the Turco decision, the General Secretariat of the Council has disclosed an increasing number of documents containing legal advice, but it is not apparent that those documents have been released based on the overriding public interest test. Apparently, the institutions are simply considering the public interest when balancing the interests in the first phase.[359]

5.2 MEMBER STATE AND THIRD PARTY DOCUMENTS

Before the current Transparency Regulation, the Member States had the right to veto when access to documents originating from them was requested. This right of veto was abolished when the Transparency Regulation entered into force.[360] The abolishment of the veto was considered one of the improvements strengthening transparency.[361] Thus, regardless of the original source or author of the document, it is for the institution to decide whether to disclose the document.[362]

357 Joined cases C-39/05 P and C-52/05 P *Sweden and Turco/ Council*, ECLI:EU:C:2008:374, paras 38, 40, 44, 45–50, 59–60, 67–68.

358 See for example Case T-529/09, *In 't Veld v Council*, ECLI:EU:T:2012:215, para 20; Case T36/04, *API v Commission*, ECLI:EU:T:2007:258, paras 54, 94.

359 See for example also B. Driessen, *Transparency in EU Institutional Law: A Practitioner's Handbook*, (Kluwer 2012) 70.

360 C. Malmström, "Sveriges agerande i Öppenhetsmål inför EG-domstolen – politik och juridik hand in hand" in *Europarättslig tidskrift*, 10 (2008), 11–20; Council decision on public access to Council documents, 20.12.1993.

361 Ibid.

362 See, to that effect, for example Case C-135/11 P, *IFAW International Tierschutz-Fonds gGmbH /European Commission,* ECLI:EU:C:2012:376, paras 57, 61.

Even if the institution has to make the final decision on whether to disclose the document and it is responsible for the lawfulness of the said decision, it is bound to a certain procedural basis laid down in the Transparency Regulation, and finally also to the opinion of the Member State. The Transparency Regulation provides some safeguards, which guarantee that the interests of the Member States and third parties shall be taken into account when assessing the disclosure of the document.[363]

Article 4 of the Transparency Regulation contains clear exceptions in paras 1–3 when the provisions in paragraphs 4–7 are rather procedural. These provisions set the guidelines on how to apply exceptions in some particular cases. According to Article 4(5) of the Transparency Regulation, a Member State may request that the institution not disclose a document originating from that Member State without its prior agreement. Article 4(4) in turn stipulates how to release documents originating from a third party.

The institutions should consult the Member States when releasing documents originating from them. However, it is of utmost importance to note that sole procedural actions cannot be regarded as sufficient on the institutions' part. Firstly, following from the abolishment of the veto, there has been an onus on the Member State to provide reasons when it denies the further disclosure of the said document. It cannot simply ban the disclosure of the document.[364] Secondly, the Member State is bound to exceptions laid down in the Transparency Regulation.[365] Thus the Member State cannot base its denial, for example, on national legislation. The approach adopted by the Court is quite reasonable, as the institution would hardly be in a position to assess whether such refusal is reasonably motivated.

Once the Member State has stated reasons for the refusal, it is for the institution to assess whether the given reasoning finally complies with the Transparency Regulation.[366] The institution cannot satisfactorily fulfil its obligation to give a reasoned answer to the applicant by simply referring to the negative answer from the Member State.[367] This seems quite natural; after all, it is the institution who has to defend the possible complaint later, for example in court. The Court of Justice has recently specified how the institution can fulfil this obligation. First, the institution must ensure that the reasons given by the Member State actually exist. Second, the

363 According to Article 4(5) of the Regulation 1049/2001 a Member State may request the institution not to disclose a document originating that Member State without its prior agreement.

364 Formerly Member States had the right to veto the disclosure of a document originating from them. However, this was changed when the current Regulation 1049/2001 on public access to documents was adopted in 2001. See also for instance E. Nieto-Garrido and I.M. Delagado, *European Administration Law in the Constitutional Treaty*, (Oxford, 2007) 93–97.

365 See, to that effect, for example case C-135/11 P, *IFAW International Tierschutz-Fonds gGmbH /European Commission,* EU:C:2012:376, para 34.

366 Case C-135/11 P, *IFAW International Tierschutz-Fonds gGmbH / European Commission,* ECLI:EU:C:2012:376, para 62.

367 Ibid.

institution must refer to these reasons in its decision. However, the institution is not obliged to conduct an exhaustive examination to decide whether the reasons given by the Member State are applicable. The further reasoning of the Court of Justice seems to explain this. The duty to finally assess whether the reasons provided by the Member State are actually applicable is on the Court itself. It is therefore necessary for the Court also to request the withheld documents.[368] Thus the Member State's right to be heard before releasing a document originating from them can be placed somewhere between a procedural right and substantive exception. It is certainly a procedural right, but based on the Court's second round of IFAW judgments it appears to have some relics from the earlier right to veto as well. Even if the Member State is not entitled to simply deny the disclosure, the institution's duty is satisfied with a rather prima facie type of examination.

Compared with Member States' right to deny the further disclosure of the document as long as the denial is reasoned, the procedural rights of other third parties are not as strong. When assessing the disclosure of the information, the institution has an obligation to consult the third party from which the document originates. However, Article 4(4) of the Transparency Regulation does also contain the possibility not to consult the third party. When it is clear that the document shall or shall not be disclosed, the institution is not obliged to consult the third party. Thus, when deciding on the disclosure, the institution is not obliged to consult the third party when it is evident that the consultation is not necessary.

6. EXCEPTIONS AND CLASSIFIED DOCUMENTS

This section will examine the exceptions to the right of access of documents on a general level.[369] Each of these exceptions has created a vast amount of case-law and could be examined from several different angles. However many interesting issues might arise in this context, for the core question of this thesis it suffices to have a clear picture of the logic and overall structure of the exceptions and how the exception relating to one's privacy and data protection is placed in this entity.

All exceptions to access to documents are laid down in Article 4 of the Transparency Regulation and more precisely in paragraphs 1–3 of the said Article. The list of exceptions is rather short compared to list of exceptions in some national laws.[370] However, the scope of the interests protected by the said exceptions cannot

368 Ibid, paras 62–63, 70–77.

369 Exceptions do not lead to collision of rules. See Chapter I, section 2.

370 Depending on how the exceptions are numerated, at least ten exceptions are laid down in Regulation 1049/2001 while, for example, the Finnish public access to documents legislation (Laki viranomaisten toiminnan julkisuudesta 621/1999) contains 32 exceptions.

be deemed smaller solely based on the length of the list. The exceptions laid down in the Transparency Regulation are quite general in their nature and therefore they cover quite a wide range of different interests.

As mentioned earlier, the Transparency Regulation contains two types of exceptions. The distinction is based on the necessity to evaluate whether an overriding public interest exists. Exceptions laid down in Article 4(1) are not subject to the overriding public interest test. However, exceptions laid down in Articles 4(2) and 4(3) do include the provisions establishing the necessity to evaluate whether there is an overriding public interest.

6.1 SO-CALLED ABSOLUTE EXCEPTIONS

The exceptions laid down in Article 4(1) are sometimes described as absolute exceptions.[371] It has also been argued, that "*an institution must refuse access if a document falls within the terms of exception*".[372] Without further elaboration, describing these exceptions as absolute might be slightly misleading. If the exceptions are to be considered mandatory in a sense that they do not leave any margin of discretion for the institution, this would actually put certain types of documents entirely outside of the scope of the Transparency Regulation. Yet, the scope clearly covers all documents held by the institutions.[373] It is therefore not enough for the institution to merely establish that a certain document contains information described in one of the exceptions laid down in Article 4(1) of the Transparency Regulation. This is only the first step to be satisfied when assessing the disclosure of the document or information in the document. Thereafter, the institution has to evaluate whether the disclosure of the document would actually undermine the interests protected by the exceptions. This has also been clearly stated in the case-law of the Court of Justice of the European Union.[374] Once the institution has concluded that the document or part of the document contains information that cannot be released without undermining the interests protected by Article 4(1) of the Regulation, the institution has no margin to decide on the

371 See for instance A. Sharland, "Information rights under European Union law", in Coppel (ed.) *Information Rights*, (London, 2007), 114–115; See also B. Driessen, *Transparency in EU Institutional Law: A Practitioner's Handbook*, (Kluwer 2012) 65.

372 A. Sharland, "Information rights under European Union law", in Coppel (ed.) *Information Rights*, (London, 2007), 114.

373 Regulation (EC) No 1049/2001 of the European Parliament and the Council of 30 May 2001 regarding public access to European Parliament, Council, and Commission documents (OJ L 145, 31.5.2001, p. 43–48), article 2(3).

374 For example, Case T36/04, *API v Commission*, ECLI:EU:T:2007:258, paras 54–57, 94; see also joined cases C-514/07 P, C-528/07 P and C-532/07 P *Sweden and Others v API and Commission*, ECLI:EU:C:2010:541, para 72; joined cases T-391/03 and T-70/04 *Franchet and Byk*, ECLI:EU:T:190, para 116.

disclosure of the information. It follows that when disclosure of the information would harm the protected interests, it cannot be released for instance based on the existing public interest.

The institution has to examine the documents individually[375], which is another indication of the principle of no block exemptions. If there was no obligation to assess each document individually, the decision would be based on the nature of the document rather than its content. The refusal would then not require a harm test and this would lead to a block exemption, or at least the examination would be conducted as if there was a block exemption. However, in some exceptional cases, the duty of individual examination can be set aside. The General Court has stated that in cases where the individual examination of the documents would lead to an overwhelming administrative burden, the need for individual examination can be overlooked. However, the case-law following this decision has set the threshold for this doctrine quite high.[376] Also, the institution is obliged to reason the overwhelming burden and substantiate its existence.[377]

Thus, the exceptions laid down in Article 4(1) cannot be considered absolute in any other way but releasing the institution from the overriding public interest test. The interests considered so important that they do not leave the room for the overriding public interest test are public security, defence and military matters, international relations and the financial, monetary or economic policy of the Community or a Member State. These interests are listed alongside privacy and protection of personal data in Article 4(1).[378]

6.2 OTHER EXCEPTIONS

While so-called absolute exceptions require the interest balance test when deciding whether those exceptions are applicable at all, the exceptions laid down in Article 4(2) and 4(3) contain an overriding public interest test.[379] Thus, it has been seen

375 See for example joined cases C-514/07 P, C-528/07 P and C-532/07 P *Sweden and Others v API and Commission*, ECLI:EU:C:2010:541, para 72; Case T36/04, *API v Commission*, ECLI:EU:T:2007:258, paras 55–56.

376 See for example case T-2/03, *Verein für Konsumenteninformation v Commission*, ECLI:EU:T:2005:125; Joined cases T-424/14 and T-435/15 *ClientEarth v Commission*, ECLI:EU:T:2015:848; Case C-139/07 P, *Commission v Technische Glaswerke Ilmenau*, ECLI:EU:C:2010:376; Case T-42/05, *Williams v Commission*, ECLI:EU:T:2008:325.

377 Case T-42/05, *Williams v Commission*, ECLI:EU:T:2008:325, paras 86, 89; case T-2/03, *Verein für Konsumenteninformation v Commission*, ECLI:EU:T:2005:125, para 113.

378 Regulation 1049/2001.

379 According to Article 4(2) and 4(3) of the Transparency Regulation:

"*2. The institutions shall refuse access to a document where disclosure would undermine the protection of:*
— commercial interests of a natural or legal person, including intellectual property,
— court proceedings and legal advice,

that the interests protected by these articles could suffer a little harm in cases where there is an overriding public interest which would justify the disclosure. While this has been articulated quite clearly, the institutions rarely disclose documents based on the overriding public interest test. The institutions have rather simply noted that an overriding public interest does not exist.[380] Consequently, it seems that it has been left entirely for the Court to decide whether the said circumstances meet the conditions set for an overriding public interest.[381]

The interests protected in Article 2 can be divided into three categories. The first indent covers different commercial interests which need to be protected, the second indent covers legal advice and the third indent inspections and investigations. The exception formulated in Article 3 in turn protects the institution's decision-making process. These exceptions are examined next.

The commercial interests of both natural and legal persons are protected by the first indent of the Article 2. It has also been specifically mentioned that this exception includes intellectual property. The formulation of the exception is not limiting, and therefore other types of commercial interest are also protected by the said exception. However, the normal narrow interpretation of exceptions naturally applies.

The Court of Justice of the European Union has given a couple of landmark judgments on how to interpret the exception relating to the protection of court proceedings and legal advice. As earlier explained, the Court of Justice did set wide access to legal advice given in a course of the legislative process as a presumption in the Turco case.[382] While wide access to legal advice is a presumption if delivered in the course of the legislative process, this presumption does not apply to all legal advice and even less so when it has been given in the course of court proceedings. The Court took a rather restrictive approach for the disclosure of documents which relate to court proceedings, in particular when the said process is still ongoing.[383] These decisions have underlined the liaison between transparency and democracy;

— the purpose of inspections, investigations and audits, unless there is an overriding public interest in disclosure.

3. Access to a document, drawn up by an institution for internal use or received by an institution, which relates to a

matter where the decision has not been taken by the institution, shall be refused if disclosure of the document would seriously undermine the institution's decision-making process, unless there is an overriding public interest in disclosure.

Access to a document containing opinions for internal use as part of deliberations and preliminary consultations within the institution concerned shall be refused even after the decision has been taken if disclosure of the document would seriously undermine the institution's decision-making process, unless there is an overriding public interest in disclosure."

380 See for example documents 6224/17, Brussels, 15 February 2017 and 5961/17, Brussels, 14 February 2017.

381 For circumstances of the case, see Chapter I section 2.

382 Joined cases C-39/05 P and C-52/05 P *Sweden and Turco/ Council*, ECLI:EU:C:2008:374.

383 Joined cases C-514/07 P, C-528/07 P and C-532/07 P *Sweden and Others v API and Commission*, ECLI:EU:C:2010:541.

transparency is one of the founding principles of the democratic structures of society and, as such, an important element in the legislative process. The disclosure of similar content was assessed differently in the latter case, where the legal advice related to a court proceeding where the institution was a participant. Thus, the interests protected in the second indent of Article 4 deserve a different protection depending on the circumstances of the case and therefore the disclosure of the document is not examined solely based on the content of the said documents. The content is placed in a wider context, and this was done through the overriding public interest test.[384]

The exception formulated in the third indent has been tried several times before the Court. This is an exception which becomes relevant when infringement proceedings are taking place. In these cases, it is often the parties themselves or third parties with a specific interest in the case, who are seeking the information. The party access rules would often provide more limited access to documents than the Transparency Regulation. Another reason burdening the Transparency Regulation is "unnecessary" requests filed mostly in order to delay the inspection procedure. These requests might cover thousands of pages and when the examination must be carried out individually and based on content, going through such a vast file is naturally time consuming. In some cases, this might well serve the applicant's interest.

The second set of exceptions including the overriding public interest test relate to decision-making processes. The exception covers both the ongoing decision-making process and also situations where the process is not in an active phase anymore. It has also been seen as important to enable the institutions to protect their decision-making process in cases where a certain process has been finalized.

6.3 EXCEPTION LAID DOWN IN ARTICLE 4(1)(B) – PROTECTION OF PERSONAL DATA

The exception relating to the protection of personal data is at the very core of this research. This section will shortly introduce the said exception. More profound and detailed analysis will follow when the tension between transparency and the protection of personal data will be assessed in Chapter VI and Chapter VII.

The exception relating to protecting personal data and privacy is laid down in the second part of Article 4(1). According to Article 4(1)(b) of the Transparency Regulation, "*The institutions shall refuse access to a document where disclosure would undermine the protection of privacy and the integrity of the individual, in*

384 For contextual-based approach and circumstances of the case, see Chapter I, subsection 2.2.1.

particular in accordance with Community legislation regarding the protection of personal data". At least three different elements can be distinguished in this provision. First, the privacy or integrity of the data subject must be endangered. Second, the disclosure needs to be examined based on the Data Protection Regulation. And third, there is no overriding public interest test.

Access to the document, or parts of the document, may be refused thereby, if it contains personal data, provided that the disclosure would undermine the protection of privacy and the integrity of the individual. While the wording of the said exception refers to privacy and integrity of a person, the Court of Justice has adopted an approach, which sets the weight on the nature of the information.[385] In other words, rather than examining whether the disclosure of certain personal data would undermine the privacy and integrity of a person, the Court of Justice sees that disclosure of all personal data has to be examined in light of the Data Protection Regulation. The CJEU's reading of the said exception seems to imply that it does not see the protection of privacy and integrity as separate elements of the protection of personal data. This issue will be discussed in more detail later.

As noted, the exception relating to personal data does not contain the overriding public interest clause, and therefore the parts of the document containing personal data cannot be disclosed, once it is established that the disclosure would undermine the protected interests. As the exception also refers to Community legislation, the Union data protection legislation must be taken into account when the said exception is applied.

6.4 CLASSIFIED DOCUMENTS

As previously underlined, the Transparency Regulation covers all documents held by an institution and classified documents are not an exception to this.[386] Therefore, even sensitive documents can be requested, and also disclosed, based on the Transparency Regulation. In these cases, the possible refusal must be based on individual examination of the documents, i.e. the classified marking cannot serve as the sole reason to withhold the information. Naturally, the classification provides a strong indication of the content, but still, this does not exempt the institution from the actual and individual examination of the content. It is not unusual that documents marked as "RESTREINT UE", for example, are disclosed at least partially.[387]

385 Case C-28/08P, *Bavarian Lager*, ECLI:EU:C:2010:378.

386 See also D. Curtin, "Citizens' fundamental right of access to EU information: an evolving digital *passepartout?*" in *Common Market Law Review* 37 (2000), 23–26.

387 See for example disclosure of a document 10949/05, Brussels, 23 May 2016, available on the internet

However, the special nature of sensitive documents is recognized in the Transparency Regulation. To safeguard the special interests relating to sensitive documents, Article 9 stipulates how to handle the applications relating to these documents and who is entitled to do so. These documents also form an exception from the originator rule; the sensitive documents can be disclosed only with the permission of the originator.[388] Hence, the special nature of these documents has been recognized and interests protected by the classification safeguarded by the procedural rule.

It is quite important to note though, that Article 9 does not constitute another exception, but simply lays down the process for how classified documents are to be examined. Withholding a sensitive document has to be reasoned with the exceptions of the Transparency Regulation. And the sensitive nature of the document does not suffice alone to explain the application of certain exceptions. The Luxembourg courts have been quite consistent with this approach.[389]

Another interesting point is that only documents relating to matters defined in Article 4(1)(a) can be considered sensitive in the meaning of the Transparency Regulation. It follows that only matters relating to international relations, public security, defence and military matters and monetary policy can be regarded as sensitive and receive special treatment as such. However, it seems that this should not be interpreted as meaning that only these exceptions could be applied when examining whether a sensitive document could be disclosed. This should only be taken as a first step in the process of deciding whether to disclose information and

<http://data.consilium.europa.eu/doc/document/ST-10949-2005-DCL-1/en/pdf>[last visited 20.2.2017] and document 8807/16, Brussels, 19 May 2016, available on the internet <http://data.consilium.europa.eu/doc/document/ST-8807-2016-ADD-1/en/pdf> [last visited 20.2.2017].

388 Article 9, Treatment of Sensitive documents:

"*1. Sensitive documents are documents originating from the institutions or the agencies established by them, from Member States, third countries or International Organisations, classified as 'TRÈS SECRET/ TOP SECRET', 'SECRET' or 'CONFIDENTIEL' in accordance with the rules of the institution concerned, which protect essential interests of the European Union or of one or more of its Member States in the areas covered by Article 4(1)(a), notably public security, defence and military matters.*

2. Applications for access to sensitive documents under the procedures laid down in Articles 7 and 8 shall be handled only by those persons who have a right to acquaint themselves with those documents. These persons shall also, without prejudice to Article 11(2), assess which references to sensitive documents could be made in the public register.

3. Sensitive documents shall be recorded in the register or released only with the consent of the originator.

4. An institution which decides to refuse access to a sensitive document shall give the reasons for its decision in a manner which does not harm the interests protected in article 4.

5. Member States shall take appropriate measures to ensure that when handling applications for sensitive documents the principles in this article and article 4 are respected.

6. The rules of the institutions concerning sensitive documents shall be made public.

7. The Commission and the Council shall inform the European Parliament regarding sensitive documents in accordance with arrangements agreed between the institutions."

389 See for example Case C-350/12 P *Council v Sophie In 't Veld*, ECLI:EU:2014:2039, in particular paras 97–99; see also joined cases T-110/03, T-150/03 and T-405/03 *Sison v Council*, ECLI:EU:T:2005:143, para 73.

it only indicates that the document has to be assessed in the line with Article 9 of the Transparency Regulation. Once this has been established, the civil servant assessing the disclosure of the document should have the normal palette of the exceptions to apply if necessary.

CHAPTER IV

DATA PROTECTION

The right to the protection of personal data was earlier considered only as an element of privacy. This has naturally set the weight on different elements of privacy when data protection has been balanced with other rights, and when it has been assessed whether the core elements of data protection have been taken properly into account in the reconciliation. Only very recent developments have led to the current situation where data protection is considered as an independent fundamental right.

This chapter will first examine the relationship between privacy and data protection and then focus on data protection as an independent fundamental right. The right to self-determination is an essential element in this discussion. It will be argued that self-determination is gaining an increasing importance in the European data protection framework. This development is not only significant in the relationship privacy – data protection – self-determination. It is even more intriguing in the challenging relationship between transparency and protection of personal data.

Once the general setting for the data protection framework has been examined, this chapter will focus on those elements of the data protection legislation, which will become relevant when the existing tension between the different solutions of European transparency legislation and data protection legislation will be tackled. The discussion will take properly into account the ongoing legislative reform process and even set weight on the forthcoming data protection legislation and its provisions. Even though the data protection reform has been extensive, it does not necessarily provide answers to all of the challenges caused by fast-developing technology. These developments might become significant also in relation to transparency and access to documents legislation. An example of this is how personal data is being stored and processed. Instead of traditional data files and registers, personal data exists increasingly in data flows. This, in turn has relevance when the right of access is given to documents, not to information in more general terms. As the European data protection regime is in a transitional phase, it is necessary to examine the core concepts together with some of the new data protection elements explaining the transition in detail. This is essential for providing a coherent picture of the setting in which the tension examined in this research takes place.

1. DATA PROTECTION AS A FUNDAMENTAL RIGHT

This section will first concentrate on the concept of privacy in the European legal framework and then move on to discuss the relationship between data protection and privacy. Finally, the concept of self-determination will be discussed. These three concepts interact in several different ways. Lastly, privacy's relationship with democracy will be briefly covered.

1.1 PRIVACY

Privacy is a concept with multiple dimensions and therefore rather challenging to define. It has stimulated a vast amount of literature, yet the multidimensional character of this concept seems to be the only aspect on which most authors are willing and even eager to agree.[390] In this chapter, some of privacy's characteristic features will be examined. However, this chapter does not attempt to give a thorough picture nor definition for privacy, but rather give some guidance on how privacy is understood in this thesis.

Rights relating to informational privacy can be tracked down all the way to the 18th century and to the United States of America. In Europe, similar progress took place slightly later.[391] The first pan-European acknowledgement of the right to privacy took place in the European Convention on Human Rights. In other words, the beginning of common European standards on privacy can be placed in the 1950s.[392] In Europe, privacy rights were considered first and foremost in the relationship between individuals and the state. The approach differed from the United States, where it was rather a question relating to inter-individual relations.[393] However, the approach has later become broader in Europe and, for instance, the Parliamentary Assembly explicitly underlined in its Resolution 1165 (1998) that the protection of one's privacy should also cover interference by private actors, such as mass media.[394] Consequently, it can be argued that inter-individual relations are part of European privacy rights today.

390 H. Delany & E. Carolan, *The Right to Privacy*, (Thomson Round Hall, 2008) 4; J.Q. Whitman "The Two Western Cultures of Privacy: Dignity versus Liberty" in *Yale Law Journal* 113(2004), 1153. See also K. Hughes, "A Behavioural Understanding of Privacy and its Implications for Privacy Law" in *The Modern Law Review* 75(5) (2012), 806–808.

391 A-R. Wallin & P. Nurmi, *Tietosuojalainsäädäntö,* (Lakimiesliiton kustannus, 1990) 1–7.

392 European Convention on Human Rights was concluded on 4th of November 1950.

393 A. Rouvroy & Y. Poullet, "The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the importance of Privacy for Democracy", in S. Gutwith; Y. Poullet; P. De Hert; C. de Terwangne & S. Nouwt, *Reinventing Data Protection* (Springen, 2009), 62–76.

394 Parliamentary Assembly's Resolution 1165 (1998), point 12.

When trying capture how the concept of privacy is constructed, there are several different angles to choose from. Quite commonly privacy is explained by distinguishing the four elements it consists of. These four elements are the rights to a private life, family life, home and correspondence.[395] When taking a closer look at these four elements, it is easy to note that they have strong similarities with the European Convention on Human Rights.

For a long time, the right to privacy was closely connected to the protection of family life and all four previously-mentioned elements seem to have quite clear relations to family life. Article 8 of the European Convention on Human Rights goes as follows:

> *"Right to respect for private and family life*
>
> 1. *Everyone has the right to respect for his private and family life, his home and his correspondence.*
>
> 2. *There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."*

When the European Convention on Human Rights was negotiated, the protection of privacy was still quite clearly connected to a certain sphere, namely the home. Even today, individuals' right to privacy is not considered indispensable when in public places. An example of this is provided by the practice developed in the United States, where reasonable expectations have been used as a measurement when assessing whether there is an infringement of one's privacy.[396] Clearly, individuals' expectations cannot be the same in public places as in their private gardens. However, this doctrine allows the scope of reasonable expectations to be narrowed from public places to relatively private areas as well, such as changing rooms etc., by a simple notification of the surveillance. Also, due to the technical developments, even one's own garden does not seem to be as in the private sphere as it used to be; videotaping streetview cars might pass by any time.[397] Not to mention the most

395 H. Snijders, "Privacy of Contract", in Ziegler *Human Rights and Private Law* (Hart, 2007), 105– 116.

396 J.Q. Whitman "The Two Western Cultures of Privacy: Dignity versus Liberty" in *Yale Law Journal* 113(2004), 1162.

397 See also H. Nissenbaum, *Privacy in context – Technology, Policy, and Integrity of Social Life*, (Stanford University Press, 2010) 22–25, 51–53.

current cause of privacy dilemmas, drones. It has been rightly noted, that the non-normative approach of the reasonable expectation doctrine does not necessarily guarantee sufficient protection for individuals as the reasonable expectations might vary significantly depending on the place. For instance, the notification of video surveillance would lower the degree of the reasonable expectation, yet the right to privacy should not be deprived of individuals solely based on such notice.[398] Even if the doctrine of reasonable expectations alone might not provide an answer to the question of whether there is a breach of privacy, this doctrine provides an additional tool when assessing whether one's personal data can be disclosed. This will be elaborated in more detail in the concluding chapter.

When trying to gain a deeper understanding of the privacy rights in the ECHR context, one should take note of the case-law and also some of the Council of Europe's instruments. Unfortunately, the European Court of Human Rights has not given a universal definition of privacy. In its case-law, the right to privacy has been examined from many different angles, but one, clear and unambiguous definition is still missing.[399] Instead, the Parliamentary Assembly of the Council of Europe have defined privacy in one of its resolutions. Later, the Parliamentary Assembly confirmed its earlier definition by repeating it in its Resolution 1165 (1998). The Parliamentary Assembly stated that privacy is *the right to live one's own life with a minimum of interference*. Quite interestingly, the Parliamentary Assembly also noted that the right to control the use of one's own personal data should be included in this definition. Besides giving obvious recognition to the protection of personal data, the Parliamentary Assembly's resolution quite interestingly sets weight on self-determination. This is particularly interesting as the theory of informational self-determination was not generally accepted in most of the Council of Europe's member states at that time, according to Van Hocke & Dhont.[400] While this resolution might offer valuable guidance when framing privacy, due to its unbinding nature, that is all it can offer.

When trying to capture privacy rights in European terms, the Charter of Fundamental Rights must also be taken into consideration. The Charter states that "*everyone has the right to respect for his or her private and family life, home and communications*". The wording of Article 7 of the Charter is almost identical to the first indent of the European Convention on Human Rights.[401] The similarities are

398 A. Rouvroy & Y. Poullet, "The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the importance of Privacy for Democracy", in S. Gutwith; Y. Poullet; P. De Hert; C. de Terwangne & S. Nouwt, *Reinventing Data Protection* (Springen, 2009), 45–76.

399 H. Snijders, "Privacy of Contract", in Ziegler *Human Rights and Private Law* (Hart, 2007), 105–116.

400 M. Van Hoecke & J.Dhont, Obstacles and Opportunities for the Harmonisation of Law in Europe: Case of Privacy, in V. Heiskainen & K.Kulovesi (ed.) *Function and Future of European Law*, (Helsinki, 1999), 128.

401 Article 7 Respect for Private and Family Life; Everyone has the right to respect for his or her private and family life, home and communications.

not coincidental. When the Charter of Fundamental Rights was negotiated, the aim was to align the formulation of the provisions of the Charter with the Convention. This was to avoid the danger of contradictory interpretation of the fundamental rights by the two European courts.[402]

An attempt to define privacy has also been made in academic literature. For example, Trudel formulates privacy as follows "*Logically, not everything about an individual belongs to his or her private life. The right to privacy concerns information that affects an individual's independence and ability to exercise control over information concerning intimate relationship and life choices. However, as soon as an individual does things that concern others, his or her private life is necessarily constrained by their legitimate interests*".[403] This is quite a clever way to put it. First the information which should fall under the scope of privacy is described; the information which affects an individual's independence. Second, an indication of how the right to privacy can be exercised on a practical level is given. This is by exercising control over the information. Trudel's description of privacy reveals an element mentioned earlier when discussing the Parliamentary Assembly's Resolution, namely self-determination. Whitman, Professor of Comparative and Foreign Law at Yale, sees this feature as being very characteristic of European privacy thinking, and also an aspect differentiating it from American privacy thinking.[404] This is also a point of great interest when taking a look at the protection of personal data, which is a very European fundamental right, and which sets an increasing weight on the aspect of self-determination as I will argue later.[405] Finally, returning to the third element of Trudel's definition of privacy, this could be considered even the most significant aspect of the formulation. It frames the logical barriers of privacy; things that concern others.

Besides numerous definitions of privacy, it has also been identified through its scope. For example, the following elements have been described as forming a part of the concept of privacy. The first element is "*control over the gathering, storage, use and dissemination by the state or others of one's identifying features or personal information*".[406] All the activities mentioned in this formulation also fall quite clearly

402 See for example EU Charter of Fundamental Rights, Why the Charter of Fundamental Rights exists, available on the internet < http://ec.europa.eu/justice/fundamental-rights/charter/index_en.htm> [last visited 20.3.2017].

403 P. Trudel, "Privacy Protection on the Internet: Risk Management and Networked Normativity", in S. Gutwith; Y. Poullet; P. De Hert; C. de Terwangne & S. Nouwt, *Reinventing Data Protection* (Springen, 2009), 317–334.

404 J.Q. Whitman "The Two Western Cultures of Privacy: Dignity versus Liberty" in *Yale Law Journal* 113(2004), 1161,1196–1202.

405 For informational self-determination in European privacy thinking, see also M. Van Hoecke & J. Dhont, Obstacles and Opportunities for the Harmonisation of Law in Europe: Case of Privacy, in V. Heiskainen & K. Kulovesi (ed.) *Function and Future of European Law*, (Helsinki, 1999), 128–129.

406 A. Ieven, "Privacy Rights in Conflict: In Search of the Theoretical Framework behind the European Court of Human Rights' balancing of private life against other rights", in E. Brems (ed.), *Conflicts between Fundamental*

under the definition of the processing of personal data. Furthermore, the described information falls under the definition of personal data. Therefore, this element seems clearly to indicate the processing of one's personal data. However, this does not mean that considering this as a part of privacy would be somehow incorrect. The second element is "*control over features of one's identity and self- expression through one's names, titles, physical appearance, life-style, marital status and gender identity*".[407] Apart from lifestyle, these features fall under the definition of personal data. And also, depending of the context, lifestyle could be considered personal data as well. The third element is "*physical, moral, psychological and sexual integrity*".[408] The third element begins to diverge from the definition of personal data, even if depending on the context these elements could also be considered personal data. The fourth and fifth elements are more clearly on the solid ground of privacy alone: "*well-being in the sense of freedom from (environmental) nuisance*" and "*decisional freedom of self-determination regarding questions concerning sexuality, pregnancy and the end of life*".[409] The aim is not to form an exhaustive and solid picture of the scope of privacy through these elements. However, they do illustrate how the protection of one's personal data can be considered a part of privacy. It will later be discussed whether privacy can be seen as part of data protection as well, but it seems clear that even if the protection of one's personal data has recently gained an independent status as fundamental right, it still cannot be entirely separated from privacy. Gloria González Fuster argues correspondingly that even if the CJEU has separated privacy and data protection in some of its judgments, the CJEU does not, *de facto*, make a clear difference between the said rights in its reasoning, but rather returns to stress the element of privacy when stating reasons for the infringement.[410]

The different ways to approach the concept of privacy have now been examined and it was noted that there does not seem to be a clear way to define it. How the content of privacy should be interpreted in the context of the European data protection regime has not been unambiguously defined either. Next, this issue will be elaborated further.

Rights (Intersentia, 2008), 40. It ought to be noted that this evaluation has been given in the context of the scope of article 8 of the European Convention on Human Rights.

407 A. Ieven, "Privacy Rights in Conflict: In Search of the Theoretical Framework behind the European Court of Human Rights' balancing of private life against other rights", in E. Brems (ed.), *Conflicts between Fundamental Rights* (Intersentia, 2008), 40.

408 Ibid.

409 Ibid; for decisional privacy, see B. van der Sloot, "Decisional privacy 2.0: the procedural requirements implicit in article 8 ECHR and its potential impact on profiling" in *International Data Privacy Law* 7 (2017).

410 G. González Fuster, "Fighting For Your Right to What Exactly? The Convoluted Case Law of the EU Court of Justice on Privacy and/or Personal Data Protection" in *Birbeck Law Review*, 2(2) (2014), 263–278; G. González Fuster & R. Gellert, "The fundamental right of data protection in the European Union: in search of an uncharted rights" in *International Review of Law, Computers & Technology* 1(2012), 73–81. See also O. Lynskey, *The Foundations of EU Data Protection Law*, (Oxford, 2015) 132–135.

1.2 DATA PROTECTION AS AN INDEPENDENT FUNDAMENTAL RIGHT

It is clear from the outset that data protection has a very intimate relationship with privacy. As previously discussed, it was long considered a part of privacy in the field of fundamental rights. Sometimes it is even referred to as data privacy.[411] In other words, heavy weight on the protection of one's privacy has been given when data protection has been balanced with other fundamental rights.[412]

Data protection has become an individual fundamental right very recently. This transformation stems from the different developments in the EU's legislative framework and also from Court practice. Thereby, it has now gained the necessary institutional recognition.[413]

In Europe the recognition of data protection as a fundamental right took place at the latest when the Charter of Fundamental Rights of the European Union entered into force 1 December 2009.[414] The Charter clearly distinguishes the protection of personal data from the right to privacy. In other words, the right to the protection of personal data is now clearly laid down in Article 8 of the Charter and the right to privacy in its separate Article 7. This is a significant step forward, as the Charter clearly stipulates that personal data has an independent value in the field of fundamental rights. Article 8 states that "

1. *Everyone has the right to the protection of personal data concerning him or her.*

2. *Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.*

3. *Compliance with these rules shall be subject to control by an independent authority."*

411 S.Greenstein, *Our Humanity Exposed – Predictive Modelling in a Legal Context*, (Stockholm University, 2017) 258–263.

412 See for example case C-28/08P, *Bavarian Lager*, ECLI:EU:C:2010:378.

413 Article 8 of the Charter of Fundamental Rights; for institutional support, see Chapter I section 1.1. and in particular Dworkin, *Taking Rights Seriously*, (Duckworth 1977) 39–45, 64–68.

414 See for example EU Charter of Fundamental Rights, How the Charter became part of the EU Treaties, available on the internet < http://ec.europa.eu/justice/fundamental-rights/charter/index_en.htm> [last visited 20.3.2017]. See also comments on the reluctance for using the term privacy in the data protection legislation, I.Lloyd, "From ugly duckling to Swan. The rise of data protection and its limits", in *Computer Law and Security Review* 34 (2018), 780. See also O. Lynskey, *The Foundations of EU Data Protection Law*, (Oxford, 2015) 89–129.

As data protection has grown from the privacy right, it is natural that earlier case-law and also academic literature has underlined this aspect of data protection and often examined data protection from this angle. The umbilical cord is strong in this case, and more recent case-law is still very closely attached to this relationship.[415] Although the CJEU treats data protection as an individual fundamental right, it has not spelled out the distinctive features of data protection as Gloria González Fuster notes.[416] The CJEU has left the essence of data protection obscure and has often treated it together with the right to privacy. For example, in the so-called Data Retention judgment, the court does indeed give an independent status to data protection. It specifically states that retention of the said data has to be in line with Article 8 of the Charter. However, the Court's argument throughout the case keeps privacy and the protection of personal data very much hand in hand. The Court underlines that the content of the communication was not to be retained, but rather the information covered by the Data Retention Directive related to, for example, the source of the communication. Such data as date, time duration, calling telephone number and IP address had to be retained. The Court stressed in its reasoning that by combining this information, a very detailed information of a person's private life might be revealed. Thus, in the end, the CJEU's reasoning sets a heavy weight on the interference with one's privacy.[417] Privacy and data protection might have been treated together, but the CJEU did give data protection a specific and independent recognition. In earlier case-law the CJEU would only underline the right to privacy in the context of reconciling fundamental rights, even when the focus of the case was on the processing of personal data.[418] Finally, the Court concludes that the Data Retention Directive is invalid because it "*does not lay down clear and precise rules*

415 For an analysis of the CJEU's case-law on the concepts of privacy and data protection, see also M. Brkan, The Court of Justice of the EU, privacy and data protection: Judge-made law as a leitmotif in fundamental rights protection, in Brkan, M. & E. Psychogiopoulou (ed.) *Courts, Privacy and Data Protection in the Digital Environment*, (Edward Elgar, 2017), 10–31; G. González Fuster, "Fighting For Your Right to What Exactly? The Convoluted Case Law of the EU Court of Justice on Privacy and/or Personal Data Protection" in *Birbeck Law Review*, 2(2) (2014), 263–278; G. González Fuster & R. Gellert, "The fundamental right of data protection in the European Union: in search of an uncharted rights" in *International Review of Law, Computers & Technology* 1(2012), 73–81. See also O. Lynskey, *The Foundations of EU Data Protection Law*, (Oxford, 2015) 132–135.

416 G. González Fuster, "Fighting For Your Right to What Exactly? The Convoluted Case Law of the EU Court of Justice on Privacy and/or Personal Data Protection" in *Birbeck Law Review*, 2(2) (2014), 263–278; G. González Fuster & R. Gellert, "The fundamental right of data protection in the European Union: in search of an uncharted rights" in *International Review of Law, Computers & Technology* 1(2012), 73–81.

417 Joined cases C-293/12 and C-594/12 *Digital Rights Ireland and Kärtner Landesregierung*, ECLI:EU:C:2014:238, paras 26–30, 65. See also T. Ojanen, "Privacy Is More Than Just a Seven-Letter Word: The Court of Justice of the European Union Sets Constitutional Limits on Mass Surveillance: Court of Justice of the European Union, Decision of 8 April 2014 in Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others, Participation and Democracy" in *European Law and Polity* 3 (2014), 528–541 and M. Brkan, The Court of Justice of the EU, privacy and data protection: Judge-made law as a leitmotif in fundamental rights protection, in Brkan, M. & E. Psychogiopoulou (ed.) *Courts, Privacy and Data Protection in the Digital Environment*, (Edward Elgar, 2017), 14–15.

418 Case C-275/06, *Promusicae*, ECLI:EU:C:2008:5, para 65.

governing the extent of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter". In other words, the interference should be justified from both the data protection and privacy perspective. This judgment pushed many national stakeholders to give further interpretation on how this is to be interpreted in the national context.[419] For example in Finland, the Constitutional Committee in the Parliament developed its earlier approach further by stating that the type of data which was previously considered to be on the outskirts of the right to data protection (location data) was now coming closer to the hard core of the said right.[420]

Even if privacy is still very apparent when assessing data protection, some authors have underlined that data protection is not simply a question of informational privacy, but also of informational autonomy.[421] This is an issue which will be examined in more detail later in this chapter when self-determination is discussed. In this context, it suffices to note that I see that informational autonomy cannot be lightly separated from privacy rights. Therefore, this thesis does not try to entirely separate data protection from privacy. The aim is rather to underline the specific features of the protection of personal data and elaborate further the said relationship by distinguishing underlying principles, aims and objectives, which are characteristic to the protection of personal data.

Besides dissatisfaction with the CJEU's way of treating the rights together even when underlying the status of data protection as fundamental right[422], the separation of data protection from privacy rights has been considered somewhat unsatisfying for other reasons. These concerns are drawn from the fear that once removed from the sphere of the privacy, the underlying values of dignity and autonomy might fade out with time.[423] It might well be that practical lawyers who work with data protection issues and solve very technical questions would not speculate on these values on a daily basis. For instance, the Data Protection Directive refers to the aim of the protection of privacy while values of dignity and autonomy are not

419 See for example in Denmark 2.6.2014, "Justitsministeren ophæver reglerne om sessionslogning", available on the internet < http://justitsministeriet.dk/nyt-og-presse/pressemeddelelser/2014/justitsministeren-oph%C3%A6ver-reglerne-om-sessionslogning> [last visited 3.11.2015]; For legality of the Data Retention Directive, see also, L. Feiler, "The Legality of the Data Retention Directive in Light of the fundamental Rights to Privacy and Data Protection " in *European Journal of Law and Technology* 3 (2010).

420 PeVL18/2014 vp, p. 6.

421 See M. Tzanou, *The Added Value of Data Protection as a Fundamental Right in the EU Legal Order in the Context of Law Enforcement*, (EUI, 2012) 22.

422 G. González Fuster, "Fighting For Your Right to What Exactly? The Convoluted Case Law of the EU Court of Justice on Privacy and/or Personal Data Protection" in *Birbeck Law Review*, 2(2) (2014), 263–278; G. González Fuster & R. Gellert, "The fundamental right of data protection in the European Union: in search of an uncharted rights" in *International Review of Law, Computers & Technology* 1(2012), 73–81.

423 See for instance A. Rouvroy & Y. Poullet, "The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the importance of Privacy for Democracy", in S. Gutwith; Y. Poullet; P. De Hert; C. de Terwangne & S. Nouwt, *Reinventing Data Protection* (Springen, 2009), 45–76. For an analysis of protection of personal data turning into a fundamental right, see also M. Brkan, "The Unstoppable Expansion of the EU Fundamental Right to Data Protection: Little Shop of Horrors?" in *Maastricht Journal of European and Comparative Law*, 23 (2016).

mentioned. Furthermore, Rodotà questioned whether this general assumption is convincing as there are clearly increasing demands for data disclosure due to several different factors. These are, for example, security requirements, market interests and reorganization of the public sector[424]. Nevertheless, Rodotà does conclude, that "*the strong protection of personal data continues to be a 'necessary utopia*'".

Regardless, I see that the status as an independent fundamental right is rather a victory than a loss for the protection of personal data, and in particular for the underlying values of data protection. Clearly, this progress should have an effect when balancing data protection with other fundamental rights. Previously, data protection has been balanced with other fundamental rights as an element of privacy. This has led to situation where the focus in the reconciliation has been on ensuring that data subject's privacy is not infringed. This is still an essential aspect of data protection and it cannot be overlooked. However, there are also other aims and underlying principles for data protection. These other aims and principles should be given more weight and should now become more significant in the balancing exercise. An example of such an underlying principle would be good governance. To conclude, the balancing should not be based solely on the assessment of whether there is an infringement of privacy rights, as it has been previously.

1.2.1 PRIVACY AS A PART OF DATA PROTECTION OR DATA PROTECTION AS A PART OF PRIVACY

It has now been established that data protection originated and diverged from privacy rights. Yet, the question of whether data protection should be considered a part of privacy, or privacy a part data protection, is still stimulating interesting discussions.[425]

The origin of data protection, the aim to protect individual's privacy, is strongly present in the early European data protection instruments. They stress the importance of the protection of privacy when processing personal data.[426] Even

424 S. Rodotà, "Data Protection as a Fundamental Right" in S. Gutwith; Y. Poullet; P. De Hert; C. de Terwangne & S. Nouwt, *Reinventing Data Protection* (Springen, 2009), 77–82.

425 See for example P. De Hert & S. Gutwirth, "Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalisation in Action", in S. Gutwith; Y. Poullet; P. De Hert; C. de Terwangne & S. Nouwt, *Reinventing Data Protection* (Springen, 2009), 6; D. Manolescu, "Data Protection Enforcement: The European Experience – Case Law", in N. Ismail & E.L. Yong Cieh (eds.), *Beyond Data Protection* (Springer, 2013), 217–220. See also G. González Fuster, "Fighting For Your Right to What Exactly? The Convoluted Case Law of the EU Court of Justice on Privacy and/or Personal Data Protection" in *Birbeck Law Review*, 2(2) (2014), 263–278; G. González Fuster & R. Gellert, "The fundamental right of data protection in the European Union: in search of an uncharted rights" in *International Review of Law, Computers & Technology* 1(2012), 73–81.

426 For instance, according to Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data, Article 1, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data. Also Regulation 45/2001 on the protection of individuals with regard to the processing of

though this is the case, it has been quite correctly noted that data protection is not merely an angle of the protection of privacy. The scope of data protection can also be seen as wider than the one of privacy, and at the same time more specific. The scope can be seen as wider, because data protection also relates to other fundamental rights besides privacy. And it can be considered more specific, because it is limited to the processing of personal data. While more specific, at the same time, the scope is also considered broader as all processing of personal data is under its scope,[427] not only personal data relating to one's privacy. Next, these statements will be examined further.

It is correctly said, that data protection covers all processing of personal data, not only processing that is assumed to interfere with one's privacy. This is strongly related with one of the differences between these two concepts, namely the more specific nature of data protection. It has been noted[428] that data protection is more specific as it only relates to processing of personal data. If this argument is taken on a more concrete level, it is rather facile to observe that data protection regulation is more detailed and therefore more specific. The European data protection framework consists of several different sets of rules, such as the GDPR and the EU Institutions' Data Protection Regulation while privacy legislation consists of some clear statements, which could be considered principles as well. While data protection rules have initially been drawn up to safeguard individuals' privacy when processing their personal data, individuals' privacy is not necessarily in danger in all circumstances covered by these rules. While it is fairly safe to conclude that European data protection regulation is precisely what Dworkin and Alexy intend with rules, this is not as clear in terms of privacy regulation. The statements defining the right to privacy could be considered principles as well.

It was previously established that contrary to principles, rules apply in all-or-nothing manner. Once officials have identified which rules are to be applied in the said case, those rules will be applied. The public authority applying these rules is not entitled to discretion, unless there is a particular reason for it. Thus, the official applying data protection regulation is not supposed to balance the rules and consider whether there is actual danger of interference with someone's privacy, if the rule clearly applies and there are no specific reasons to derogate from this. The specific reasons could be, for instance, competing rules or an exception to the main rule.

---

personal data by the Community institutions and bodies and on the free movement of such data contains corresponding article as does the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

427 See for instance P. De Hert & S. Gutwirth, "Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalisation in Action", in S. Gutwith; Y. Poullet; P. De Hert; C. de Terwangne & S. Nouwt, *Reinventing Data Protection* (Springen, 2009), 4,11.

428 P. De Hert & S. Gutwirth, "Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalisation in Action", in S. Gutwith; Y. Poullet; P. De Hert; C. de Terwangne & S. Nouwt, *Reinventing Data Protection* (Springen, 2009), 6.

However, it should not be assumed that these rules are depart entirely from privacy. Instead, privacy should be considered an underlying principle for these rules. It follows that as long as these rules are applied, and no contradictions arise, the question of the protection of one's privacy does not seem to have an effect on how the rules are applied. However, once hard cases arise and a solution must be sought from the underlying levels of law, privacy becomes relevant and it must be balanced with other underlying principles. Thereby, it appears that even if data protection regulation also seemingly covers such processing of personal data where one's privacy is not directly at stake, the connection to privacy still exists in the underlying layers of law.

Furthermore, even if the scope of data protection can be considered wider than privacy in a certain respect, the protection of one's privacy does cover sectors that are not covered by data protection. Nevertheless, it is fruitless to continue this discussion further. I suggested that privacy is one of the underlying principles of data protection. In this context, it is essential to note that as an independent fundamental right, data protection might also have other underlying principles or aims and objectives which create the circumstances of the case. I argue that these other elements should gain increasing importance when balancing the right to protection of personal data with other rights, precisely because of data protection's nature as an independent fundamental right. While privacy is still a highly significant element in the data protection regime, data protection is slowly and firmly departing from its roots. In this context, it should be borne in mind that detailed data protection regulation does have aims and objectives. In other words, there would be no reason to make detailed data protection legislation just for the sake of it.

1.2.2 PERSONAL DATA AS AN ECONOMIC ASSET

The discussion of privacy, personal data and self-determination, which will be shortly analyzed in more detail, would not be complete without some remarks related to the economic value of personal data. This is particularly interesting as personal data is turning into an extremely valuable asset in economic terms and, in many ways, the development of modern society seems to be clearly linked with the ways in which personal data can or may be processed.

It has been suggested that individuals would have the right to their own personal information as an economic asset.[429] This doctrine seems to draw its justification from the data subject's right to self-determination and autonomy. If this doctrine

429 See for instance A. Rouvroy & Y. Poullet, "The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the importance of Privacy for Democracy", in S. Gutwith; Y. Poullet; P. De Hert; C. de Terwangne & S. Nouwt, *Reinventing Data Protection* (Springen, 2009), 45–76.

is set in the context where commercial actors sell massive amounts of personal data for numerous different purposes, it would indeed seem quite appropriate to argue that personal data is an economic asset of the person to whom it relates.[430] Of course, in such a scenario the time, effort and other investments that the controller might have made in this "product" would be disregarded.

Furthermore, once it has been established that data protection is an independent fundamental right, we are bound by the basic characteristics of human rights. The idea of one selling their personal data seems slightly problematic from the fundamental right angle.[431] This is particularly interesting as this might not be perceived similarly in non-European countries. It appears to be a very European approach that a certain extent of self-determination would remain on the person even when there has been an economic gain for that person.[432] Furthermore, data subjects do not own their personal data in a sense that they could freely deliberate how to use it.[433]

1.3 SELF-DETERMINATION AS A PART OF PRIVACY AND DATA PROTECTION

This chapter first examined different definitions and characteristics of privacy rights. This was followed by an analysis of data protection. Before engaging in a more detailed discussion of data protection's different elements and provisions, self-determination is addressed in this section. Self-determination is closely linked with both privacy and data protection. It therefore seems rational to discuss all three of these concepts simultaneously.

Some authors have argued that the right to privacy, and also to data protection, are means to obtain other goals and to realize the underlying values of privacy, rather than the goals themselves. This conclusion is drawn from German legal practice.[434] The German Constitutional Court gave a landmark decision in the 1980s in which

430 See also for instance N. Barber "A Right to Privacy" in Ziegler *Human Rights and Private Law* (Hart, 2007), 67 – 77.

431 See also for instance S. Rodotà, "Data Protection as a Fundamental Right" in S. Gutwith; Y. Poullet; P. De Hert; C. de Terwangne & S. Nouwt, *Reinventing Data Protection* (Springen, 2009), 77–82. He concludes that "*the right to data protection has to do with protecting one's personality, not one's property*".

432 J.Q. Whitman "The Two Western Cultures of Privacy: Dignity versus Liberty" in *Yale Law Journal* 113(2004), 1198.

433 P. De Hert & S. Gutwirth, "Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalisation in Action", in S. Gutwith; Y. Poullet; P. De Hert; C. de Terwangne & S. Nouwt, *Reinventing Data Protection* (Springen, 2009), 3. See also for instance Case C-524/06 *Heinz Huber*, ECLI:EU:C:2008:724.

434 A. Rouvroy & Y. Poullet, "The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the importance of Privacy for Democracy", in S. Gutwirth; Y. Poullet; P. De Hert; C. de Terwangne & S. Nouwt, *Reinventing Data Protection* (Springen, 2009), 45–76.

it underlined the importance of informational self-determination.[435] Hence, the underlying aim referred to by some authors is self-determination.

The German Constitutional Court has stressed two elements of self-determination; human dignity and self-development. These elements were later elaborated on in academic literature.[436] While the importance of the said values has been underlined, it has simultaneously been acknowledged that the right to self-determination cannot be considered absolute.[437]

As it has come out earlier, privacy has traditionally been considered as the cornerstone of the data protection legislation. However, I argue that self-determination is gaining increasing importance and a more independent role in the data protection framework. Many of the new provisions put forward by the European Commission in its proposal for the General Data Protection Regulation stemmed precisely from self-determination.[438] For example, data portability and the right to be forgotten reflect this underlying aim or principle of data protection. Besides the new provisions introduced by the Commission's proposal, some of the existing elements reflecting self-determination did gain more importance or stronger status in the Commission's proposal and in the GDPR as it was adopted. An example of this would be consent. The Commission's proposal did set quite detailed requirements for the fulfillment of consent.

When analyzing this development, an essential element which needs to be recognized is the increasing role of social media. The new data protection provisions support the argument of the increasing role of self-determination in the data protection framework. Furthermore, I see that social media and the internet environment offer the explanation for the need to strengthen self-determination in the said framework. In this new environment, self-determination has a very different role than in a more traditional, register-based data protection framework. When the data subject him or herself is the active source of the personal data, and also in some cases the controller or processor of the said data, it seems quite rational

435 Judgment by the German Constitutional Court, BVerfGE 65, 1 (15 December 1983).

436 A. Rouvroy & Y. Poullet, "The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the importance of Privacy for Democracy", in S. Gutwirth; Y. Poullet; P. De Hert; C. de Terwangne & S. Nouwt, *Reinventing Data Protection* (Springen, 2009), 45–76.

437 A. Rouvroy & Y. Poullet, "The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the importance of Privacy for Democracy", in S. Gutwith; Y. Poullet; P. De Hert; C. de Terwangne & S. Nouwt, *Reinventing Data Protection* (Springen, 2009), 45–76. See also for instance Case C-524/06, *Heinz Huber*, ECLI:EU:C:2008:724.

438 See Articles 7, 17, 20 of the Regulation (EU) No 679/2016 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) (OJ L 119, 4.5.2016, p. 1–88). For similar comments, see also W.Li, "A tale of two rights: exploring the potential conflict between two rights to data portability and right to be forgotten under the General Data Protection Regulation" in *International Data Privacy Law* 8 (2018), 316. See also O. Lynskey, *The Foundations of EU Data Protection Law*, (Oxford, 2015) 229–272.

that an objective such as self-determination is gaining more significance and a separate role from privacy.

After establishing that self-determination is gaining increasing importance in the European data protection regime, the next step is to define the tentative dimensions of self-determination in the data protection context.[439]

From the outset, the notion of self-determination seems quite self-explanatory, but there is more to it. One angle of self-determination to examine is to separate the control over producing data from the control over existing personal data. I argue that when personal data is produced by the data subject themselves, there is more ground to set weight on self-determination. I argue that this is also the element from which self-determination's divergence from privacy stems. When the data subject is producing the data and controlling its processing, data subjects' rights are protected as far as the data subject has control over the data.

It has been noted though that the right to self-determination should not be perceived as one's right to somehow control or manipulate the information about oneself.[440] This is why "self" should be separated from the information. Furthermore, it has been argued that self-determination does not imply that data subjects would have "ownership" rights over their own personal data.[441]

Even if self-determination can be seen as part of privacy and it was argued that privacy is an underlying principle of data protection, it would be false to claim that there is always a data subject's privacy at stake when self-determination plays a part in the data protection field. An example of this would be data portability as proposed by the European Commission and later adopted in the General Data Protection Regulation.[442] The core of data portability is the right to move your own personal data from one system to another. This personal data could be, for example, on Facebook and the data subject[443] might have shared this information with hundreds if not thousands of followers on Facebook. In other words, the personal information might not be private in its nature at all. The concrete goal in this respect seems to be to give the data subject control over his or her own personal data. Therefore,

439 For autonomy and self-determination in different forms of democracy, see J. Habermas, *Between Facts and Norms*, (The MIT Press, Cambridge, Massachusetts, 1996), 82–118.

440 This is an argument which might need to be redeveloped in light of the Google v Spain judgment, Case C-131/12, *Google Spain and Google Inc*, ECLI:EU:C:2014:317. Self-determination has also been assessed in the context of protection of personal data and public access to documents as a part of right of public access, see T. Pöysti, *Tehokkuus, informaatio ja eurooppalainen oikeusalue*, (Helsinki, 1999) 478.

441 See A. Rouvroy & Y. Poullet, "The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the importance of Privacy for Democracy", in S. Gutwith; Y. Poullet; P. De Hert; C. de Terwangne & S. Nouwt, *Reinventing Data Protection* (Springen, 2009), 51.

442 Proposal for a Regulation of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM (2012) 11 final, p. 9, 26, 38 and 53.

443 The data subject could be considered a processor in such a situation. For waiving the right to privacy, see K. Hughes, "A Behavioural Understanding of Privacy and its Implications for Privacy Law" in *The Modern Law Review* 75(5) (2012), 820.

privacy and self-determination are considered as separate aims or principles of data protection in this thesis.

1.4 DATA PROTECTION IN TERMS OF DEMOCRACY

After having discussed the different viewpoints of data protection as an independent fundamental right, it is also essential to view how data protection comes together with democracy. In this assessment, privacy as an underlying principle of data protection is of particular interest.

The relationship between transparency and democracy[444] was examined earlier and it was concluded that transparency is a prerequisite for well-functioning democracy. According to some[445] privacy can also be considered a prerequisite or at least an element of democratic society and, for instance, of the freedom of speech. The connection between privacy and democracy is drawn from the assumption that in order to be able to form and freely express personal opinions, one should have privacy to develop and elaborate these thoughts.[446] If access to documents is inserted into this equation, we immediately notice, that without first having the relevant information, the meaning of privacy becomes void via-à-vis democracy. Thus, the opportunity to elaborate one's thoughts without interference is quite quickly rendered fruitless if one is not provided with sufficient information.

Even if there might be some grounds to consider privacy a prerequisite or an element of democracy, it still seems quite a far-fetched construction, in particular when this connection is assessed together with the right of access to documents. Given recent revelations on the big data solutions applied by Cambridge Analytica for targeted election campaigns, this discussion could be taken to another level with a particular interest in such data protection rules as profiling. However, from the outset, the core issue would seem to come back to what was said on the privacy to develop and elaborate one's thoughts.

In the context of the discussion on democracy and the protection of personal data, a closer look at the personal data of public figures must also be taken.

---

444 See Chapter III, section 1.2. More detailed analysis will follow in Chapter VII, subsection 2.1.1.1.

445 See for instance A. Rouvroy & Y. Poullet, "The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the importance of Privacy for Democracy", in S. Gutwith; Y. Poullet; P. De Hert; C. de Terwangne & S. Nouwt, *Reinventing Data Protection* (Springen, 2009), 45–76.

446 A. Rouvroy & Y. Poullet, "The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the importance of Privacy for Democracy", in S. Gutwirth; Y. Poullet; P. De Hert; C. de Terwangne & S. Nouwt, *Reinventing Data Protection* (Springen, 2009), 45–76. See also S. Greenstein, *Our Humanity Exposed – Predictive Modelling in a Legal Context*, (Stockholm University, 2017) 159–161.

1.4.1 PUBLIC FIGURES

It has now been established that expectations for one's right to privacy is not as high in public places. Also, the right to privacy of public figures is more restricted than the common man's. Public figures are those who are acting in one way or other in the public sphere. This might be due to their post, as is a case with representatives of the government, or they might be public figures for other reasons, like athletes and artists. The Parliamentary Assembly has defined public figures in its Resolution 1165 (1998) as persons holding public office and/or using public resources and, more broadly speaking, all those who play a role in public life, whether in politics, the economy, the arts, the social sphere, sport or in any other domain. However, the ECHR has taken a narrower approach to the definition of public figures in its judgment in Hannover v Germany.[447] The European Court of Human Rights stated that "*a fundamental distinction needs to be made between reporting facts – even controversial ones – capable of contributing to a debate in a democratic society relating to politicians in the exercise of their functions, for example, and reporting details of the private life of an individual who, moreover, as in this case, does not exercise official functions. While in the former case the press exercises its vital role of 'watchdog' in a democracy by contributing to impart[ing] information and ideas on matters of public interest, it does not do so in the latter case*". Some have argued that this distinction between public figures and average people, being essential for democracy, should also be recognized when applying data protection regulation.[448] This argument will be examined further in the concluding chapter.

Quite interestingly, it has also been noted that it seems that on some occasions the right to privacy has been extended to a right to "protection of personal life". The underlying idea of this is that not all elements falling in one's personal life should necessarily be considered private.[449] As concluded earlier, the right to control the use of one's own personal data is not absolute. Similarly, the right to privacy is not absolute.

447 ECtHR 24 June 2004, *Von Hannover v Germany* (2004–VI).

448 P. Trudel, "Privacy Protection on the Internet: Risk Management and Networked Normativity", in S. Gutwith; Y. Poullet; P. De Hert; C. de Terwangne & S. Nouwt, *Reinventing Data Protection* (Springen, 2009), 317–334.

449 P. Trudel, "Privacy Protection on the Internet: Risk Management and Networked Normativity", in S. Gutwith; Y. Poullet; P. De Hert; C. de Terwangne & S. Nouwt, *Reinventing Data Protection* (Springen, 2009), 320–321.

1.4.2 REASONABLE EXPECTATIONS

Rightful interference in one's privacy is sometimes measured with reasonable expectations. The reasonable expectations doctrine has evolved in the case-law of the European Court of Human Rights. Some authors have taken up the concept of "legitimate expectations" in their vocabulary when reasonable expectations are assessed. Even if reasonable expectations can serve as a useful tool when assessing the hard core of privacy rights, some have quite rightfully noted that such a tool might actually set the standards lower in the European legal framework.[450] When surveillance techniques are becoming available for the public at large and becoming more efficient, the standards of reasonable expectations might at the same time become lower.

2. CENTRAL DATA PROTECTION CONCEPTS

The previous section discussed the founding values of data protection. The latter part of this chapter will take the discussion to a more concrete level and focus on the core concepts and provisions of the European data protection framework. First, the most central data protection concepts will be elaborated. This will be followed by the discussion of some main elements of the data protection legislation.[451] After this, some sub-elements of data protection will be examined. The discussed concepts are the relevant elements vis-à-vis European transparency regulation. Lastly, some new data protection concepts developed in the renewed data protection framework and in particular in the context of the GDPR will be tackled.

The formulation of the most essential data protection concepts has not gone through a significant transformation since the Data Protection Directive entered into force more than 20 years ago.[452] This is also the case after 25 May 2018. One could think that over the past 20 years, the content of the core concepts would have stabilized. Yet, this is not the case. Even in the most recent cases tried before the Court or at the data protection authorities, the fundamental issue often culminates in the question of whether some activity should be considered processing of personal data at all. In other words, whether some information is personal data and secondly,

450 S. Nouwt, B.R. de Vries & R. Loermans, Analysis of the Country Reports, S. Nouwt, B.R. de Vries & C. Prins (eds.) *Reasonable Expectations of Privacy? Eleven Country Reports on Camera Surveillance and Workplace* Privacy, (Asser Press, 2005), 351–357.

451 These principles are different from Dworkin's and Alexy's principles, even if they might sometimes overlap. For Dworkin's and Alexy's principles, see Chapter I.

452 Directive 95/46/EC of the European Parliament and 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 (OJ L 281, 23.11.1995, p. 31–50).

whether the activities carried out with the data is to be considered processing or who is the controller.[453]

One of the factors causing continuous confusion with the fundamental concepts of data protection legislation is ever-developing technology. New innovations and evolution are constantly creating situations where a rather old regulatory framework should provide answers to new dilemmas. An already outdated example of this would be Google Street View and other similar services. One of the questions arising in this context was whether collecting and processing Street View pictures is processing personal data.[454]

The European legal framework was drawn in a technologically neutral way and has so far been able to answer the demands created by new technology.[455] The broad definition of personal data has been a central element in this development. When data is not to be considered personal data or the activities not considered processing personal data, the activity does not fall in the scope of the data protection legislation. This is the case even when such values as individuals' privacy is at stake. As the argumentation around data protection legislation often returns to these fundamental concepts, it is necessary to examine their content.

2.1 THE CONCEPT OF PERSONAL DATA

The scope of the concept of personal data constantly causes debate due to new technological innovations, which place this concept in areas not known to legislators when drafting data protection legislation decades before. An example of this is the CJEU's ruling where the Court decided that dynamic IP addresses can be considered personal data.[456] Clearly, defining the concept of personal data is also at the very core of this thesis as data protection legislation covers only the processing of personal data, not any other type of data.

453 See for example Case C-131/12, *Google Spain and Google Inc*, ECLI:EU:C:2014:317; case C-210/16, *Datenschutz Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein GmbH,* ECLI:EU:C:2018:388 and case C-25/17, *Tietosuojavaltuutettu*, ECLI:EU:C:2018:551; Joined cases C-141/12 and C-372/12, *YS e.a.*, ECLI:EU:C:2014:2081, paras 33–48; Case C-212/13, *Ryneš*, ECLI:EU:C:2014:2428. For allocation of responsibility, see also M. Brkan, "Data Protection and Conflict-of-laws: A Challenging Relationship" in *European Data Protection Law Review*, 2 (2016).

454 See for example Decision of Administrative Court of Helsinki 30.12.2011, dnro 01026/11/1204.

455 For technology neutral, see for example B-J. Koops, "Should ICT Regulation be Technology-Neutral?", in Koops, Lips, Prins & Schellekens (eds.), *Starting Points for ICT Regulation. Deconstructing Prevalent Policy On-Liners* (Asser Press, 2006); C. Reed, "Taking Sides on Technology Neutrality", in *SCRIPT-ed 4* 3(2007); B-J. Koops & JP Sluijs, "Network Neutrality and Privacy According to Art. 8 ECHR" in European Journal for Law and Technology 3 2(2012).

456 See C582/14, *Patrick Breyer v Bundesrepublik Deutschland*, ECLI:EU:C:2016:779.

2.1.1 CONVENTION 108, THE GDPR AND EU INSTITUTIONS' DATA PROTECTION REGULATION

The European legal framework provides many sources for capturing the concept of personal data. To start with, this concept has been defined in Convention 108[457] and in the former Data Protection Directive[458], as well as in the GDPR and EU Institutions' Data Protection Regulation.

In chronological order, Convention 108 defines personal data as *"any information relating to an identified or identifiable individual (' data subject')"*. The GDPR and EU Institutions' Data Protection Regulation defines personal data in turn as *"any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"*. The definition of personal data was essentially same as under the previous data protection regime. The GDPR does clarify an already existing concept of identifier in relation to personal data and provides some further examples of identifiers. Besides these specifications, there are further elements in the recitals of the GDPR clarifying the scope of the concept. For example, deceased people are expressly excluded from the scope.[459]

All the definitions provide a similar starting point; quite a wide definition of the concept of personal data.[460] The fact that the data subject does not need to be identified as far as he or she is identifiable, broadens the scope the concept significantly, as does the possibility to identify the person indirectly. Furthermore, it cannot be overlooked that protection of personal data is a fundamental right.[461] This sets certain limits for the restrictive interpretation of the said concept. The question of whether data is to be considered personal data, has arisen for instance in the following cases: sound records, deceased people, licence plates, the pictures captured by different Street View services, like Google, or written answers given in a professional examination.[462]

---

457 Convention 108 for the Protection of Individuals with Regard to Automatic Processing of Personal Data.

458 Directive 95/46/EC of the European Parliament and 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 (OJ L 281, 23.11.1995, p. 31–50).

459 See for example Council of European Union, 9565/15, Brussels, 11 June 2015, Recital 23(aa).

460 For the broad interpretation of data protection terminology, see D. Erdos "From the Scylla to the Charybdis of License? Exploring the Scope of the 'Special Purposes' Freedom of Expression Shield in European Data Protection" in *Common Market Law Review* 52 (2015), 121–123.

461 See for example joined cases C-92/09 and C-93/09 *Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen*, ECLI:EU:C:2010:662 and joined cases C-293/12 and C-594/12 *Digital Rights Ireland and Kärtner Landesregierung*, ECLI:EU:C:2014:238.

462 Case T-121/05, *Borax Europe v Commission,* ECLI:EU:T:2009:64; Decision of the Finnish Data Protection Board (tietosuojalautakunta) 4/2010, dnro 1/933/2010 and 4/932/2010; Decision of Administrative Court of

To frame the concept of personal data, different elements can be distinguished. A quite well-elaborated approach separates four aspects of the said concept.[463] The first element is "any information", the second element is "relating to", the third element is "identified or identifiable [natural person]" and the fourth element is "natural person".[464] These four elements will be examined next.

2.1.2 ANY INFORMATION

It is apparent that the notion of "any information" is indeed very broad.[465] The Article 29 Data Protection Working Party (WP 29, current EDPB) has provided some guidance on the interpretation of the said wording. WP 29 sees that "any information" covers both objective and subjective information, it covers opinions and statements of the data subject as well as false information. Furthermore, WP 29 sees that the position of the data subject does not have significance in the interpretation. In other words, information relating to persons acting in their professional capacity is personal data.[466] Objective information is probably the most typical type of personal data. An example of this would be someone's height or weight. This is also the type of information which can relatively easily be proven true or false. As WP 29 noted, information does not need to be correct to be considered personal data. It is easy to agree with WP 29 on this particular point; data protection legislation does contain different provisions providing the data subject with the right to rectify incorrect information.

The most intriguing analysis carried out by the WP 29 relates to subjective information. Subjective information would cover, for example, opinions and statements of the data subject. An analysis of an employee provides an example of subjective information. However, WP 29 does not take stand on a question of whether subjective information should also cover opinions and statements by the data subject. However, WP 29's quite far-reaching opinion stating that drawing can be considered personal data, because it reveals the mood of a child seems to indicate that opinions and statements by the data subject could also be considered personal data. Subjective information is evidently quite a challenging type of

Helsinki 30.12.2011, dnro 01026/11/1204; Decision of the Finnish Data Protection Board (tietosuojalautakunta) 2/2009, dnro 1/933/2008 and Case C-434/16, *Nowak*, ECLI:EU:C:2017:994.

463 Article 29 Data Protection working party, "Opinion 4/2007 on the concept of personal data", 01248/07/EN WP 136, p. 6–21.

464 Ibid.

465 For terms data and information, see D. Erdos "From the Scylla to the Charybdis of License? Exploring the Scope of the 'Special Purposes' Freedom of Expression Shield in European Data Protection" in *Common Market Law Review* 52 (2015), 121–123.

466 Article 29 Data Protection working party, "Opinion 4/2007 on the concept of personal data", 01248/07/EN WP 136, p. 6–7.

personal information. For example, a data subject's right to rectify information is quite demanding to execute when it comes to subjective information.

Besides the type of information, WP 29 has also drawn attention to the format of the information. It has clarified that the format does not have significance when assessing whether the information is to be considered personal data. The information could be alphabetical, numerical, graphical, photographic, acoustic etc., to be considered personal data.[467] This approach leans firmly on the CJEU's case-law and national practice adopted in the Member States. In the Borax case, the CJEU decided that voices on audiotapes are personal data. Also, the nature of numerical and photographical information was assessed by national data protection authorities in several Member States when Google Street View launched its service in Europe. An example of this would be the Fonecta case examined by the Finnish Data Protection Board. This service and collection of the data is very much like Google Street View. The service provider argued that the collected data was not personal data at all.[468] Contrary to the service provider's argument, the Board held that pictures of people are personal data and this was also the case regarding licence plate numbers. This decision was later held by the Court of Appeal.[469]

2.1.3 "RELATING TO"

European data protection legislation defines personal data as information *relating to* a natural person. The Charter of Fundamental Rights in turn states that everyone has the right to the protection of personal data *concerning* him or her. Different wording does not lead to contradiction here. The former defines personal data and the latter clarifies that the protection of personal data is the right of the data subject.

It suffices to note that with the reference "relating to", all information about the data subject is covered. WP 29 has specified "*that in order to consider that the data "relate" to an individual, a "content" element or a "purpose" element or a "result" element should be present*".[470] Wachter and Mittelstadt provide an intriguing analysis of the interpretation of the concept of personal data by the CJEU. A particular focus has been on information, which relates to the data subject, such as correction marks on an examination taken by the data subject.[471] Not entirely satisfied with the CJEU's general line of interpretation, the authors doubt in particular the CJEU's approach

467 Ibid.

468 Decision of the Finnish Data Protection Board (tietosuojalautakunta) 4/2010, dnro 1/933/2010 and 4/932/2010; Decision of Administrative Court of Helsinki 30.12.2011, dnro 01026/11/1204.

469 Ibid.

470 Article 29 Data Protection working party, "Opinion 4/2007 on the concept of personal data", 01248/07/EN WP 136, p. 12–15.

471 See Case C-434/16, *Nowak*, ECLI:EU:C:2017:994.

in the *YS e.a* case[472], where the data subject was not given full access to information related to him, but only to a summary of it.[473] The authors approach can be argued by the principle of good governance. However, when the definition of the scope of personal data is considered in very broad terms, it simultaneously widens the tension between public access to documents and protection of personal data. While the broad approach might ensure better data subject's rights in general, it could simultaneously lead to an unnecessary restriction of public access to documents.

2.1.4 IDENTIFIABLE

The third element of the concept of personal data is "identifiable". Someone is identifiable when this person can be distinguished from other persons. To meet the requirements laid down in European data protection legislation the person is either already recognized or, alternatively, it is *possible* to identify that person.[474]

To assess whether the person is identifiable, two elements should be taken into account. First, identification might take place in the future. Naturally, identification should be reasonably foreseeable. In other words, the endless possibilities of technological innovations do not suffice as such to make any information personal data. This is in particular the case when the information will not be stored for long period of time.

Second, identification does not need to happen directly. Identification might take place for instance when a particular piece of information is combined with other information. A decision by the Finnish Data Protection Board provides a practical example of this. The Board concluded in its decision[475] that licence plate numbers are personal data. In this particular case, the prospective data controller did not plan to have other information related to natural persons in its register.[476] However, this did not play a central element in the Board's assessment. The information needed for identification would have been easy to fetch from the nationwide register with very reasonable costs. Therefore, the Data Protection Board concluded that licence plate

472 Joined cases C-141/12 and C-372/12, *YS e.a.*, ECLI:EU:C:2014:2081.

473 S. Wachter & B.Mittelstadt "A Right to reasonable interference: Re-thinking data protection law in the age of big data and AI" in *Columbia Business Law Review* 2 (2019), 29–50.

474 Article 29 Data Protection working party, "Opinion 4/2007 on the concept of personal data", 01248/07/EN WP 136, p. 12.

475 Decision of the Finnish Data Protection Board (tietosuojalautakunta) 1/2010, dnro 2/932/2009. Borax had appealed Commission decision. Commission had refused to disclose audio tapes from a meeting held by Commission and experts and industry representatives in the chemicals' field. Commission had refused access to audio tapes based on articles 4(1)(b) and 4(3) of the Regulation 1049/2001.

476 For more detailed analysis of the concept of personal data by Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data.

numbers are personal data. Even if this decision is based on national legislation[477], several decisions and opinions taken by different data protection authorities in other EU Member States in Google Street View cases reflect a similar approach; in most cases Google is required to blur the licence plate numbers on its Street View service.[478]

Another example of indirect identification is provided by the General Court's decision in the Borax case.[479] In this case, the Commission had refused to grant access to audio tapes based on two grounds. Among other things, the Commission argued that the individuals on the audio tapes were identifiable even if their names were erased. Identification was possible as these particular individuals spoke different languages, had different accents and they made references to their national context in the course of the discussion. Even though the General Court annulled the Commission's decision, it did not differentiate from the Commission's interpretation of personal data. The General Court simply stated that it does not suffice to establish that the exception relating to the protection of personal data is applicable in principle, it also has to be satisfied that the disclosure of the document would concretely, not only hypothetically, undermine the interests protected by the related exception of the Transparency Regulation.

The examples provided in this section illustrate that the concept of personal data is very wide indeed; dynamic IP addresses, licence plate numbers and audio tapes without name references to the voices played on the tape are all personal data.

2.1.5 NATURAL PERSON

The fourth central element distinguished by WP 29 is "natural person". In other words, only natural persons have the right to the protection of their personal data. This excludes legal persons from the scope of the data protection legislation. Previously legal persons might have benefitted from data protection legislation indirectly in such cases where the data subject can be identified based on the information about the legal person. This would be the case for example when a company's name is derived from a natural person.[480] This did change when the

477 According to article 3(1) of the Finnish Personal Data Act, personal data means any information on a private individual and any information on his/her personal characteristics or personal circumstances, where these are identifiable as concerning him/her or the members of his/her family or household.

478 See for example Privacy & Information Security Law Blog, *Authorities in Austria and Switzerland Rule on Google Street View*, 3 May 2011, available on the internet < https://www.huntonprivacyblog.com/2011/05/03/authorities-in-austria-and-switzerland-rule-on-google-street-view/> [last visited 8.4.2017].

479 Case T-121/05 *Borax Europe v Commission,* ECLI:EU:T:2009:64.

480 Article 29 Data Protection working party, "Opinion 4/2007 on the concept of personal data", 01248/07/EN WP 136, p. 12. See also joined cases C-92/09 and C-93/09 *Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen,* ECLI:EU:C:2010:662.

GDPR become applicable in May 2018. The GDPR clarifies that legal persons are not in the scope of the Regulation.[481]

2.1.6 CONCERNS RAISED BY THE WIDE DEFINITION

The wide definition of personal data has raised some concerns. When among other things IP addresses are considered personal data, some have expressed fears that the concept is enlarging in a manner that will have serious consequences later.[482] Narrowing the concept of personal data could lead to unintended consequences at a later stage when new innovations not known today become part of everyday life, but these concerns cannot be overlooked. When nearly anything can be considered personal data, there is a risk of the controller's administrative burden becoming disproportionate when fairly insignificant personal data is being processed. As a practical example, one could mention drawings. If drawings are considered personal data on more general terms, this would mean that, for example, kindergartens should not hang children's drawings on the wall. Of course, parents' consent could be asked for this purpose, but even so, this cannot be in line with the aims and objectives of the European data protection legislation.

One could argue that if the incorporation of the so-called risk-based approach in the GDPR is later successfully applied, the concept of personal data can be broad. Appropriate measures to protect the personal data would then be adopted in line with the risks that the processing of personal data involves.[483]

The brief examination of the concept of personal data has given a clear picture of the broadness of the scope of the said concept. Personal data can be a wide variety of things: pictures, licence plates, audio tapes, IP addresses, even drawings and naturally also names, identification numbers etc. The given examples simply illustrate how wide the scope of the personal data is.

---

481 Regulation (EU) No 679/2016 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) (OJ L 119, 4.5.2016, p. 1–88), recital 14. Recital 14 clears that the GDPR "*does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person*".

482 See for example European Digital Rights, *Key aspects of the proposed General Data Protection Regulation explained: What are they? Why are they important? What are common misconceptions? What can be improved?*, available on the internet < https://edri.org/files/GDPR-key-issues-explained.pdf> [last visited 8.4.2017].

483 For the risk-based approach, see for example *The Risk-Based Approach in the GDPR: Interpretation and Implications* by Gabriel Maldoff, available on the internet <https://iapp.org/media/pdf/resource_center/GDPR_Study_Maldoff.pdfxx> [last visited 4.8.2018].

2.2 PROCESSING OF PERSONAL DATA

Similarly to the concept of personal data, processing of personal data has been broadly defined in the European legal framework. For the European data protection legislation to be applicable, the first requirement is that the data at stake is personal data. Thereafter, it must be assessed whether personal data is being processed. The personal data needs to be processed before the data protection legislation becomes applicable.

The former Data Protection Directive did define processing of personal data as follows: "*processing of personal data ('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction*". The approach adopted in the GDPR and in the EU Institutions' Data Protection Regulation follows this definition. The definition does provide some additional examples of processing, such as structuring and restriction. This does not, however, signify that the definition of processing would have been modified; the list is not exhaustive.

The requirements for processing of personal data are easily met. The broad definition of processing leads to a situation where nearly any activity carried out with personal data is to be considered processing and therefore in the scope of the European data protection framework.

2.3 DATA PROTECTION PRINCIPLES AND THE PURPOSE LIMITATION PRINCIPLE

Data protection principles are often considered the backbone of the data protection regime.[484] All processing of personal data must be carried out in accordance with the data protection principles. The Data Protection Directive did define six principles relating to data quality. These principles were derived from the European Data Protection Convention.[485] The data protection principles have been maintained in the GDPR. While the core idea has not changed, some differences in emphasis

484 See for instance S. K. Karanja, *Transparency and Proportionality in the Schengen Information System and Border Control Co-operation*, (Leiden, 2008) 135–136.

485 Convention 108 for the Protection of Individuals with Regard to Automatic Processing of Personal Data. In the English version, principles are called criteria, however, in French, Finnish and Swedish versions they are clearly named principles.

occur. The new principle of accountability stresses the controller's responsibility, and the need to process personal data in a transparent manner has been underlined.[486]

The concepts of principle and rule were studied in Chapter I of this thesis. It was discovered that arguments founding the underlying principles are arguments aiming to establish individual rights. Another characteristic feature of principles is dimension. It is precisely the dimension of principles which allows balancing, instead of applying them in an all-or-nothing manner as rules are to be applied.[487]

It has been argued, that data processing which does not comply with these principles is illegitimate.[488] It was earlier established that principles do not function in an all-or-nothing manner. This leads to a question whether of these principles should actually be considered rules in the sense of Alexy and Dworkin even if named principles. This argument is further supported by Article 23 of the GDPR, which empowers the national and Union legislator to derogate from the data protection principles in certain situations. The need for such empowerment is debatable if data protection principles were duly principles as they are understood in this thesis. Thus, the precise nature of these concepts remains unclear. They do contain principle-like features, but their nature approaches rules to certain extent. However, they will be called principles as this is the vocabulary adopted in the European data protection legislation. The data protection principles have been further specified in the national legislation of some Member States. For instance, in the United Kingdom, the former Data Protection Act defined eight data protection principles.[489]

Next, the most relevant principle for the purposes of this thesis will be studied. This is the purpose limitation principle, which supports some specific data protection rules. The actual content of the principle must be drawn from the data protection rules which it supports. The principle of proportionality is not elaborated in this section. The issues related to proportionality are elaborated on more general level in this thesis.

The purpose limitation principle is one of the corner-stones of the European data protection framework. It sets boundaries for the processing of personal data. The core idea of the purpose limitation principle is that personal data may be processed only for the purposes for which it was originally collected. This principle is also the root of one of the key issues which needs to be solved in the relationship with access to documents legislation.

---

486 Proposal for a Regulation of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM (2012) 11 final.

487 See Chapter I.

488 S. K. Karanja, *Transparency and Proportionality in the Schengen Information System and Border Control Co-operation*, (Leiden, 2008) 135.

489 The GDPR does not leave similar margin for member states. The nature of the legal instrument does not allow national implementation in this regard.

Before engaging in more detailed discussion of the purpose limitation principle, it must be acknowledged that the structures of data processing are changing and the consequences of this change have not yet been duly reflected in the European data protection regime. While personal data was traditionally collected in specific databases, vast data flows are now taking the place of traditional data files. And even more importantly, different big data applications are commonly used by certain stakeholders. The sustainability of the traditional data protection principles has not been properly tested in this changing environment yet. However, this intriguing issue will be set aside when assessing the purpose limitation principle.

The purpose limitation principle has been laid down in different European data protection instruments. Consequently, it should exist in Member States' national legislations.[490] After May 2018, it follows directly from the GDPR. The formulation might vary in different instruments, but the core idea remains the same. The EU Institutions' Data Protection Regulation sets the purpose limitation principle in Article 4(b) which states that "*personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes*". This was very similar to the former Data Protection Regulation and former Data Protection Directive, which the GDPR did not change.

The purpose limitation principle can be addressed in several ways. The weight can be, for example, on the aim of the said principle. It has been suggested that the principle has two aims: firstly, the data subject must be informed of the purpose of the processing, and secondly, the personal data cannot be used later on for purposes incompatible with the original purpose.[491] This is, indeed, one way to perceive this principle. However, this section will examine the principle from a different angle. The purpose limitation principle contains three elements, which will be analyzed. First, the purpose of the data collection must be specified. Second, the purposes for the collection must be both explicit and legitimate. And third, further processing of the personal data cannot be incompatible with the original purpose of the data collection.[492] These elements do also cover the two aims mentioned earlier.

2.3.1 SPECIFICITY

The data processing purposes should be defined before the personal data is collected. Only personal data which is necessary, adequate and relevant for the processing

490 For instance, the former Finnish Personal Data Act includes an article concerning the defined purpose of processing and another article relating to exclusivity of purpose.

491 C. Kuner, *European Data Privacy Law and Online Business*, (Oxford, 2003) 59–61.

492 For further processing and compatible processing purposes, see case C-536/15, *Tele2 (Netherlands) and others*, ECLI:EU:C:2017:214, paras 34–40.

purposes may be collected.[493] In other words, first the controller has to know why the personal data will be collected and thereafter the controller can only collect data that is necessary for the said purpose.

Processing purposes should not be defined in a wide manner, even if this might seem tempting when all the possible scenarios for further processing are not evident at the time of the data collection. It is possible to have several processing purposes for the data collection though. In such cases each processing purpose should be separately and specifically defined according to Working Party 29.[494]

The requirement to process personal data for specific purposes is also apparent in the Schrems case, even if the CJEU did not underline this in its reasoning but rather argued the case based on proportionality. The personal data transferred to the United States was not processed for the specific commercial purposes for which it was initially collected when the local authorities had vast rights to access this data in order to process it for national security purposes.[495] Hence, the data was processed for different purposes from the original purpose for which the data was stored.

2.3.2 EXPLICITLY AND LEGITIMACY

It was earlier noted that the purpose limitation principle can also be seen referring to the duty to inform the data subject of the purposes of the data collection. It can be argued that the requirement for explicit data processing includes this element. However, when assessing the meaning of the said requirement, the core element is that the processing purposes must be clearly defined by the controller. The processing purposes should be unambiguously expressed, in such a manner that both data protection authorities and also data subjects would have the same solid understanding of the processing purposes.[496]

As for the legitimate purposes, it clearly refers to the legal basis for processing laid down, for example, in Article 6 of the GDPR.[497] However, legitimacy has been considered wider than simply the legal processing of personal data. It has been suggested that legitimacy also implies such things as cultural values, fair processing and necessity.[498] Further, it has been suggested that such elements as customs, codes

493 WP 29 Opinion 3/2015, p. 15–16.

494 WP 29 Opinion 3/2015, p. 15–16.

495 Case C-362/14, *Schrems,* ECLI:EU:C:2015:650, para 90. See for example Article 29 Data Protection Working Party, Opinion 3/2013 on purpose limitations, p. 17–18.

496 See for example Article 29 Data Protection Working Party, Opinion 3/2013 on purpose limitations, p. 17–18.

497 For legal basis, see also Case C-13/16, *Rigas satiksme,* ECLI:EU:C:2017:336.

498 L.A. Bygrave, *Data Protection Law, Approaching Its Rationale, Logic and Limits,* (Kluwer, 2002), 57–61.

of conduct, codes of ethics, contractual arrangements and the general context and facts of the case form part of the legitimate purposes.[499]

2.3.3 FURTHER PROCESSING

The third element of the purpose limitation principle relates to further processing. Personal data may not be further processed for purposes which are incompatible with the original purpose of the data collection. This requirement also stems from the Charter of Fundamental Rights, which emphasizes that personal data must be processed for specified purposes.[500] However, data processing for historical, statistical and scientific purposes are not considered incompatible with the original processing purpose.

It has been suggested that this requirement can be approached from two angles. It can be examined either from the data controller's perspective or from the data subject's perspective. When the question is studied from the data controller's viewpoint, the emphasis would be on the realization of the original processing purpose. The further processing should not render the actualization of the original purpose void or even difficult. When examined from the data subject's perspective, the emphasis would be on legitimate expectations etc.[501] This approach might appear alluring when personal data is increasingly processed for further purposes, which are unknown at the time of the data collection. An example of such use is the transfer of flight passengers' name records for security purposes.

However, the core of the idea of this principle is that personal data must not be further processed for purposes which are incompatible with the original processing purpose. The Data Protection Regulation does not give clear guidelines on how to interpret the purpose limitation principle nor does the EU Institutions' Data Protection Regulation, former Data Protection Directive or the GDPR. When applying this principle, the reasonable and legitimate expectations of the data subject should be taken into consideration. In other words, for example, genetic data, which was collected in the course of scientific research, cannot be used by insurance companies later when assessing the risk a particular client might pose for the company. However, this should not be considered as an absolute ban for further processing of personal data. When assessing what further processing is allowed, the emphasis should be on the reasonable and legitimate expectations of the data subject.[502] For instance, when a public figure has participated in a public

499 Article 29 Data Protection Working Party, Opinion 3/2013 on purpose limitations, p. 19–20.

500 Charter of Fundamental Rights of the European Union (OJ C 303, 14.12.2007, p. 1–16), article 8.

501 L.A. Bygrave, *Data Protection Law, Approaching Its Rationale, Logic and Limits,* (Kluwer, 2002), 340.

502 For the extent of consent and further processing, see Case C-536/15, *Tele2 (Netherlands) and others*,

meeting, he or she should reasonably expect that his or her name will be disclosed at a later stage.

2.3.4 EXCEPTIONS TO PURPOSE LIMITATION PRINCIPLE

There are some exceptions to the purpose limitation principle laid down in the GDPR and also in the EU Institutions' Data Protection Regulation. Despite the purpose limitation principle, personal data may be processed for archiving purposes in the public interest or for scientific, statistical or historical purposes. In other words, processing personal data for scientific research purposes or to draw up statistics has been considered privileged in the sense that the purpose limitation principle is seen to create unnecessary obstacles for such processing.[503]

While this might clarify the situation when personal data is processed for the said purposes, this might cause some confusion how to interpret "compatible" and "incompatible". It is important to note that this Article only states that processing for these purposes is not incompatible. It does not claim that processing for these purposes would be compatible with the original purposes. In other words, the core idea of this provision is that personal data may be processed for the said purposes despite the requirements set by the purpose limitation principle. The importance of the difference in what is meant by "not incompatible" and "compatible" becomes evident when what can be considered compatible processing is assessed in more general terms. If the said processing purposes were considered compatible with the original processing purposes, the weight on the assessment would lay on the importance of the secondary processing purpose. Not on the assessment of whether the secondary processing actually fits in the scope of the original processing purposes. However, in such cases, the assessment should rather be carried out by assessing whether there exist grounds to consider the aim of the secondary processing purposes as a public interest and whether the secondary processing meets the requirements of proportionality.[504]

ECLI:EU:C:2017:214, paras34–40.

503 For the collection of personal data for statistical purposes, see also a judgment by the German Constitutional Court, BVerfGE 65, 1 (15 December 1983).

504 For proportionality and the overriding public interest in the context of further processing, see judgment by the German Constitutional Court, BVerfGE 65, 1 (15 December 1983).

2.3.5 FURTHER PROCESSING BASED ON LEGISLATION

It is often seen that data processing in the public sector requires stronger frames than that taking place in the private sector.[505] Generally speaking, processing in the public sector derives its legitimacy from legislation. While the GDPR leaves a rather wide margin for assessing the legitimacy of processing in the private sector (processing is based on the legitimate interest of the controller), this is not the case when it comes to the public sector.

The CJEU has also given some further guidance on the stipulations of national legislation on data processing carried out by public authorities. The CJEU clarified that when personal data is transferred from one public authority to another public authority, the data subjects should be informed in certain cases. The CJEU underlined the fact that national legislation which provided the legal basis for such data transfers did not cover all of the information transferred to another public authority, nor the manner in which it was transferred. The CJEU saw that data subjects had to be informed that their personal data was transferred. [506] One could argue that the CJEU's decision could be read in a way which allows the disclosure of personal data to another public authority when it is regulated in a detailed manner in national legislation. Another significant point in the said judgment is that it did not articulate anything on the right to object, but simply on the data subject's right to be informed.

How further processing based on legislation and the purpose limitation principle will be perceived under the new data protection regime remains obscure. Nevertheless, it does seem that further processing based on legislation does not need to be compatible with the original processing purposes. In such cases, the legislator has deemed the secondary processing purposes so important that the purpose limitation principle can be derogated. Clearly, the legislator is not free to stipulate on the matter however it wishes. The Charter of Fundamental Rights sets the parameters for the legislator to reconcile different interests, without interfering with the essence of the rights protected by the Charter.

505 See for example the exclusion of public sector in the last sentence in Art. 6(1)(f) of the GDPR.

506 C-201/14, *Samaranda Bara and others*, ECLI:EU:2015:638, paras 35, 37–43.

3. SOME ELEMENTS OF DATA PROTECTION LEGISLATION

This section will discuss some of the core elements of data protection legislation. These elements play an essential role in relation to European transparency regulation. This section will first focus on consent, which is one of the legal bases for the processing of personal data. This will be followed by the right of access to personal data and the right to rectification. All these elements share a common feature – they are recognized by the Charter of Fundamental Rights – and therefore must be considered to form the core of the right to data protection. Thereafter, the data subject's right to object will be briefly examined.

As noted earlier, some consider some of the elements which will be discussed in this section as principles. The principle referring to these rights is formulated as an individual participation principle.[507] However, the definition of principle in the context referred to diverges from the principles as they are understood in Dworkin and Alexy's terms; in the context referred to, the non-applicability of the principles renders the processing of personal data illegitimate. As these elements are applicable in an all-or-nothing manner, I separate these elements from principles as understood in this thesis.[508] For example, if a data subject is not granted access to his or her personal data, there must be an exception applicable to that specific case. The data controller is not entitled to freely balance the different interests at stake. Naturally, it could be examined whether there are some underlying principles which these elements reflect, like the individual participation principle, which would be balanced on a case-by-case basis. However, this seems unnecessary from the surface; the underlying principles should rather be sought from the more general principles beneath the data protection regulation.

3.1 DATA SUBJECT'S CONSENT

Processing of personal data must always have a legal basis. The data subject's consent forms a legal basis for data processing, but there are also other alternatives.[509] Consent, like the other elements examined in this section, reflects

507 S. K. Karanja, *Transparency and Proportionality in the Schengen Information System and Border Control Co-operation*, (Leiden, 2008) 145.

508 See Chapter I, section 1.1.

509 See for example Article 6 of the GDPR. Besides consent, personal data may be processed if processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior entering into a contract; or processing is necessary for compliance with legal obligation to which the controller is subject; or processing is necessary in order to protect the vital interests

self-determination.[510] However, as has been underlined on several occasions, the principle of self-determination is not absolute in a sense that data subjects would have absolute control over their own personal data.[511]

First, some basic elements of consent will be discussed and thereafter consent will be assessed from two different angles: firstly, can the processing of personal data be solely based on the consent of the data subject and secondly, how far-reaching is the data subject's right to disallow the processing of his or her personal data.

Consent has been defined in the European data protection framework. It must be a freely-given, specific and informed indication of the data subject's wishes. The GDPR defines consent as "*any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her*". The form of consent was not previously specified in the European data protection regime, not in the former Data Protection Directive nor in the former Data Protection Regulation.[512] The GDPR in turn sets quite detailed requirements for consent.[513]

Even if the form of the consent was not specified in the earlier legislation, such terms as "unambiguous" and "express" have appeared in practice. These terms suggest that the doctrine of implied consent cannot be applied when personal data is processed based on consent.[514] Thus, a simple notification by the controller stating that he is processing personal data, for example for marketing purposes, could not be considered unambiguous or express consent. It has been also suggested that simply clicking an icon referring to acceptance on a commercial website would not necessarily meet the requirements set for consent when the rules and conditions are very long and not easily understandable.[515]

---

of the data subject or of another person; processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; or processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party.

510 See for example S. Holm & S. Madsen, "Informed consent in medical research – a procedure stretched beyond breaking point?", in O. Corrigan; John McMillian; Kathleen Liddell; M.Richards & C.Wijer, *the limits of consent, A socio-ethical approach to human subject research in medicine* (Oxford University Press, 2009), 12.

511 A. Rouvroy & Y. Poullet, "The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the importance of Privacy for Democracy", in S. Gutwith; Y. Poullet; P. De Hert; C. de Terwangne & S. Nouwt, *Reinventing Data Protection* (Springen, 2009), 45–76. See also for instance Case C-524/06 *Heinz Huber*, ECLI:EU:C:2008:724. See also judgment by the German Constitutional Court, BVerfGE 65, 1 (15 December 1983).

512 Similarly, the implementing national legislations often do not contain provisions regarding the form of consent, see for instance the former Finnish Personal Data Act or UK's Data Protection Act.

513 Proposal for a Regulation of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM (2012) 11 final, p. 46–47 (Articles 7 and 8).

514 See also for consent as regards cookies; Article 29 Working Party, Opinion 2/2010 on online behavioural advertising, adopted 22 June 2010.

515 C. Kuner, *European Data Privacy Law and Online Business*, (Oxford, 2003) 68.

Besides being express, the consent must be freely given. This raises the question of whether consent as a prerequisite for some other action – like getting a loan – is actually a consent, in particular when exceeding what is considered proportional processing of personal data for the specified purposes.[516]

3.1.1 PROCESSING PERSONAL DATA BASED ON CONSENT

It has been suggested that the data subject's consent as justification for the processing of personal data is threefold. Firstly, it should be considered a procedural justification rather than a substantive one. In other words, the justification rests on someone's authorization rather than on the merits of the case, i.e. the right to process the personal data would not follow from the nature of the data or the circumstances, but from the authorization. This leads to the second point: the consent would be valid vis-à-vis the consenting party, not necessarily as a justification for the processing of personal data as such. Thirdly, the consent would primarily function as a "negating wrong", and not create the basis for the right to process personal data.[517] The second point could signify, for instance, that the Data protection authorities would not allow some processing of personal data, even if the data subject had given their consent for the processing. However, the consent could have an effect, for example, on the data subject's right to claim for compensation for the sole reason of the insufficient legal basis for the processing.

Furthermore, it has been noted that the wording of the European legal framework does not suggest that consent alone would provide sufficient grounds for the processing of personal data. For instance, the requirement of proportionality should be respected despite of the potential consent of the data subject.[518] And not only proportionality, but also other principles governing the processing of personal data

516 The European Parliament took a stand on this issue during the negotiation process on the General Data Protection Regulation suggesting in its text that "*the execution of a contract or the provision of a service shall not be made conditional on the consent to the processing of data that is not necessary for the execution of the contract or the provision of the service pursuant to Article 6(1), point (b)* ". The outcome of the trilogue negotiations leaves this issue more open. Article 7(4) of the GDPR stipulates that "*when assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract*". Thus, the final formulation of the GDPR has some relics of the approach taken by the European Parliament, but does not take as strict an approach as the European Parliament. For the European Parliament's approach, see European Parliament legislative Resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).

517 R. Bronsword, "Consent in Data Protection Law: Privacy, Fair Processing and Confidentiality" in S. Gutwith; Y. Poullet; P. De Hert; C. de Terwangne & S. Nouwt, *Reinventing Data Protection* (Springen, 2009), 88–101.

518 A. Rouvroy & Y. Poullet, "The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the importance of Privacy for Democracy", in S. Gutwith; Y. Poullet; P. De Hert; C. de Terwangne & S. Nouwt, *Reinventing Data Protection* (Springen, 2009), 62–76.

should always apply. An example of this would be a decision taken by the Finnish Data Protection Board.[519] The Board took the view that the data subject's consent does not suffice to form the basis for the processing of personal data. Furthermore, the Board saw that consent did not justify derogating from the data protection principles; the processing of personal data had to be in line with the data protection principles. The Supreme Administrative Court later confirmed this approach by holding the decision of the Data Protection Board.

It is quite natural that certain established principles of the regulatory framework should apply regardless of the data subject's consent. In other words, the data subject cannot consent to differing from the data protection legislation's provisions or principles, but solely to form a basis for the processing.[520] If this was not the case, the data subject and data controller could quite freely stipulate how to process the personal data, rendering data protection regulation somewhat void.

3.1.2 THE LIMITS OF CONSENT

It has been now established that not all of the requirements of data protection legislation are met solely based on the data subject's consent. In other words, processing should always meet the other requirements set out in the regulatory framework. It was also established that consent should rather be considered a procedural justification than a substantive one. This leads to the following question: when the legitimacy for the processing of personal data is not derived from the nature of the data or the circumstances in which the data is being processed, what significance should be given to the nature of the data and circumstances vis-à-vis the data subject's consent? Two questions are of particular interest in this context. Firstly, when processing is based on the data subject's consent, how far-reaching is the data subject's control over their personal data once the processing of personal data has begun? And secondly, could the nature of the data or the circumstances in which the data has been processed create boundaries to what the data subject can consent to?

It is clear that when processing is based on consent, the legal basis vanishes when the data subject withdraws his or her consent. But could the nature of the data or circumstances in which it has been processed require processing regardless

519 See for example Decision of the Finnish Data Protection Board (tietosuojalautakunta) 4/2007, dnro 6/932/2006.

520 This approach was confirmed by the adoption of the GDPR. According to Article 7(2) of the GDPR "*2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.*"

of the data subjects' wishes? For example, when personal data is being processed for scientific research purposes based on consent and the data subject withdraws his or her consent, it seems reasonable to argue that the circumstances where data is being processed create justification to continue the processing. Clearly, the data should not be processed for new research purposes but withdrawing certain data from the research sample could lead to corrupted results.

It was already established that the controller or processor cannot circumvent the requirements set out in data protection legislation simply by gaining the data subject's consent. But another question is whether the data subject can agree to any type of processing, regardless of the nature of the data or the circumstances. I see at least two situations in which there appear to be natural limits to consent. First, quite often processing carried out in the public sector derives from legal obligations and, as such, it seems quite reasonable to expect that the processing is based on legislation. In these cases, consenting should not play a significant part. Secondly, there are situations where basing the processing of personal data on consent sets too much responsibility on the data subject. An example of this would be scientific research and the data banks used in scientific research, which are constructed solely based on the consent of the data subject. The core issue is not necessarily whether their consent is freely given but whether the data subject is in reality in such a position that he or she can assess the actual consequences of their consent.[521] It seems that the burden set on the data subject is too heavy in such a construction, and such processing should rather have its legitimacy and safeguards in the legislation.[522]

3.2 THE DATA SUBJECT'S RIGHT OF ACCESS TO DATA

While all elements discussed in this section reflect the right to self-determination, there is a difference between consent and the other elements, the right of access and the right to rectification and objection. Consent is one of the legal bases provided in Article 6 of the GDPR.[523] In other words, it creates a basis for data processing. The other elements examined in this section create rights for the data subject when the processing of personal data takes place. When the relationship between data protection and transparency is examined, the data subject's right of access to his

521 For an interesting case related to the significance of consenting to processing of personal data in relation to online disclosure of data, see case T-343/13, *CN v Parliament*, ECLI:EU:T:2015:926.

522 For the grounds to use consent as legal basis in the public sector, see also T. Pöysti, Trust on Digital Administration and Platforms, in *Scandinavian Studies in Law* 65(2018), 339.

523 Similarly, in Article 5 of EU Institutions' Data Protection Regulation.

or her personal data in the said context will be studied in more detail. At this stage, the data subject's right of access will be briefly examined on more general level.

The right of access is on solid ground in the European data protection framework. After the adoption of the former Data Protection Directive, the right of access was reinforced by the Charter of Fundamental Rights, which states that everyone has the right of access to data which has been collected concerning him or her.[524]

As was the case under the previous data protection regime, both the GDPR and EU Institutions' Data Protection Regulation contain provisions, which regulate the right of access. The right of access enables individuals to know if their personal data has been processed and, if so, what personal data is being processed and for what purposes. In other words, controllers in the European Union have to provide data subjects with this information. Besides multinational companies like Facebook and Google, this also applies to public sector controllers, such as the Union institutions.[525]

Data subject's rights inevitably create duties for the controller and might cause administrative burden. The obligation to search all electronic and paper files has been criticized as a significant administrative and financial burden for the data controllers.[526] However, if searching the information described above does create an immense administrative burden for the controller, it ought to be considered whether this burden could be avoided by designing the data processing systems from the outset in such a manner that answering data subjects' requests was feasible. After all, one of the reasons for the genesis of the European data protection regime derives from the increasing possibilities to easily search and combine personal data from different data files.

3.3 RIGHT TO RECTIFICATION AND RIGHT TO OBJECT

Like the right of access, the right to rectification has been reinforced by the Charter of Fundamental Rights. The Charter now says that everyone has the right to have personal data concerning him or her rectified.[527] Furthermore, like the right of access, the right to rectify also reflects the values of self-determination. The right of access is a prerequisite for the right to rectification. Without access to his or her personal data, the data subject would not be able to ask for it to be rectified.

The Data Protection Directive did set an obligation for the Member States to provide data subjects with the right to rectification, in particular when the data was

524 Charter of Fundamental Rights of the European Union (OJ C 303, 14.12.2007, p. 1–16), Article 8.

525 However, the duty to provide data subjects with the said information is based on different legal instruments; private entities must comply with the General Data Protection Regulation, and EU institutions the Data Protection Regulation.

526 P. Carey, *Data Protection*, (Oxford 2009) 130, 133.

527 Charter of Fundamental Rights of the European Union (OJ C 303, 14.12.2007, p. 1–16), Article 8.

incomplete or inaccurate.[528] The GDPR provides a similar right and so does the EU Institutions' Data Protection Regulation. According to Article 16 of the GDPR, "*the data subject shall have the right to obtain from the controller without undue delay the rectification of personal data concerning him or her which are inaccurate. Having regard to the purposes for which data were processed, the data subject shall have the right to obtain completion of incomplete personal data, including by means of providing a supplementary statement*".[529]

Lastly, it ought to be mentioned that the right of access and right to rectification are often associated with transparency in the data protection context. It ought to be underlined that transparency in this context differs from the transparency rights examined in this thesis. When transparency is used in the context of data protection, it most often refers to transparent processing of personal data.[530] In other words, the data subjects' right to know how and for what purposes their data is being processed. In the context of the public access to documents regime, transparency is not limited to one's own personal data, but covers more generally all information and the public in general.[531]

Unlike the right of access and rectification, the right to object does not draw on the Charter of Fundamental Rights. However, it did already exist under the previous data protection regime. Both the GDPR and the EU Institutions' Data Protection Regulation provide the said right. This right, which reflects self-determination, as do the other elements studied in this section, applies to situations where data is processed based on the controller's legitimate interest or the public interest.[532] In other words, when data processing is carried out for example to fulfil the legal obligations of the controller, based on Article 6(1)(c) of the GDPR, the right to object does not apply.

The right to object is not absolute. A data subject may object to data processing based on grounds relating to his or her particular situation. The wording "*particular situation*" sets the threshold for the application of this right rather high. This is the first restriction laid down by the legislator. Further, when controller is able to demonstrate that there are compelling legitimate grounds for the processing, the processing of the said personal data may continue if such grounds override the interests of the data subject. Furthermore, it ought to be noted that Article 23 of

528 Article 12 of the Data Protection Directive.

529 Article 16 of the GDPR.

530 Article 29 Data Protection working party, "Guidelines on transparency under Regulation 2016/679", 17/EN WP 260.

531 For collective public see D. Erdos "From the Scylla to the Charybdis of License? Exploring the Scope of the 'Special Purposes' Freedom of Expression Shield in European Data Protection" in *Common Market Law Review* 52 (2015), 119–154. For collective interests, see M. Van Hoecke & J. Dhont, Obstacles and Opportunities for the Harmonisation of Law in Europe: Case of Privacy, in V. Heiskainen & K.Kulovesi (eds.) *Function and Future of European Law*, (Helsinki, 1999), 110–111.

532 Article 21 of the GDPR.

the GDPR and Article 25 of the EU Institutions' Data Protection Regulation provide the possibility to derogate from this right, based on national or Union legislation, and also even based on internal rules.

3.4 NEW DATA PROTECTION CONCEPTS

It was earlier argued that ever-developing technology has caused a shift on the weight from the privacy to self-determination in the data protection framework. This issue is now further elaborated through some new data protection concepts, namely the right to be forgotten and data portability. It is necessary to examine these concepts to form a solid picture of the shift from privacy to self-determination. These concepts illustrate excellently how self-determination is gaining more importance in the European legal framework for data protection. They all present new elements in the European data protection framework. The new provisions related to profiling, for example, also reflect the same tendency. However, for the purposes of this thesis, deeper analysis of the two above-mentioned concepts should be enough. Furthermore, it will later be argued that self-determination should be perceived differently in the social media context vis-à-vis public sector processing. For this purpose, it is essential to examine some of the concepts that reflect the said progress in detail.

3.4.1 RIGHT TO BE FORGOTTEN

Ever-developing technology has created pressure to launch new data protection concepts, the right to be forgotten being one of them.[533] The right to be forgotten was taken into a more formal sphere with the GDPR.[534] While it had been previously mentioned in seminars and in academic articles[535], the Commission took it to a new level by first introducing it in its Communication and thereafter naming one of the articles accordingly in its proposal for the GDPR.[536] The core idea of the right to be

533 The question of whether right to be forgotten is diverging from the right to protection of personal data and turning into its own right with underlying principles is excluded from this discussion.

534 See Commission Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) COM(2012) 11 final (25.1.2012) and Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1–88).

535 For example, Jeroen Terstegge, Corporate Privacy Officer/ Senior Counsel, Digital Europe at a Data Protection conference in Brussels 19 May 2009.

536 Communication from the Commission to the European Parliament, The Council, the Economic and Social Committee and the Committee of Regions, A comprehensive approach on personal data protection in the

forgotten might not be novel, but the new circumstances, such as social media and different online applications, have taken it to a new level.

The right to be forgotten is drawn from existing elements in the European data protection framework, such as the data subject's right to have his or her data erased and the data subject's right to have his or her personal data rectified. However, the core idea underneath the right to be forgotten is fresh one, and caused by technological developments. The right to be forgotten is closely tied with developments in our societal structure following on from technological development. This evolution has been described as a move from village culture to the global village, and during this journey there has been a short stop at city culture[537]. In villages, people knew each other well; the accomplishments achieved, and the pranks played in childhood and youth remained in the collective memory of the village and had an impact on the individual's role and status in the village. Life in city culture was more anonymous; someone could easily move from one role to another and even have quite radical changes in lifestyle without having the past following him or her. Now, we have arrived at the third stage of this progress, the global village. Besides the features of the classic village society, the new element in this societal structure is the global dimension. This has been created through the online world and the internet, where the things one has done and said might take on a life of their own and have more or less eternal life cycle.

I see that the new societal structures can be seen as one reason for the intense debate that the right to be forgotten frequently causes.[538] Another reason for the heated debate is unrealistic expectations linked with the right to be forgotten. When personal data has been released on the internet, it cannot be entirely erased. The possibility of copies circulating around is not purely hypothetical. Even innovations targetted at creating short lifespans for messages cannot realize the right to be forgotten. An example of this is a relatively new social media forum, Snapchat. Ten-year-old children very quickly learned to take screen captures of messages sent in snapchat and thus, the lifespan of the data very quickly became eternal again.

European Union, COM 2010 (609) final; Commission Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) COM(2012) 11 final (25.1.2012); Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1–88).

537 For example, Jeroen Terstegge, Corporate Privacy Officer/ Senior Counsel, Digital Europe at a Data Protection conference in Brussels 19 May 2009.

538 See for example The Guardian, "We need to talk about the right to be forgotten", by David Drummond, available on the internet <https://www.theguardian.com/commentisfree/2014/jul/10/right-to-be-forgotten-european-ruling-google-debate> [last visited 9.4.2017]; Eric Posner, "Debate about the Right to be Forgotten, March 13 2015, available on the internet < http://ericposner.com/debate-about-the-right-to-be-forgotten/ > [last visited 9.4.2017]; K. Brimsted, "*The Right to be forgotten: can legislation put the data genie back in the bottle?*" in Privacy and Data Protection 4 (2011).

Some have underlined that the ultimate rationale behind the right to be forgotten had traditionally been the protection of the individual's dignity by giving them tools to control the sensitive information relating to them.[539] Personal data does not need to be sensitive when the data subject wishes to apply his right to be forgotten.[540] However, it seems easy to agree that protecting one's dignity is a central element in right to be forgotten. Once this connection is established, its relation to self-determination must also be acknowledged. While the right to be forgotten clearly derives from self-determination, it also reflects the underlying values of privacy. When the data subject wishes to have some data erased, it seems natural to claim that this is done precisely for the purposes of protecting privacy. In other words, in the right to be forgotten both privacy and self-determination are clearly apparent.[541]

The right to be forgotten lived through some changes during the GDPR negotiations. The Commission also took a more moderate tone in relation to the right to be forgotten and underlined that it is not, after all, a new right.[542] It was also questioned whether the right to be forgotten actually brings any added value to the existing legal framework.[543] I see that it does. The new element that it brings to the existing legal framework is the weight and recognition it sets on data subjects' rights in the cloud environment. The new societal environment certainly sets some expectations for reframing the data protection regime. Maybe the new problems that emerged in the data protection framework were not entirely solved, but at least they were duly recognized.

539 K. Brimsted, "*The Right to be forgotten: can legislation put the data genie back in the bottle?*" in Privacy and Data Protection 4 (2011).

540 Article 17 of the GDPR.

541 During the negotiation process in the Council and European Parliament, the Commission's original proposal for the right to be forgotten lived through some changes. The data controller will for example not be held liable for information which is processed by third parties. In other words, the Commission's proposal was very much stripped of its innovative elements targetted at challenges created in the cloud environment, and was left with the skeleton which exists already in the Data Protection Directive. See for example Communication from the Commission to the European Parliament, The Council, the Economic and Social Committee and the Committee of Regions, A comprehensive approach on personal data protection in the European Union, COM 2010 (609) final; Commission Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) COM(2012) 11 final (25.1.2012); Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1–88).

542 See for example Viviane Reding, Vice-President of the European Commission, EU Justice Commissioner, SPEECH/12/26, *The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age*, available on the internet < http://europa.eu/rapid/press-release_SPEECH-12-26_fi.htm > [last visited 3.7.2017] and Financial Times, *Brussels welcomes Google 'right to be forgotten' measure*, May 30, 2014, available on the internet <https://www.ft.com/content/bc116b3e-e810-11e3-9cb3-00144feabdc0?mhq5j=e1> [last visited 3.7.2017].

543 K. Brimsted, "*The Right to be forgotten: can legislation put the data genie back in the bottle?*" in Privacy and Data Protection 4 (2011).

3.4.2 DATA PORTABILITY

Data portability is one of the new data protection concepts introduced by the GDPR. Together with the right to be forgotten and some of the other novelty elements in the Commission's proposal[544], data portability reflects the underlying idea of self-determination. The core idea is that the data subject would have control over the personal data, which he has earlier submitted to the controller in cases where the data processing is based on consent or contract. Besides strengthening control over one's own personal data, this right provides the data subject with the right to have his personal data in an electronic and commonly-used format. In other words, the data subject could transfer his personal data from one system to another.[545] The controller could not prevent this by invoking different electronic systems and claiming it is not technologically feasible.

The basic elements of this right did exist in the earlier data protection framework. Based on the provisions laid down in the Data Protection Directive and Data Protection Regulation, the data subject had the right of access to his personal data. Together with the right to obtain a copy of his personal data, these rights create the basis for data portability.[546] However, data portability would take this right much further. The core idea behind data portability is the data subject's right to transfer his or her personal data from one system to another.[547] Previously, the data subject was indeed able to request his information, for example from Facebook based on the rights drawn from the Data Protection Directive, but the outcome might have been some hundred pages of paper.[548] After the entry into force of the GDPR, the data subject can get information in a format which allows him to reuse this data. It seems justified to enhance the data subject's control over their personal data when data processing takes place for example on social media. The whole content of the site is created by the data subject, while the controller or processor simply provides the structure and forum to present this content.

I argue that at least two significant elements regarding data portability must be distinguished when data protection is assessed in relation to transparency legislation. First, data portability applies to situations where the data subject is the active party himself and legitimizing the data processing derives from the data subject's self-determination. In this respect, it ought to be noted that public sector processing is largely excluded from the scope of this right. This is apparent in the wording of the said right but could also be derived from the first paragraph of the said Article.

544 See for example Article 20 on the right to data portability and strengthened rules on the consent.

545 Commission's proposal Article 18.

546 Directive 46/95, Articles 10–12, Regulation 45/2001, Articles 10–13.

547 Commission proposal Article 18.

548 See for example Case C-362/14 *Schrems,* ECLI:EU:C:2015:650.

Processing of personal data in the public sector hardly ever takes place based on contract or the data subject's consent.[549] Second, when the data subject provides his or her personal data for processing on a voluntary basis and for sharing on social media, the underlying principle of privacy diverges from this right. When the data subject shares the information with hundreds of people, who cannot all be known to him, it seems justified to argue that it is rather the control over his data which is significant for the data subject. In other words, underlining the importance of self-determination is justified when the processing of personal data takes place in the internet environment, or in the cloud as it is put in this decade.

4. TOWARDS THE NEW DATA PROTECTION REGIME

When writing this chapter, the trilogue negotiations on the GDPR were still ongoing. This was preceded by long negotiations in the Council after the European Commission presented its Data Protection Package in January 2012. The first indications of the reform process were given in the Commission's Communication in 2010.[550] In the said Communication, the Commission underlined that the underlying principles and objectives of the data protection legislation were still as valid as they were at the time of the adoption of the Data Protection Directive.[551] Thus, the reform process does not affect the analysis presented in this chapter. The key changes introduced by the data protection reform have been analyzed when relevant in relation to public access to documents.

A point discussed by the Commission in its Communication was the challenge created by fast-developing new technology.[552] This was one of the issues addressed in the GDPR proposal. Even if the data protection regime was based on technologically-neutral rules, the question of whether these rules are technologically current had arisen.[553] The Commission drew attention specifically to the challenges provided by social networking sites, cloud computing and the fact that personal data is collected in more sophisticated ways; including, even more importantly, in ways which are not always easily detectable.

549 Article 20 of the GDPR.

550 Communication from the Commission to the European Parliament, The Council, the Economic and Social Committee and the Committee of Regions, A comprehensive approach on personal data protection in the European Union, COM 2010 (609) final.

551 Ibid.

552 Communication from the Commission to the European Parliament, The Council, the Economic and Social Committee and the Committee of Regions, A comprehensive approach on personal data protection in the European Union, COM 2010 (609) final.

553 For example, Jeroen Terstegge, Corporate Privacy Officer/ Senior Counsel, Digital Europe at a Data Protection conference in Brussels 19 May 2009.

The data protection reform has strengthened the European – and also global – data protection landscape in many ways. However, for the purposes of this thesis, it is of particular interest to note the shift introduced by the GDPR on the increasing weight set on self-determination. As discussed in this chapter, many of the new provisions reflect this, as do the more detailed rules on consent. Taking into consideration that references to privacy have faded in the GDPR, it appears that the balance of underlying principles and aims of data protection is moving from privacy towards self-determination with the entry into force of the GDPR, whether this has been intentional or not.

It is justified to underline the importance of self-determination instead of privacy in certain cases. An example of such a case is the social media environment. In such a context, it is reasonable to approach data subjects' rights through self-determination instead privacy. While the data subject might quite willingly disclose personal information through social media, he or she is not a passive data subject, but also the data controller or processor at some level. In such cases, the importance of the data subject retaining control over his or her personal data is apparent. When the information has been disclosed to vast audience, privacy does not seem to play an essential role anymore. This intriguing question, which is highly relevant in this thesis, will be addressed in more detail in the concluding chapter.

PART 2
CASE STUDIES

CHAPTER V

ACCESS TO DOCUMENTS AND PROTECTION OF PERSONAL DATA IN LIGHT OF CASE-LAW

This chapter will examine the case-law from the CJEU and the European Court of Human Rights (ECtHR). The three CJEU cases that will be discussed illustrate the tension between public access to documents and the protection of personal data at both a practical level and in terms of underlying principles. Once the three cases have been examined, the chapter will focus on the case-law of the ECtHR.

Commission v Bavarian Lager[554] was the first case in which the Court of Justice addressed the dilemma of the conflicting rules of data protection and access to documents. The Court provided some initial guidance for the simultaneous application of the Transparency[555] and Data Protection[556] Regulations, the basis of its judgment being the full application of both Regulations. Follow-up cases providing more precise guidelines, and hence greater certainty in the simultaneous application of the Transparency and EU Institutions' Data Protection Regulations, can still be expected.[557] In contrast, the opinion delivered by Advocate General Sharpston in this case was ambitious and can be considered a first attempt at a more profound reconciliation of these Regulations.[558] The Opinion thus deserves careful study alongside the Court's judgments, even though the CJEU did not adopt any of AG Sharpston's propositions.

The significance of the Bavarian Lager judgment for the overall theme of this study cannot be overstated. This is for three reasons. First, it was the first judgment by the Court of Justice delivered in the area of conflicting rules of data protection and access to documents and it did set the basic principle for reconciliation. This

554 Case C-28/08P, *Bavarian Lager*, ECLI:EU:C:2010:378.

555 Regulation (EC) No 1049/2001 of the European Parliament and the Council of 30 May 2001 regarding public access to European Parliament, Council, and Commission documents (OJ L 145, 31.5.2001, p. 43–48).

556 Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1–22).

557 The General Court delivered a judgment in Case C-82/09, *Dennekamp v Parliament*, ECLI:EU:T:2011:688 on 23 November 2011. The requirement to state reasons for the disclosure was assessed in this case. The General Court later examined a similar case and delivered its judgment on 15 July 2015. For that, see Case T-115/13, *Dennekamp v Parliament*, ECLI:EU:T:2015:497. The CJEU has further elaborated the requirement to state reasons in case C-127/13 P, *Strack v Commission*, ECLI:EU:C:2014:2250 and case C-615/13 P, *ClientEarth and PAN Europe v EFSA*, ECLI:EU:C:2016:489.

558 Opinion of AG Sharpston in Case C-28/08, *Bavarian Lager*, ECLI:EU:C:2009:624, delivered 15 October 2009.

principle still forms the basis for the balancing. The follow-up cases examined by the General Court and the CJEU have further elaborated the interpretation of the principle, but often in the context of other issues.[559] Second, besides the underlying conflicting principles, it relates first and foremost to actually conflicting rules. Third, compared to the decision of the General Court, the Bavarian Lager judgment showed the importance of the fundamental questions relating to 1) stating reasons for the application and 2) the data subject's right to object the processing of personal data, together with 3) the data subject's consent.

The Bavarian Lager study, together with current legislation, will show that full application of both Regulations does not seem achievable. It will be argued that one of the essential differences between the Regulations examined in this thesis, the obligation to state reasons for the application, has eventually to be carried out solely under either the Transparency Regulation or the EU Institutions' Data Protection Regulation. The role of the data subject's right to object and the significance accorded to professional activities will also be examined. These two elements are also apparent in the other cases examined in this chapter. In addition to providing an in-depth understanding of the reasoning of the CJEU, this discussion will pave the way for the final argument presented in the concluding chapter.

The second case study – *Volker und Markus Schecke GbR* and *Hartmut Eifert v Land Hessen*[560] –and the third – *Satakunnan Markkinapörssi Oy and Satamedia Oy*[561] – from the Court of Justice of the European Union must be examined together. Both involve public control over expenditure of public funds and will show that transparency can be considered a legitimate reason to limit one's right to the protection of personal data.

While the Bavarian Lager study relates to conflicting rules in the Dworkinian sense, the central issues in these cases relate to the more profound tension between one's right to the protection of personal data and the right of public access to documents. While the Bavarian Lager case covers very real conflicts between different provisions of the two Regulations, the second case study concerns the validity of certain provisions of Regulation 1290/2005.[562] This validity is examined in terms of underlying principles. However, this second case involves no apparent conflict of rules on the surface level of law.[563] The third case study complements

559 See for example Case T-115/13, *Dennekamp v Parliament*, ECLI:EU:T:2015:497; Case T-493/14, *Mayer v EFSA*, ECLI:EU:T:2017:100; Case C-615/13 P, *ClientEarth and PAN Europe v EFSA*, ECLI:EU:C:2016:489.

560 Joined cases C-92/09 and C-93/09 *Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen*, ECLI:EU:C:2010:662; for an analysis, see M.Bobek "Joined Cases C-92 & 93/09, Volker und Markus Schecke GbR and Hartmut Eifert" in *Common Market Law Review* 6 (2011), 2005–2022.

561 Case C-73/07, *Satakunnan Markkinapörrsi and Satamedia*, ECLI:EU:C:2008:727.

562 Council Regulation (EC) No 1290/2005 of 21 June 2005 on financing common agricultural policy (OJ L 209, 11.8.2005, p. 1–25).

563 For more on the various levels of law, see K. Tuori, *Kriittinen oikeuspositivismi*, (Helsinki, 2000).

the second, in that while the findings of the Court in the second case study are of the utmost important for this thesis in providing clear guidelines for balancing the two principles, these findings should be read in conjunction with other judgments of the Court, as this will provide the right context for the judgment.

The Luxembourg Court makes some first attempts to strike a balance between the conflicting principles in these two cases. As the conflict appearing on the surface level of law between the Transparency and Data Protection Regulations has not been clearly resolved through explicit rules or case-law, these two cases and the reasoning of the Court can provide guidance on how to achieve this.[564]

The second part of this chapter will provide the background for the European Convention on Human Rights and the case-law of the European Court of Human Rights. Once this initial step has been taken and the institutional and judicial context is clear, the section will examine one of the more recent cases that illustrates how the European Court of Human Rights has approached the values associated with the protection of personal data and access to documents. In the absence of clear provisions addressing these issues in the legislative framework of the European Convention on Human Rights, the significance of the case is clear. The objective of this section is to provide a comparative approach and to place the current situation in the European Union in its wider European context, providing a broader understanding of the relevant European legislation and case-law, and extending the scope of this study beyond just EU law.

Besides providing a more extensive European framework, that section will argue that prior agreement should not have an effect when examining a request for access to documents. Another characteristic feature of the Strasbourg judgment is the part played by legitimate interests and rightful interference in someone's privacy. As for data subjects' consent and the significance of the professional activities discussed above, the final argument and conclusion on the role of legitimate interests will be provided in the concluding chapter.

The concluding section will examine the approaches of the Luxembourg and Strasbourg Courts in this area and the ways they have dealt with the tension between these sometimes conflicting values. The main features of the core concepts relating to this tension are also examined in light of the case-law discussed in this chapter. The objective of this section is to provide both an understanding of the current case-law and a coherent picture of the tension at a conceptual level. This will pave the way for Chapter VI, where further examples of potential conflicts will be first identified and then examined. The examples in Chapter VI are hypothetical and, unlike the examples in this chapter, have not necessarily been examined by the Courts at this stage. Once Chapters V and VI have examined the tension between

564 The EU Institutions' Data Protection Regulation will clarify certain issues in the referred relationship. This will be elaborated in more detail in the relevant context.

public access to documents and the protection of personal data, the way will be clear for a normative analysis of how to resolve these conflicts in Chapter VII.

1. COURT OF JUSTICE OF THE EUROPEAN UNION

1.1 EUROPEAN COMMISSION V BAVARIAN LAGER

The judgment in the so-called Bavarian Lager case was delivered by the Grand Chamber of the Court of Justice of the European Union in the summer of 2010.[565] This case was the first time that the Court of Justice examined the relationship between the Transparency Regulation and the Data Protection Regulation,[566] and is still the only ruling by the highest European court relating to this particular question. The fundamental issue in this case was how to resolve a situation involving conflicting rules. However, principles and rights naturally underlie this conflict.[567] In this particular case, the applicant had asked for the disclosure of documents containing some personal data. As the EU institutions are bound by the Regulations on transparency and the protection of personal data, the issue arising was how to assess the disclosure of personal data which is a part of a public document, based on either Regulation or both.[568]

The General Court[569] had previously annulled the Commission's decision to refuse full disclosure of the minutes of a meeting, granting only partial access. While the General Court decided the conflict in favour of transparency, AG Sharpston took quite a different approach, suggesting that the provisions in the Regulations are not actually contradictory at all. She justified her approach idiosyncratically, creating different categories for access to document requests.[570] However, the Court of Justice did not adopt her Opinion, and it also set aside the judgment of the General Court in so far as it annulled the Commission's decision.

565 Case C-28/08P, *Bavarian Lager*, ECLI:EU:C:2010:378.

566 European Data Protection Supervisor *Public access to documents containing personal data after the Bavarian Lager ruling*.

567 Opinion of AG Sharpston in Case C-28/08, *Bavarian Lager*, ECLI:EU:C:2009:624, delivered 15 October 2009, para 97.

568 According to article 2(3) of Regulation 1049/2001 "*This Regulation shall apply to all documents held by an institution […]* and according to article 3(1) of Regulation 45/2001 *This Regulation shall apply to the processing of personal data by all Community institutions and bodies insofar as such processing is carried out […]*"

569 The Court of First Instance at the time the judgment was delivered.

570 Opinion of AG Sharpston in Case C-28/08, *Bavarian Lager*, ECLI:EU:C:2009:624, delivered 15 October 2009, para 104.

1.1.1 THE FACTS OF THE CASE

The applicant, Bavarian Lager, had requested the minutes of a meeting, including the names of the participants. The Commission had granted partial access to these minutes, but had excluded some names. In essence, Bavarian Lager wanted to import German beer into the United Kingdom, primarily the North of England. However, this turned out to be impossible. This did not reflect the lack of appreciation of German beer in the United Kingdom but were caused by UK legislation, under which it seemed to be quite normal for British pubs to be tied to particular breweries for their beer supplies. However, there was legislation guaranteeing the pubs the right to buy beer from other suppliers under certain circumstances. This so-called "Guest Beer Provision" (GBP) regulated this right and provided the rules that, among other things, specified that the beer bought from other suppliers had to be conditioned in a cask and its alcohol percentage had to be more than 1.2%. Bavarian Lager considered the GBP to fall under the prohibition of Article 28 TFEU as a measure having an effect equivalent to a quantitative restriction[571] on imports, as most beers produced outside of the United Kingdom did not meet the GBP requirements. Bavarian Lager lodged a complaint with the European Commission, which led to the initiation of an infringement procedure against the UK. In the course of these proceedings, the Commission sent a formal notice to the United Kingdom. However, this is where the action against the United Kingdom ended. The decision not to pursue the infringement procedure was based on certain amendments to the GBP by the United Kingdom, under which bottled beer was now assimilated with the cask-conditioned beer. A meeting was held on 11 October 1996 to discuss the GBP, with officers of the Directorate-General for the Internal Market and Financial Services, officials of the United Kingdom Government Department of Trade and Industry and representatives of the Confédération des Brasseurs du Marché Commun. Bavarian Lager had also requested the opportunity to attend this meeting, but had been refused.[572]

The request by Bavarian Lager for the minutes, more precisely the names included, relate to this meeting.[573] In addition to these minutes, Bavarian Lager had also requested disclosure of various other materials such as the submissions of companies and organizations mentioned in this case. After the initial refusal and the exchange of letters between the Ombudsman and the Commission, the Commission granted partial access to these documents, withholding the personal data of those

571 For more on equivalent effect, see, for instance, D. Chalmers, G. Davies & G. Monti, *European Union Law*, (Cambridge, 2010) 744–783.

572 Case T-194/04, *Bavarian Lager v Commission*, ECLI:EU:T:2007:334, paras 15–27.

573 Case C-28/08P, *Bavarian Lager*, ECLI:EU:C:2010:378, para 1.

participants who had either not answered the Commission's inquiries concerning the disclosure of their personal data or had refused disclosure.[574] [575]

Following the General Court's annulment of the Commission's decision, the Commission, supported by the Council and some Member States, appealed to the Court of Justice.[576] The appeal was based on three grounds, two of which the Court of Justice examined together. Of the two arguments examined together, the first was an argument concerning errors in the interpretation and application of Article 4(1)(b) of the Transparency Regulation in declaring that Article 8(b) of the protection of personal data Regulation was not applicable, and the second was the argument that the General Court had made an error in interpreting the condition in Article 4(1)(b) of the Transparency Regulation restrictively, thus excluding the Community legislation on protection of personal data contained in a document from its scope. Given its findings and responses to the first two arguments, the Court of Justice did not examine the third argument.[577]

The Commission argued that the General Court had made errors in law in interpreting the exception concerning the protection of one's personal data.[578] The General Court's interpretation largely reflects the Dworkinian idea of rules.[579] In a very much "all-or-nothing" fashion, the General Court had set aside the provisions of this Regulation entirely. While principles contain dimension, which allows balancing, this is not the case with rules.[580] The Commission was particularly concerned over the omission to consider its Articles 8(b) and 18(a).[581] It must be borne in mind, however, that the General Court's decision did not render these rules void in general but only in relation to the Transparency Regulation and only as far as the data subject's privacy was not at stake. While Dworkin recognizes that rules might well involve exceptions,[582] the General Court's approach could not be explained by this. The General Court examined the application of a particular exception to the Transparency Regulation and decided the case in favour of rules relating to access to documents. While doing this, it did entirely omit the rules laid down in the

574 Case T-194/04, *Bavarian Lager v Commission*, ECLI:EU:T:2007:334, paras 26–28, 34–37.

575 For more on the Ombudsman's contribution, see the Decision of the European Ombudsman on complaint 713/98/(IJH)/GG against the European Commission; a letter from the European Ombudsman to the President of the European Commission, 30.9.2002/7411.

576 Case C-28/08P, *Bavarian Lager*, ECLI:EU:C:2010:378, paras 29–30.

577 Case C-28/08P, *Bavarian Lager*, ECLI:EU:C:2010:378, paras 40–41, 81. For analysis of the judgment of the General Court, see, for instance, H. Kranenborg, "Access to documents and data protection in the European Union: on the public nature of personal data" in *Common Market Law Review* 45 (2008), 1094–1096.

578 Case C-28/08P, *Bavarian Lager*, ECLI:EU:C:2010:378, para 40.

579 R. Dworkin, *Taking Rights Seriously*, (London, 2009) 14–81.

580 See R. Dworkin, *Taking Rights Seriously*, (London, 2009) 22–28.

581 Case C-28/08P, *Bavarian Lager*, ECLI:EU:C:2010:378, paras 45, 47.

582 R. Dworkin, *Taking Rights Seriously*, (London, 2009) 14–81. For the exceptions, see also H. Kelsen, General Theory of Norms, (Oxford, 1991) 126–127.

Community data protection legislation, even if the Transparency Regulation had set a specific requirement to take the said provisions into consideration.

1.1.2 SIMULTANEOUS APPLICATION OF THE TRANSPARENCY AND DATA PROTECTION REGULATIONS

It has already been noted that AG Sharpston suggested that provisions of the two Regulations might not actually be in conflict.[583] As mentioned in Chapter I, Zucca emphasizes that genuine constitutional conflicts need to be distinguished from spurious ones,[584] also noting that conflicts resolved by rational argument must also be distinguished from the genuine conflicts.[585] If AG Sharpston's Opinion had been adopted, the dilemma would have been resolved very much in line with Zucca's thesis; the conflict between these two Regulations being recognized as spurious. Thus, genuine conflict between rights would not exist and the dilemma could be resolved by recognizing the conflict for what it actually is.

However, both the General Court and the Court of Justice did identify a tension between rights even if they took different approaches to solving it. In relation to the more specific provisions, the main disagreement in the Bavarian Lager case seems to relate to the conflict between Article 6(1) of the Transparency Regulation and Articles 8(a) and 18(a) of the Data Protection Regulation. In addition to this conflict, this case provides an example of the tension between the two Regulations at the level of principles in the Dworkinian sense.[586] In this case, the conflict of rules is only a surface-level consequence of a tension in the underlying principles. As such, the solution must be deduced from the underlying levels of law.[587]

The General Court concluded that the full minutes, including the names, did not fall under the exception provided in Article 4(1)(b), which concerns the protection of one's personal data. As this exception was not applicable, the provisions of the protection of personal data Regulation were not applicable either.[588] [589] Thus, under the judgment of the General Court, it seems that the application of these two Regulations in situations such as that of Bavarian Lager, consists of two steps: first,

583 Opinion of AG Sharpston in Case C-28/08, *Bavarian Lager*, ECLI:EU:C:2009:624, delivered 15 October 2009, para 104.

584 L. Zucca, Conflicts of Fundamental Rights as Constitutional Dilemmas, in Brems (ed.) *Conflicts between Fundamental Rights*, (Intersentia, 2008), 24– 26.

585 L. Zucca, Conflicts of Fundamental Rights as Constitutional Dilemmas, in Brems (ed.) *Conflicts between Fundamental Rights*, (Intersentia, 2008), 24– 28.

586 R. Dworkin, *Taking Rights Seriously*, (London, 2009) 14–81.

587 For more on the various levels of law, see K. Tuori, *Kriittinen oikeuspositivismi*, (Helsinki, 2000).

588 Case T-194/04, *Bavarian Lager v Commission*, ECLI:EU:T:2007:334, paras 133–136, 139.

589 See also H. Kranenborg, "*Access to documents and data protection in the European Union: On the public nature of personal data*" in Common Market Law Review 45 (2008), 1094–1096.

whether the exception laid down in Article 4(1)(b) is applicable must be evaluated, and second, if it is, the disclosure of personal data must be evaluated under the provisions of this Regulation.[590]

AG Sharpston adopted the General Court's approach in part. However, unlike the General Court, the AG attempted to provide a more comprehensive approach to solving the dilemma.[591] Given this bold attempt, this Opinion is worth examining, even if the Court of Justice did reject it. The essence of her Opinion seems to lie in the definition of the scope of the Data Protection Regulation and its relation to the Transparency Regulation. Her approach is closely related to the interpretation of Article 3(2) of the Data Protection Regulation. Sharpston notes, for example, that "*the clear implication of Lindqvist is that, as soon as processing of personal data is automatic or partly automatic, it falls within the scope of the data-protection legislation (be that Directive 95/46 or Regulation No. 45/2001). However, a request for disclosure of documents made under Regulation No 1049/2001 is not – as I understand it – treated that way. Rather it is examined individually and manually*".[592] It is not entirely clear how this should be interpreted. It seems as if the AG is assessing how to define the requests for disclosure of documents, i.e. whether the requests for access are to be considered as processing of personal data that falls within the scope of the Data Protection Regulation.

It should first be noted that the definition of processing of personal data as laid down in Article 2(b) of the Data Protection Regulation clearly covers the functions described above.[593] According to Article 2(b), disclosure by transmission, dissemination or otherwise making personal data available are to be considered as processing of personal data, among other things. This would clearly cover the requests for the disclosure of documents as well. The AG's approach would mean that the disclosure of documents should be considered processing of personal data, which partly falls outside of the scope of the Data Protection Regulation. To decide what documents would fall outside its scope, AG Sharpston created two different categories of requests for documents that include personal data.[594] In

590 The European Data Protection Supervisor also supported this approach; see, for example, Pleading of the EDPS in Public Hearing in Case C-28/08P (16 June 2009), available on the internet < http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Court/2009/09-06-16_pleading_C-28-08P_EN.pdf> [last visited 29.9.2011] as well as European Data Protection Supervisor, *Public access to documents containing personal data after the Bavarian Lager ruling*.

591 It ought to be mentioned that the Opinion was found quite exceptional among the various stakeholders, which the requests of the Commission and the European Data Protection Supervisor to re-open the case after the Opinion was delivered clearly indicate. See case C-28/08P*, Bavarian Lager*, ECLI:EU:C:2010:378, paras 35–39.

592 Opinion of AG Sharpston in Case C-28/08, *Bavarian Lager*, ECLI:EU:C:2009:624, delivered 15 October 2009, para 125. See also Case C-101, *Lindqvist*, ECLI:EU:C:2003:596.

593 This did not change with the entry into a force of the EU Institutions' Data Protection Regulation.

594 Opinion of AG Sharpston in Case C-28/08, *Bavarian Lager*, ECLI:EU:C:2009:624, delivered 15 October 2009, paras 158–166.

essence, she distinguished "real requests" from "disguised requests" based mostly on the amount of personal data that the documents covers.[595] However, the Court of Justice stated quite clearly in the Satakunnan Markkinapörssi case that all exceptions to the protection of personal data must be carried out as narrowly as strictly necessary.[596] Excluding some processing of personal data entirely from the scope of the Regulation seems to create even more limitations on the protection of personal data than the broad interpretation of exceptions. It seems to follow that the scope of the Regulation should be interpreted broadly rather than narrowly as suggested in the AG's Opinion. Furthermore, it is not obvious which functions other than requests for access to documents should be excluded if the AG's approach were to be adopted. It appears that there must be other functions containing processing of personal data individually and manually. Such questions could potentially arise at national level. Just consider a bank assessing an application for a loan; it would seem quite risky to state that this processing of personal data falls outside of the scope of the Data Protection Directive as its Article 3(1) is similar to Article 3(2) of the Data Protection Regulation.[597]

AG Sharpston argued in favour of the narrow interpretation that a broad interpretation would unnecessarily restrict the application of Transparency Regulation.[598] While this concern is justified, the correct balance between the two Regulations can be achieved by other means. For instance, one of the founding principles of the Transparency Regulation is that all exceptions are laid down in the Regulation itself. In accordance with well-established case-law, since all these exceptions are to be interpreted narrowly,[599] the provisions of the Data Protection Regulation should be interpreted in light of the founding principles of the Transparency Regulation when a case is examined under its provisions. Thus, simultaneous application of both Regulations should not be read as setting aside the provisions or principles of the Transparency Regulation as such. Furthermore, the distinction between "real" and "disguised" requests for documents does not seem to solve the problem but rather create a new one, since it would be rather difficult to separate the so-called disguised access to document requests from the real ones.

While AG Sharpston's Opinion offers an interesting alternative for solving the dilemma of this thesis, the Court of Justice chose the approach of setting the full

595 Ibid.

596 Case C-73/07, *Satakunnan Markkinapörrsi and Satamedia*, ECLI:EU:C:2008:727, para 56.

597 The same applies regarding the GDPR and new EU institutions' Data Protection Regulation.

598 Opinion of AG Sharpston in Case C-28/08, *Bavarian Lager*, ECLI:EU:C:2009:624, delivered 15 October 2009, para 149.

599 See, to that effect, Case T-20/99, *Denkavit Nederland* v *Commission*, ECLI:EU:T:2000:209, para 45; Case C-64/05 P, *Sweden* v *Commission and Others*, ECLI:EU:C:2007:802, para 66; Joined cases C-39/05 P and C-52/05 P *Sweden and Turco/ Council*, ECLI:EU:C:2008:374, para 36.

application of both Regulations as a founding principle.[600] Despite the merits of the two-step approach adopted by the General Court, the Court of Justice did not accept this approach either, providing its own interpretation of the relationship between the two Regulations. In essence, the focal point in both the General Court and the Court of Justice judgments, and the point of disagreement between the two courts, was the relationship between the Transparency and the Data Protection Regulations.

The Court of Justice found that the General Court had limited the application of Article 4(1)(b) of the Transparency Regulation to only those cases where the privacy or the integrity of the persons concerned were at stake, and in doing so had not taken the EU legislation regarding the protection of personal data properly into account. The Court of Justice went further, stating that "*in acting that way, the General Court disregards the wording of Article 4(1)(a) of Regulation No 1049/2001, which is an indivisible provision and requires that any undermining of privacy and the integrity of the individual must always be examined and assessed in conformity with the legislation of the Union concerning the protection of personal data, and in particular with Regulation No 45/2001*". Before coming to this conclusion, the Court of Justice had also noted that the two Regulations had been adopted around the same time and neither included any provision that would justify displacing the other Regulation.[601] If this had been the case, the legislator would have resolved the tension between two different principles in favour of one, and drafted the provisions accordingly. Thus, no collision of rules would exist, simply an exception to the main rule.[602]

Thereafter, the Court of Justice concluded that in applying the Transparency Regulation in situations where the documents to which the applicant is seeking access include personal data, the Data Protection Regulation becomes applicable as well. The Court of Justice underlined that all of its provisions will apply in these cases in their entirety, including Articles 8 and 18. The Court of Justice concluded that the General Court had dismissed the application of these articles in its judgment.[603] Thus the Court of Justice decided to set aside General Court's decision as far as it annulled the Commission's decision and adopted an entirely different approach to solving the dilemma.

600 Case C-28/08P, *Bavarian Lager*, ECLI:EU:C:2010:378, para 56.

601 Case C-28/08P, *Bavarian Lager*, ECLI:EU:C:2010:378, paras 56, 58–59.

602 As earlier noted, exceptions do not lead to conflict in the Dworkinian sense.

603 Case C-28/08P, *Bavarian Lager*, ECLI:EU:C:2010:378, paras 63, 64.

1.1.3 THE DATA SUBJECT'S RIGHT TO OBJECT TO THE PROCESSING OF DATA RELATING TO HIM OR HER

One of the issues arising in the aftermath of the Court's judgment is how to apply the provisions relating to the data subject's right to object to the processing of personal data relating to him or her. While the Data Protection Regulation contains provisions regulating the consent of the data subject, it also contains another provision, Article 18(a), reflecting the principle of self-determination. This Article provides that the data subject has the right to object to the processing of personal data of this kind. As noted earlier, one of Commission's particular worries related to the non-application of this Article.[604] Article 18(a) declares that the data subject has the right to object at any time on compelling legitimate grounds relating to his or her particular situation. Furthermore, where there is a justified objection by the data subject, the processing in question may no longer involve such data.[605]

According to the judgment delivered by the Court of Justice, these articles are also entirely applicable when assessing the disclosure of the document based on the Transparency Regulation. Thus, the query arising concerns the application of these provisions when a request for access to documents has been made based on this Regulation. In the course of this particular process, the Commission had already given extensive access to documents.[606] The parts of the minutes which the Commission did not release contained the names of the participants at the meeting. However, the Commission had released the names of those participants who had consented to disclosure. This meant that in the end there were five names not disclosed to the applicant, two of whom had refused the disclosure of their data and three of whom the Commission had been unable to reach.[607] However, as noted by some authors, even extensive disclosure of documents might not serve the purpose of public access to documents if the applicant is unable to obtain access to the particular information important to the applicant.[608]

While the disclosure of names can be justified by the consent of the data subject without clear guidelines concerning the simultaneous application of Transparency and Data Protection Regulations, I see that the lack of consent or objection to the

604 This concern had also been expressed by some authors; see, for instance, Kranenborg, "Access to documents and data protection in the European Union: On the public nature of personal data" in *Common Market Law Review* 45 (2008), 1095. This particular issue has not been developed further in the CJEU's later case-law, see case C-127/13 P, *Strack v Commission*, ECLI:EU:C:2014:2250 and case C-615/13 P, *ClientEarth and PAN Europe v EFSA*, ECLI:EU:C:2016:489.

605 The right to object to the processing of data relating to him or her does not cover cases regulated by Article 5 (b) (c) and (d) of Regulation 45/2001.

606 Case T-194/04, *Bavarian Lager v Commission*, ECLI:EU:T:2007:334, para 35.

607 Case T-194/04, *Bavarian Lager v Commission*, ECLI:EU:T:2007:334, paras 35–37.

608 P. Leino, "Just a little sunshine in the rain: The 2010 case-law of the European Court of Justice on access to documents" in *Common Market Law Review* 48 (2011).

processing of data should not lead to the reverse conclusion.[609] The simultaneous application of both Regulations should not impact this question. First, the data subject's consent cannot be considered as an absolute requirement for the processing of personal data.[610] Second, the right to object does not provide an absolute right to decline the disclosure of personal data.[611] The judgment of the Grand Chamber also supports this view. The Court noted that in the absence of convincing arguments or legitimate justification for the application, the Commission was unable to balance competing interests.[612] If the objection should be considered absolute in its nature, there would naturally be no need to balance these competing rights, since the objection would be sufficient.

While the second part of Article 18 clearly contains the procedural right of the data subject to be informed before personal data is disclosed, the first part also contains features of procedural rights,[613] apparently conferring on the data subject the right to be heard and in the case of legitimate reasoning, an obligation for the institution to act accordingly. However, based on the formulation of the right to object, it seems quite clear that Article 18(a) does not provide any right to decline the processing of one's personal data.[614] Thus withholding personal information while giving access to other parts of the document should not be justified solely by the lack of the data subject's consent or objection to the disclosure.

1.1.4 STATING REASONS FOR THE APPLICATION

One of the key elements in the Bavarian Lager case was the obligation to provide reasoning for the application, or the absence of such reasoning. According to Article 8(b) of the Data Protection Regulation, personal data shall only be transferred to recipients if they establish the necessity to have the data transferred, and if there is no reason to assume that the data subjects' legitimate interests might be prejudiced. However, Bavarian Lager was firmly of the view that it should not state the reasons or the necessity for its request. This approach was supported by the European Data Protection Supervisor,[615] and was justified by one of the fundamentals of the access

609 For online disclosure of personal data, see case T-343/13, *CN v Parliament*, ECLI:EU:T:2015:926.

610 R. Bronsword, "Consent in Data Protection Law: Privacy, Fair Processing and Confidentiality" in S. Gutwith; Y. Poullet; P. De Hert; C. de Terwangne & S. Nouwt, *Reinventing Data Protection* (Springen, 2009), 83 –109.

611 This argument will be developed further in Chapters VI and VII.

612 Case C-28/08P*, Bavarian Lager*, ECLI:EU:C:2010:378, paras 77–80.

613 According to Article 18(b), the data subject shall have right to be informed before personal data is disclosed for the first time to third parties or before they are used on their behalf for the purposes of direct marketing, and will be expressly offered the right to object, free of charge, to such disclosure or use.

614 This remains essentially the same under the EU Institutions' Data Protection Regulation.

615 European Data Protection Supervisor "Public access to documents containing personal data after the Bavarian Lager ruling", p. 4.

to documents Regulation; the applicant's right not to be obliged to state reasons for the application.[616] This can be seen as supporting another fundamental principle in this area, the possibility of applying for access to documents anonymously.

When considering that the provisions of Data Protection Regulation were not applicable, as the requirements under Article 4(1)(b) were not met, the General Court held that the applicant did not have to reason their application pursuant Article 6(1) of the Transparency Regulation.[617] This meant that the applicant did not have to do so under Article 8(b) of the Data Protection Regulation either.[618] Thus these two rules could not be applied simultaneously and the General Court resolved the conflict between these rules in favour of transparency. This, as the Commission pointed out, rendered the data subjects' rights laid down in Article 18(a) void.[619]

In adopting an approach different from the General Court, the Court of Justice stated that full application of both Regulations should be ensured and that Article 8(b) should be fully applicable when the institution assesses disclosure of a document based on the Transparency Regulation.[620] However, full application of both Article 6(1) of the Transparency Regulation and Article 8(b) of the Data Protection Regulation does not seem achievable. The applicant either has to reason the application or does not. Anything in between renders Article 6(1) partly void. Thus, there is a clear conflict between the Dworkinian rules, and only one provision can be applied in its entirety. Which one remains applicable is to be decided by deducing the answer from the underlying principles. This question will be further examined, and the circumstances constructing the rules for the application of other principles in the line with Alexy's thesis will be provided later in this thesis. At that stage, the new provisions of the EU Institutions' Data Protection Regulation relating to stating reasons will also be elaborated in more detail.

1.1.5 PERSONS ACTING IN A PROFESSIONAL CAPACITY

The individuals whose personal data was at stake in this case were all acting in a professional capacity, participating in a meeting in the course of their duties. As the European Ombudsman, Jacob Söderman, quite righty noted at the very initial stages of the Bavarian Lager case, there is no "*general right to participate anonymously*

616 See for instance M. Maes, "Le refronte du reglement (CE) n 1049/2001 relatif a l'access du public aux documents du Parlement européenne, du Conseil et de la Commission" in *Revue du Droit de l'Union Européenne* 3 (2008), 584 – 585.

617 According to article 6(1) of Regulation 1049/2001, the applicant is not obliged to state reasons for the application.

618 Case T-194/04, *Bavarian Lager v Commission*, ECLI:EU:T:2007:334, paras 107–109.

619 Case C-28/08P, *Bavarian Lager*, ECLI:EU:C:2010:378, para 47.

620 Case C-28/08P, *Bavarian Lager*, ECLI:EU:C:2010:378, para 63.

in public activities" and the Data Protection Regulation should not be interpreted as implying that this was so.[621] The approach adopted by the General Court reflected the Ombudsman's position: "*In the circumstances of this case, the mere disclosure of the participation of a physical person, acting in a professional capacity, as the representative of a collective body, at a meeting held with a Community institution, where the personal opinion expressed by that person on that occasion cannot be identified, cannot be regarded as an interference with that person's private life.*"[622] Thus the General Court saw professional activities as playing a role when assessing the possible disclosure of personal data. However, AG Sharpston partly disagreed with the General Court, noting for instance that in accordance with the case-law of the ECtHR, the concept of interference with one's private life is broad. [623] This question will be further examined later in this thesis.

In finding that both Regulations are to be applied simultaneously, the Court of Justice did not distinguish between personal data relating to activities carried out in a professional capacity and any other personal data. However, the Court did not examine this aspect of the case in the absence of the reasoning for the application. It is therefore for future case-law to show how to weight professional activities in the context of breaches of privacy.

1.1.6 CONCLUSION IN THE BAVARIAN LAGER CASE

Before the Court's decision in the Bavarian Lager case, it was not clear what provisions are applicable when public access is requested to documents which contain personal data. The Court of Justice clarified that the provisions of the Data Protection Regulation are also to be applied in these cases. However, as the issue was whether its provisions would be applicable at all, the approach adopted by the Court should not be interpreted as giving supremacy to this Regulation over the Transparency Regulation. It is of the utmost importance to note that the Court of Justice also clarified that *full* application of *both* Regulations should be ensured in principle, which seems to return the conflict to the underlying levels of law. This statement naturally also requires the full application of the Transparency Regulation. Furthermore, the principle of transparency and the principles deriving from the right of access to documents cannot be overlooked in cases where access to personal data is based on regulation governing public access to documents. The focal point

621 A letter from the European Ombudsman to the President of the European Commission, 30.9.2002/7411.

622 Case T-194/04, *Bavarian Lager v Commission*, ECLI:EU:T:2007:334, para 128.

623 Opinion of AG Sharpston in Case C-28/08, *Bavarian Lager*, ECLI:EU:C:2009:624, delivered 15 October 2009, paras 153 – 154.

of this discussion after the Bavarian Lager judgment seems to be precisely the dimensions of the said principles.[624]

Furthermore, as the judgment of the Court of Justice focused on the relationship between the two Regulations rather than the actual relationship between the two rights, the judgment cannot be interpreted as giving supremacy to one of these rights over the other. The judgment merely provides some very basic guidelines on how to assess the application of two different Regulations in the situation where the document requested contains personal data. Later case-law has provided some further guidance for interpretation, in particular on stating reasons.[625] These guidelines can be expected to be developed further in future case-law.

While the full application and the equivalence of these Regulations are clear after the Bavarian Lager judgment, the remaining questions concern the role of the reasoning of the application and the data subject's right to object and the importance of professional activities. As a matter of fact, these questions have become even more important as a result of the approach adopted by the CJEU in the Bavarian Lager judgment.

1.2 VOLKER UND MARKUS SCHECKE GBR AND HARTMUT EIFERT V LAND HESSEN

The Court of Justice of the European Union delivered a judgment on 9 November 2010 in the joined cases of Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen.[626] This judgment was an interesting mixture of various questions relating to transparency, expenditure of public funds, protection of personal data and proportionality. Whereas the focal point in Bavarian Lager was the contradictory requirements of two different Regulations, this case centred on the validity of certain articles[627] of Council Regulation (EC) No 1290/2005[628] as amended by Council Regulation No 1437/2007.[629] While in Bavarian Lager, the tension between two different principles emerged at the level of rules, this case provides a very clear example of the tension between the principles. There are no conflicting rules at stake in this case. The proportionality of the underlying principles was questioned

624 For more on dimensions of principles, see R. Dworkin, *Taking Rights Seriously*, (London, 2009) 22–28.

625 Case C-615/13 P, *ClientEarth and PAN Europe v EFSA*, ECLI:EU:C:2016:489; case C-127/13 P, *Strack v Commission*, ECLI:EU:C:2014:2250.

626 Joined cases C-92/09 and C-93/09 *Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen*, ECLI:EU:C:2010:662.

627 Articles 42(8b) and 44a.

628 Council Regulation (EC) No 1290/2005 of 21 June 2005 on financing common agricultural policy (OJ L 209, 11.8.2005, p. 1–25).

629 Council Regulation (EC) 1437/2007 of 26 November 2007 amending Regulation (EC) No 1290/2005 on the financing of the common agricultural policy (OJ L 322, 7.12.2007, p. 1–5).

and, as such, the validity of certain Regulations. This case was also considered in the Grand Chamber, reflecting its importance.[630]

1.2.1 THE FACTS OF THE CASE

The EU legislation obliged a Member State to publish the beneficiaries of certain agricultural funding provided by two different foundations; EAGF[631] and EAFRD[632]. This requirement was a part of the European Transparency Initiative, the underlying aim of which was to reinforce public control over the expenditure of public funds.[633] However, two German farmers, considering that publishing data relating to them violated their right to privacy, lodged a complaint before the national court. The argument of the farmers in the national proceedings seemed to be that there was no overriding public interest served by publishing the amounts[634] they had received from the EAGF or the EAFRD.[635]

The publication of the data was based on certain articles of Regulation 1290/2005. These rules ensure, in particular, that the beneficiaries of funds are informed that some data may be made public and may be processed by auditing and investigating bodies for the purpose of safeguarding the financial interest of the Communities. The Regulation obliged the Member States to publish the beneficiaries of the EAGF and the EAFRD and the amounts received annually by the beneficiaries.[636] [637]

1.2.2 NATURE OF THE PERSONAL DATA

The applicants and complainants in the national proceedings were an agricultural undertaking and a full-time farmer, who could be identified by the way in which they

630 The conclusion of this case will be provided together with the conclusion of the Satakunnan Markkinapörssi case at the end of section 5.1.3.

631 European Agricultural Guarantee Fund.

632 European Agricultural Fund for Rural Development.

633 Communication from the Commission Follow-up to the "European Transparency Initiative" green paper COM 2007 (127) final.

634 The internet site provided by the state of Hesse covered the information on beneficiaries' names, postal codes and the annual amounts of funding.

635 Joined cases C-92/09 and C-93/09 *Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen*, ECLI:EU:C:2010:662, para 74.

636 More detailed rules on the publication of the information on the funds beneficiaries receive are laid down in Commission Regulation (EC) No 529/2008 of 18 March 2008 setting out detailed rules for the application of Council Regulation (EC) No 1290/2005 on publication of information on the beneficiaries of funds deriving from the European Agricultural Guarantee Fund (EAGF) and the European Agricultural Fund for Rural Development (EAFRD) .

637 Joined cases C-92/09 and C-93/09 *Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen*, ECLI:EU:C:2010:662, paras 4, 15–17, 24.

were listed on the internet site.[638] Transmitting or disclosing this data is processing of personal data in the sense of the Data Protection Directive.[639]

The funding received by the beneficiaries was an integral part of their income and, as noted by the Court of Justice, it might form a considerable part of a farmer's total income.[640] Publishing the amounts received could therefore clearly indicate their income levels. There are no clear guidelines in European data protection legislation on how to assess the personal information relating to a person's income. It is evident, however, that information related to one's income does not enjoy the same special treatment as special categories of personal data defined in Article 8 of the Data Protection Directive.[641] In accordance with the earlier case-law of the Court of Justice, the disclosure of data related to an individual's income might well be justified in some cases.[642]

1.2.3 CONSENT OF THE DATA SUBJECT AND RIGHTFUL INTERFERENCE IN ONE'S RIGHT TO PROTECTION OF PERSONAL DATA

Even if the national court saw from the outset that publishing the applicants' names on an internet site breaches their right to protection of personal data, it was not convinced that it was unjustified, seeing that the applicants had consented to publication. The CJEU also examined the significance of this so-called consent. The CJEU noted that the applicants had indeed foreseen that their personal data would be published, but also saw that the applicants had merely stated that they were aware of the requirements to publish the data. Thus, publication was not based on the of the consent of data subjects but on the EU legislation.[643]

Once it was clear that there was interference in their privacy, the CJEU moved on to one of the key issues of the case; it had to examine whether interference in one's right to the protection of personal data could be justified. This right is guaranteed

638 Joined cases C-92/09 and C-93/09 *Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen*, ECLI:EU:C:2010:662, paras 25, 53–54.

639 Directive 95/46/EC of the European Parliament and 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 (OJ L 281, 23.11.1995, p. 31–50).

640 Joined cases C-92/09 and C-93/09 *Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen*, ECLI:EU:C:2010:662, para 58.

641 According to Article 8, Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership and the processing of data concerning health or sex life.

642 Joined cases C-465/00, C-138/01 and C-139/01 Österreichischer Rundfunk and Others, ECLI:EU:C:2003:294.

643 Joined cases C-92/09 and C-93/09 *Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen*, ECLI:EU:C:2010:662, paras 61–64.

by the Charter of Fundamental Rights.[644] However, it is not an absolute right,[645] and must therefore be balanced against other rights and, as noted by the CJEU, "*in relation to its function in society*".[646] The referring national court was of the view that increased transparency, which was the rationale behind the obligation to publish the data, would not in fact enhance prevention of irregularities. It saw that the aim pursued by this legislation was sufficiently protected by other means as there were already control mechanisms in place for this purpose. Thus, the further transparency attained by the Regulation would not bring significant added value to control over the expenditure of public funds, particularly taking the principle of proportionality into consideration.[647]

The dimensions of the underlying principles establishing these rights are of great interest in seeking the correct balance between these rights.[648] It was not clear that the provisions which were challenged contradicted Articles 7 and 8 of the Charter. These articles and the underlying principles had to be assessed in light of the objective of transparency. In this case, this balance had initially been carried out by the legislator and now the Court of Justice took its turn. First, the Court of Justice noted that the internet site containing information on the beneficiaries' names and the exact amounts they received did indeed interfere with their private lives in the sense of Article 7 and fell under the protection of personal data in the sense of Article 8 of the Charter[649]. However, as noted above, one's right to the protection personal data is not absolute. It was therefore necessary to decide whether this interference could be justified. This very much reflects the Dworkinian type of balancing of principles.[650] Throughout the whole case, it was clear that neither Article 7 nor 8 would be void even if the balancing had been decided in favour of transparency. However, how to find the proportional balance between principles still had to be determined. Here, the Court of Justice focused on examining whether the interference was compatible with the legitimate limitations on fundamental rights and freedoms as laid down in the Charter.[651]

---

644 According to Article 8(1) of the Charter, everyone has the right to the protection of their own personal data.

645 For more about absolute rights, see Case C-112/00, Schmidtberger, ECLI:EU:C:2003:333; for further reading, H. Delany & E. Carolan, *The Right to Privacy: A doctrinal and Comparative Analysis*, (Thomson Round Hall, 2008), 58–65.

646 Joined cases C-92/09 and C-93/09 *Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen*, ECLI:EU:C:2010:662, para 48; Case C-112/00, Schmidtberger, ECLI:EU:C:2003:333, para 80.

647 Joined cases C-92/09 and C-93/09 *Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen*, ECLI:EU:C:2010:662, para 30.

648 For more on dimensions of principles, see R. Dworkin, *Taking Rights Seriously*, (London, 2009) 22–28. Also, if the Dworkinian parameters of individual and collective rights are accepted, it provides an interesting perspective on the relation between these two rights. See 90–123.

649 Joined cases C-92/09 and C-93/09 *Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen*, ECLI:EU:C:2010:662, paras 58, 60.

650 R. Dworkin, *Taking Rights Seriously*, (London, 2009) 14–81.

651 In examining the case, the Court of Justice underlined the necessity of evaluating the validity of the provisions

1.2.3.1 Article 51 of the Charter

Guidance on what can be considered legitimate limitations to the rights and freedoms laid down in the Charter is provided in Article 52. Once the Court had established that there was interference with the right to the protection of personal data and that processing the data was not based on the applicants' consent, the Court of Justice went on to determine whether the criteria under Article 52(1)[652] of the Charter were met in this case.[653] Placing the criteria in Article 52 of the Charter in Robert Alexy's framework shows them as the justifying circumstances in considering the weight and dimension of principles leading to a situation where one principle is considered weightier.[654] The Court first examined whether the limitations were regulated by law without losing the essence of the rights which were breached. It then had to assess whether these limitations were in accordance with the general interests of the European Union and in line with the principle of proportionality.[655]

1.2.3.2 Objectives of general interest recognized by the EU

Firstly, the Court of Justice noted that the requirement that the interference be provided by law was clearly met in this case. Secondly, the Court of Justice examined the question of the limitations genuinely meeting the objectives of general interest recognized by the Union.[656] The aim of the Regulation was quite clear. As it was described in the recitals, it was to strengthen public control over the expenditure of public funds by enhanced transparency.[657] Hence, the objective of the Regulations was clear and was not disputed at any stage of the proceedings.

---

laid down in Regulation 1290/2005 and Regulation 259/2008 in light of the freedoms and principles set out in the Charter of Fundamental Rights of the European Union, recalling that it has the same legal force as the treaties.

652 According to Article 52(1) of the Charter, any limitation on the exercise of the rights and freedoms recognized by the Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognized by the Union or the need to protect the rights and freedoms of others.

653 Joined cases C-92/09 and C-93/09 *Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen*, ECLI:EU:C:2010:662, para 64.

654 R. Alexy, *A Theory of Constitutional Rights*, (Oxford, 2010) 100–109.

655 Joined cases C-92/09 and C-93/09 *Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen*, ECLI:EU:C:2010:662, para 65.

656 Ibid, paras 66–67.

657 According to Recital 14 of Regulation 1437/2008, "*making this information accessible to the public enhances transparency regarding the use of Community funds in the [CAP] and improves the sound financial management of these funds, in particular by reinforcing public control of the money used. Given the overriding weight of the objectives pursued, it is justified with regard to the principle of proportionality and the requirement of the protection of personal data to provide for the general publication of the relevant information as it does not go beyond what is necessary in a democratic society and for the prevention of irregularities*". Recital 6 of Regulation 259/2008 contains a similar statement.

Furthermore, the Court of Justice pointed out that the principle of transparency itself had been recognized in the Treaty on European Union as well as in the Treaty on the Functioning of the European Union.[658] Very significantly for this study, the Court specifically reiterated its earlier statement that "*the principle of transparency enables citizens to participate more closely in the decision-making process and guarantees that the administration enjoys greater legitimacy and is more effective and more accountable to the citizen in a democratic system*".[659] Consequently, the wording borrowed from the recitals of the Transparency Regulation can be considered an integral part of the settled case-law. Thus, there seems to be no doubt as to the status of the principle of transparency at this stage. Since the principle of transparency seems to have gained the necessary institutional support in the Dworkinian sense in the European Union legal framework, the remaining question is therefore how to balance this principle with other principles.[660]

The Court concluded that the Regulations served the goals of the principle of transparency.[661] Thus, the Court first established that this principle is indeed a general interest recognized by the European Union and, secondly, that the Regulations were based on that general interest.

1.2.3.3 Proportionality

Once it was established that the criteria concerning the legislation and the objectives of general interest recognized by the Union had been met, it was still necessary to see whether the measures taken had been proportional and necessary in the sense of Article 52(1) of the Charter. The Court of Justice examined this question in some detail, taking the following facts into consideration. First, the applicants had argued that publication of the funding information enabled third persons to draw conclusions about their income[662]. Second, as noted earlier, the publication of the information undoubtedly increased transparency of the use of the agricultural aid in question and increased people's ability to observe how the public funds were being used. Third, determining whether the measures were necessary required that these

658 Joined cases C-92/09 and C-93/09 *Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen*, ECLI:EU:C:2010:662, para 68.

659 Case C-41/00 P, *Interpoc v Commission*, ECLI:EU:C:2003:125, para 39; Joined cases C-92/09 and C-93/09 *Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen*, ECLI:EU:C:2010:662, para 68. For a Case C-41/00 P, *Interpoc v Commission*, see also S. Kadelbach, "Case Law A. Court of Justice", in *Common Market Law Review* 38 (2001), 184–186.

660 R. Dworkin, *Taking Rights Seriously*, (London, 2009) 40.

661 Joined cases C-92/09 and C-93/09 *Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen*, ECLI:EU:C:2010:662, paras 71, 75.

662 The funding formed 30% and 70% of the total annual income of the applicants concerned.

measures be reconciled with the fundamental rights to protection of personal data and respect for private and family life.[663]

In establishing the balance between transparency and the protection of personal data, the Court – with references to its earlier case-law – underlined that derogations and limitations relating to the protection of personal data must apply only where strictly necessary.[664] The Court of Justice had indeed stated this previously in the Satakunnan Markkinapörssi and Satamedia case.[665] However, this statement of the Court of Justice should not be taken as a general approach. Rather, it is significant to note that the statement was issued in the context of balancing two fundamental rights. Furthermore, the Court of Justice came to this conclusion only after having first stated that "*in order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary, first, to interpret notions relating to that freedom, such as journalism, broadly*".[666] Consequently, limitations on data protection are to be imposed in a balanced relation to other rights.

Finally, the Court of Justice held that the institutions had not ascertained that publishing the names of the beneficiaries would not exceed what was actually necessary to attain the goal.[667] The Court of Justice justified its conclusion by pointing out that there was no distinction based on the duration, frequency, nature or the amount of aid received. It also elaborated more restricted ways of publishing names than the way that was actually adopted. The Court also underlined that more limited publication did not seem to provide an insufficient or incorrect picture of the funds granted. In addition, the Court emphasized that "*no automatic priority can be conferred on the objective of transparency over the protection of personal data*". While doing this, it did however reiterate that taxpayers, i.e. the general public, did indeed have the right to know how public funds are spent.[668] [669]

Thereafter, the Court of Justice concluded that the Commission and the Council had not properly balanced the EU's interest in transparency and the appropriate use of public funds against the protection of personal data and respect for private and family life. Thus, the Court declared Articles 42(8b) and 44a invalid as far as they concern natural persons and are not drafted in more detail, making a distinction between the particular issues described in the judgment.

---

663 Joined cases C-92/09 and C-93/09 *Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen*, ECLI:EU:C:2010:662, paras 58, 73, 75, 76, 77.

664 Joined cases C-92/09 and C-93/09 *Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen*, ECLI:EU:C:2010:662, para 77.

665 Case C-73/07, *Satakunnan Markkinapörrsi and Satamedia*, ECLI:EU:C:2008:727, para 56.

666 Ibid.

667 Joined cases C-92/09 and C-93/09 *Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen*, ECLI:EU:C:2010:662, para 86.

668 Ibid., paras 79, 81–83, 85.

669 Joined cases C-465/00, C-138/01 and C-139/01 Österreichischer Rundfunk and Others, ECLI:EU:C:2003:294.

The Court of Justice also underlined that the fact that the data relates to activities of a professional nature was not relevant in this case. This approach was justified by the case-law of the European Court of Human Rights,[670] which has clarified that the right to privacy might cover activities of a professional nature[671] and should therefore not be limited simply because the data relates to such activities. While keeping in mind that the right to privacy does cover these activities, it should be remembered that interfering with one's right to the protection of personal data, or privacy for that matter, can be justified in some circumstances.

Even though the Court of Justice did find that certain provisions of the Regulation interfered with the rights of natural persons beyond what was necessary, it did not see this as being the case vis-à-vis legal persons.[672] As previously mentioned, the identity of the natural persons behind the legal entities was recognizable in this case. The Court of Justice held however that there are significant differences between natural and legal persons, reiterating that legal persons are under stricter obligations to publish data relating to them in comparison with natural persons from the start. The Court of Justice also took a rather practical approach by stating that obliging the national authorities to verify whether there are identifiable natural persons behind legal persons would cause an unreasonable administrative burden.[673]

1.3 THE TIETOSUOJAVALTUUTETTU V SATAKUNNAN MARKKINAPÖRSSI OY AND SATAMEDIA OY CASE

To provide a more comprehensive picture of the underlying principles examined in the Markus Schecke and Hartmut Eifert case, it is important to consider the Satakunnan Markkinpörssi case briefly as well.[674] The Court of Justice delivered this preliminary ruling in December 2008. While the Schecke and Eifert case concerned disclosure of information giving a clear indication of the incomes of farmers, the Satakunnan Markkinapörssi case relates to publication of the taxation information of a vast number of ordinary citizens.[675]

---

670 Joined cases C-92/09 and C-93/09 *Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen*, ECLI:EU:C:2010:662, para 59.

671 ECtHR 16 February 2000, *Amann v Switzerland* (2000–II) and ECtHR 4 May 2000, *Rotaru v Romania,* (RJD 2000–V).

672 Joined cases C-92/09 and C-93/09 *Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen*, ECLI:EU:C:2010:662, paras 87– 88.

673 Ibid., para 87.

674 Case C-73/07, *Satakunnan Markkinapörrsi and Satamedia*, ECLI:EU:C:2008:727. The case was also tried before the European Court of Human Rights. The European Court of Human Rights found that there was no violation of Article 10 regarding freedom of expression. ECtHR 27 June 2017, *Satakunnan Markkinapörssi Oy and Satamedia Oy v Finland* (ECLI:CE:ECHR:2017:0627JUD000093113).

675 For an analysis of the case, see W. Hins, "Case C-73/07, Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy, Judgment of the Grand Chamber of 16 December 2008" in *Common Market Law*

1.3.1 THE FACTS OF THE CASE

Satakunnan Markkinapörssi Oy and Satamedia Oy had run a business publishing the taxation information of ordinary citizens for several years, information which is in the public domain in Finland and which Satakunnan Markkinapörssi had collected from various Inland Revenue Offices. The information had then been published in records taking the form of a journal, organized by income and municipality. While many other journals publish taxation information as well, the activities of Satakunnan Markkinapörssi differed in the extent of their data, with the taxation information on nearly 1.2 million taxpayers[676] being published. The information contained the first and last names of the person and their income, listed in alphabetical order. The publications contained hardly anything other than the taxation information with some rare exceptions.[677]

Following complaints by some individuals claiming that their right to privacy had been breached, the national Data Protection Ombudsman scrutinized Satakunnan Markkinapörssi's activities, concluding that its processing of personal data did not comply with national data protection legislation. The Data Protection Ombudsman then sought an order to ban this processing of personal data. In the course of these proceedings, the Supreme Administrative Court of Finland referred the case for a preliminary ruling in Luxembourg.[678]

1.3.2 LEGITIMATE INTEREST

The Supreme Administrative Court posed several questions to the Court of Justice, including questions related to the definition of processing of personal data and the definition of journalistic purposes. The Court of Justice took the view that the data processing described in the previous section could be considered as having been done for journalistic purposes. Whether it was done for this reason was left for the national court to decide. Hence, the processing of this information was to be considered justified if certain criteria were met.[679]

In its decision, the Court of Justice provided some guidelines for the interpretation of journalistic purposes. It also emphasised that freedom of speech is indeed of the utmost importance in a democracy. It follows that all notions related to freedom of speech, such as journalism, must be interpreted broadly. Once this was clearly

Review 47 (2010), 215–233.

676 This figure should be set in the context of the whole population in Finland, which is 5.3 million.

677 Case C-73/07, *Satakunnan Markkinapörrsi and Satamedia*, ECLI:EU:C:2008:727, paras 25–26, 28.

678 Ibid., para 31–32.

679 Ibid., paras 34, 50, 61–62.

established, the Court underlined that all exceptions to the right to the protection of personal data must be defined as narrowly as possible to achieve a fair balance between the two fundamental rights.[680]

At the national level, the Supreme Administrative Court took the view that Satakunnan Markkinapörssi's activities were not conducted for journalistic purposes. [681]

1.3.3 THE NATURE OF THE DATA

As already noted, information related to income does not enjoy special treatment under European data protection legislation. Whereas the information in the public domain gave indications of farmers' incomes in the Schecke and Eifert case, in the Satakunnan Markkinpörssi case the information disclosed explicitly revealed the income of the data subjects. Nevertheless, the Court of Justice did not see processing such data as being contrary to data protection legislation provided that it was carried out solely for journalistic purposes.[682] This approach mirrored the approach the Court took in the Rundfunk case, where the Court decided that disclosing annual income information is not to be considered contrary to EU data protection legislation provided that it is necessary to guarantee the proper management of public funds.[683]

1.3.4 CONCLUSION OF THE SCHECKE AND EIFERT AND SATAKUNNAN MARKKINAPÖRSSI CASES

The Court of Justice of the European Union was balancing the underlying principles of data protection with other values in these two cases. There was no conflict of rules at the surface level, but rather a tension arising at the underlying levels with an effect on the validity of some legislation. In these judgments, the Court of Justice set some basic guidelines, or Alexy's circumstances, which would dictate the correct

680 Case C-73/07, *Satakunnan Markkinapörrsi and Satamedia*, ECLI:EU:C:2008:727, para 56–62.

681 KHO 2009: 82. The Supreme Administrative Court elaborated its decision quite extensively. Among other things, it reasoned its decision as follows. Where the register that has been created for journalistic purposes is published extensively, almost in its entirety, and even if the publication takes place in separate community-based pieces, this type of processing of personal data cannot be considered as being for journalistic purposes. This reasoning was based on national legislation, which required some minimum standards to be met when personal data was processed this reason. The Supreme Administrative Court held that when the information is released as extensively as in this case, these minimum standards are not actually met, and the processing cannot be considered as carried out for journalistic purposes.

682 Case C-73/07, *Satakunnan Markkinapörrsi and Satamedia*, ECLI:EU:C:2008:727, para 65.

683 See joined cases C-465/00, C-138/01 and C-139/01 Österreichischer Rundfunk and Others, ECLI:EU:C:2003:294.

balance between these principles in this and similar cases. These circumstances could be called conditions of balancing in line with Alexy's theory.[684]

The Court of Justice of the European Union examined transparency in relation to public funding in these cases. Today, when Europe is again on the edge of financial crisis, transparency on expenditure of public funds should be put under even closer scrutiny. Even if the Court of Justice saw the underlying principles of one's right to privacy and the protection of personal data as weighing more than transparency in the Schecke and Eifert case, this was subject to certain qualifications. First and foremost, the Court of Justice did not consider the underlying principles of data protection more weighty in general. To start with, according to the Court, information relating to legal persons could still be published as before. Under the Data Protection Directive, this information might be personal data if it allows identification of the persons behind the legal undertaking.[685] Consequently, the personal data was divided into two categories subject to different criteria for publication. Besides, the Court of Justice did not take the view that information relating to private farmers could not be published at all, seeing the current legislation as disproportionate in respect of its aims and methods. Thus, according to the Court, the disclosure of this information should be done under more detailed provisions, providing clearer limits and boundaries. In the more recent Manni case for example, the CJEU did not see the public access to personal data stored by public authorities as disproportionate from the outset.[686]

Reading this judgment together with the Court's judgment in the Satakunnan Markkinapörssi case, it does not seem likely that the Court's intention would have been to take a definite stand against the disclosure of personal data relating to the expenditure of public funds, but rather to underline the importance of correct balancing between the two principles. In Satakunnan Markkinapörssi, since the Court of Justice did consider that the taxation information on numerous people could be released if it was done for journalistic purposes, disclosing personal data relating to public expenditure can be justified under certain circumstances.[687] However, it should not be done lightly, and in a way which compromises privacy and the right to protection of personal data only to the extent strictly necessary in order to achieve the other goals. In other words, balancing must be carried out in accordance with Hesse's doctrine of practical concordance.

---

684 R. Alexy, *A Theory of Constitutional Rights*, (Oxford, 2010) 100–109.

685 According to Article 2(a) of Directive 95/46, 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'), an identifiable person being one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. This did change with the entry into force of the GDPR. The GDPR specifies that it does not apply to undertakings established as legal persons.

686 Case C-398/15, *Manni*, ECLI:EU:C:2017:197.

687 See also joined cases C-465/00, C-138/01 and C-139/01 Österreichischer Rundfunk and Others, ECLI:EU:C:2003:294.

2. THE EUROPEAN COURT OF HUMAN RIGHTS

2.1 GENERAL

Even though the European Convention on Human Rights has no provisions regulating the protection of one's personal data or access to documents, the European Court of Human Rights has recognized these rights through other articles of the Convention.[688] One of the landmark judgments in this respect was Gaskin v United Kingdom.[689] The ECtHR based its decision on Article 8, concerning the right to privacy, and rejected the claim based on Article 10 which concerns freedom of speech. The judgment strongly reflects the data subject's right to access his or her personal data. Mr Gaskin had requested access to some official files containing information on his childhood. The national authorities had eventually granted him access to files where the contributors to them had given their consent for disclosure, but denied him access to the rest. The European Court of Human Rights held that since the right to privacy imposes some positive obligations on the state, beside the negative obligation not to interfere with one's private and family life, the applicant should be entitled to have access to these documents containing information relating to him. Even if the decision mostly relates to the processing of personal data, it also reflects some aspects of access to document principles. First, the access was sought to official documents apparently drafted by civil servants or someone in a similar position. Second, the objection to releasing the documents by some contributors did not finally stop the Court from coming to the conclusion that it did. This approach has been confirmed in more recent case-law as well. For instance, in Turek v Slovakia, the Court held that there had been a deficiency in the national procedure where Turek sought the opportunity to correct information relating to him.[690]

While the previous cases relate to the right to the protection of personal data, public access to documents (contrary to access to public documents) was at stake in Guerra v Italy, a case related to environmental information.[691] The state's liability for dissemination of information which is not otherwise directly accessible was largely

688 There also are two international Conventions drawn up in the framework of the Council of Europe relating to these rights; Convention 108 for the Protection of Individuals with Regard to Automatic Processing of Personal Data and Convention 205 on Access to Official Documents (the latter has not come into force yet).

689 ECtHR 7 July 1989, *Gaskin v the United Kingdom*.

690 ECtHR 14 February 2006, *Turek v Slovakia*, (2006–II), See also Case C-345/06, *Heinrich*, ECLI:EU:C:2009:140. In the Heinrich case, the Court of Justice held that obligations to citizens cannot be based on legislation which is not accessible to the public. For an analysis of the said case, see M. Bobek, "*Case C-345/06, Gottfried Heinrich, Judgement of the Court of Justice (Grand Chamber) of 10 March 2009*" in Common Market Law Review 46 (2009) 2077–2094.

691 ECtHR 19 February 1998, *Guerra and Others v Italy*, (1998–I).

discussed in the case.[692] However, the ECtHR has not taken a definite stand on this question, but rather resolved the cases by applying Article 8 of the Convention.[693]

It seems clear that the legitimate interest of the applicant has a central role to play in the ECtHR's case-law. The interest might be individual as it was in Gaskin v United Kingdom, or it might have a more a general character as in Guerra v Italy.

2.2 GILLBERG V SWEDEN

As previously noted, while public access to documents is not a clearly defined human right under the European Convention on Human Rights, the ECtHR has considered this type of right through other rights protected by the Convention. Even if some authors[694] have claimed that attempts to interpret Article 10 of the Convention as covering the right of access to public documents have failed, the recent case-law of the Court shows that access to public documents is indeed considered equivalent to human rights protected by the Convention. This right can either be considered as a human right protected by the Convention or equivalent to these rights as an important element of a democratic society.

The right balance between privacy and rightful interference in the name of democracy was the main issue considered by the ECtHR in Gillberg v Sweden.[695] After the Third Section had decided that there was no violation, the Grand Chamber accepted the case for reconsideration based on the applicant's request for referral.[696] Given that this is quite exceptional, the case is clearly of wider significance.[697] It is also of interest to note that the judgment of the Third Section was not unanimous, the decision on the alleged violation of Article 8 being split 5:2.

Even if the proceedings at the national level were largely focused on the relationship between the protection of personal data and access to official documents, and the ECtHR very similarly examined whether there had been a violation of Articles 8 or 10 of the Convention, the approach of the ECtHR was very different

692 Ibid.

693 ECtHR 19 October 2005, *Roche v United Kingdom,* (2005–X).

694 See, for instance, A. Sharland, "The Influence of the European Convention on Human Rights, etc.", in Coppel (ed.) *Information Rights*, (London, 2007), 88 – 100.

695 ECtHR 2 November 2010, *Gillberg v Sweden*.

696 The case is currently pending before the Grand Chamber of the ECtHR. The oral hearing took place on 29th of September 2011.

697 According to Article 43 of the European Convention on Human Rights "*any party to the case may, in exceptional cases, request that the case be referred to the Grand Chamber. Thereafter a panel of five judges […] shall accept the request if the case raises a serious question affecting the interpretation or application of the Convention […], or a serious issues of general importance*". The Grand Chamber delivers approximately 20 judgments per year. This figure also comprises the cases relinquished by the Chamber. Available on the internet < http://www.echr.coe.int/NR/rdonlyres/8E30641D-6122-439C-9E08-3C712C02A379/0/ListarrGC.pdf > [last visited 25.7.2011].

from that of the national courts. The ECtHR was assessing whether the rights of applicants had been violated under Articles 8 or 10, not the actual relationship or the tension between these articles. However, this does not mean that the issue was not raised by the ECtHR. In examining the procedure before the national court, the ECtHR naturally also touched on the question of how to assess the relationship between the right of access to documents and the right to protection of personal data.

2.2.1 THE FACTS OF THE CASE

The applicant, Mr Christopher Gillberg, lodged a complaint to the ECtHR, arguing that his rights guaranteed by the European Convention on Human Rights had been violated. Mr Gillberg, a Swedish psychiatry professor and Director of the Department of Child and Adolescent Psychiatry at the University of Gothenburg, had conducted research involving children suffering from ADHD[698] or DAMP[699]. The research sample contained 141 children. When the research material was collected, the participants – or in the early stages their parents – were told that the information obtained would not be further disclosed and were even promised absolute confidentiality.[700] The research material included a vast number of records, test results, interview replies, questionnaires and video and audiotapes, which had served as the basis for several doctoral theses. According to Mr Gillberg, when he took up his duties as the head of the Department of Child and Adolescent Psychiatry, the university's Ethics Committee had set confidentiality as a precondition for its research permit.[701]

In 2002, an application to access these research documents was filed. The applicant, named K in the judgment by the Third Section of the European Court of Human Rights, noted that she had no interest in the personal data which these files contained. She was interested in the material because she wished to examine the method used in the previous research as well as the evidence on which the previous conclusions of the research had been based. The University of Gothenburg declined access to the research material, basing its decision on two grounds. Firstly, K had not demonstrated any relation between her own research and the research material in question. Secondly, the material contained vast amounts of personal data. Disclosing this data would be likely to harm the individuals concerned.[702]

698 Attention-Deficit Hyperactivity Disorder.

699 Deficits in Attention, Motor Control and Perception.

700 ECtHR 2 November 2010, *Gillberg v Sweden*, paras 1, 3, 7–9, 4.

701 Ibid., paras 7–8.

702 Ibid., para 15.

K appealed the decision to the Administrative Court of Appeal, which referred the case back to the university for closer consideration; the university was to assess whether the documents could be released under certain conditions or after erasing the personal data from the research material. The university refused to grant access to the research documents, stating that they could not be released after the removal of personal data and also rejected the possibility of disclosing the information under stipulated conditions.[703]

Meanwhile, a second application to access to the research documents was filed. Applicant E was also conducting research of his own. The university refused to disclose the documents to him, the decision being based on the same grounds as the previous refusal. Both E and K appealed to the Administrative Court of Appeal, which concluded in February 2003 that both had a legitimate interest in the material, and that the documents should therefore be disclosed under conditions decided by the University of Gothenburg.[704]

This judgment of the Administrative Appeal Court and the subsequent refusal by the Supreme Administrative Court to examine the application was followed by a bureaucratic merry-go-round. Briefly, the university considered certain conditions as appropriate provided that the data subjects gave their consent to disclosure, but the applicants did not agree with some of the conditions and appealed to the Administrative Court of Appeal. The Court made some adjustments to the conditions and maintained its initial position on disclosure. Similar procedural rounds took place twice after February 2003. It seems that in these considerations the legitimate interest of the applicants was always assessed. After the last round before the Administrative Court of Appeal, some colleagues of Mr Gillberg destroyed the research material.[705]

These actions led to criminal proceedings against Mr Gillberg and some of his colleagues. Mr Gillberg was given a suspended sentence and was fined.[706] At the Court of Appeal, Mr Gillberg had, for instance, claimed that because of Article 8 of the European Convention on Human Rights, his actions should be considered excusable since disclosure of the information would have violated the rights of the data subjects under Article 8 of the Convention.[707]

703 Ibid.

704 ECtHR 2 November 2010, *Gillberg v Sweden*, paras 16–17.

705 Ibid., paras 18–31.

706 The amount of the day fines defines the seriousness of the crime, according to Swedish penal code (brotssbalk 2 §). The range varies from 30 to 150.

707 Ibid., paras 32–33.

2.2.2 THE RULING OF THE THIRD SECTION OF ECTHR

One of the questions examined by the Third Section was whether the outcome of the criminal proceedings against Mr Gillberg breached the rights guaranteed by Articles 8 and 10 of the Convention.[708] Thus, the Court was balancing the underlying principles, particularly of Article 8, to decide whether the outcome of the case was justified. Mr Gillberg argued that this was not the case as confidentiality, the precondition for his research, had not been sufficiently considered by the national courts.[709] He claimed that this fact should have been taken into account as a mitigating circumstance.[710]

The Third Section eventually concluded that there was no violation of Article 8 of the Convention, specifying that the basic question was whether the conviction in question was necessary in a democratic society and finding that this was the case. The Third Section stated that "*[…] the fact that the Court of Appeal did not take into account as a mitigating circumstance the fact that the applicant had attempted to protect the integrity of the participants in the research does not, in the Court's view, overstep the state's margin of appreciation in this case*". In its evaluation of the case, the Third Section also examined the question of the proportionality of the conviction, but did not find against the state in this respect either.[711]

2.2.3 PRIOR AGREEMENT AND THE DATA SUBJECT'S CONSENT

Two of the fundamentals of this case were prior agreement and the data subject's consent, both of which played a significant role in balancing the principles of privacy and transparency.

One of the corner-stones of Swedish access to documents legislation is the obligation to assess each request for access to an official document individually and in terms of the content of the document. There are no block exemptions or other similar instruments under the Swedish legislation.[712] It naturally follows that any agreement deviating from this should be considered void. Further, all exceptions to the general principle of access to a document must be laid down in law.[713] Therefore

708 Ibid., paras 65, 75.

709 Ibid., para 76, 85.

710 Ibid., para 111.

711 ECtHR 2 November 2010, *Gillberg v Sweden*, paras 116–119.

712 Tryckfrihetsförordning (1949:105).

713 In other words, exceptions to the law cannot be granted through legal instruments below the level ordinary law, for instance, through decisions of various governmental agencies.

civil servants cannot impose limitations differing from the law, nor can they make such things as decisions on secrecy without the backing of the legislation.[714]

When the determination of whether to disclose the document must be based on its content, assurances not to disclose documents before they have even been drawn up do not seem to be in line with this requirement. Also, as public access to a document is a right guaranteed by the Swedish Constitution,[715] it does seem unlikely that two parties could conclude an effective agreement limiting a third party's right of access to official documents.

The assurances given by the applicant were given more weight in the dissenting opinion of judges Gyulumyan and Ziemele, who also considered the assessment of these assurances by the national court insufficient.[716] It seems that the importance and weight given to these assurances can be considered slightly misleading. As noted, it seems that the applicant could not validly conclude an agreement which would limit a third party's right of access, so that the assurance itself cannot have a substantial role in the considerations. However, the underlying reasons for these assurances should have been thoroughly considered. The assurance had presumably been given because the research project included processing a vast amount of very sensitive personal data and, even more importantly, sensitive personal data relating to children. It does not seem likely that it would have been possible to collect this data without the consent of the data subjects.

Seemingly then, the researcher and data subjects had agreed that the research data would not be further disclosed. The assurance given to the participants or their parents was formulated as follows: "*All data will be dealt with in confidence and classified as secret. No data processing that enables the identification of your child will take place. No information has been provided previously or will be provided to teachers about your child except that when starting school she/he took part in a study undertaken by Östra Hospital, and its present results will, as was the case for the previous three years ago, be followed up*". The research material was collected over a long period, and another assurance of confidentiality was made later: "*participation is of course completely voluntary and as on previous occasions you will never be registered in public data records of any kind and the data will be processed in such a way that nobody apart from those of us who met you and have direct contact with you will be able to find out anything at all about you*".[717]

Thus, these assurances had been offered prior to the data subjects' consent, forming the basis for the actual consent. A data subject's consent reflects

714 A. Bohlin, *Offentlighets principen*, (Stockholm, 1996) 154–157.

715 Tryckfrihetsförordningen 2 Kap. Om allmänna handlingarnas offentlighet; 1 § Till främjande av ett fritt meningsutbyte och en allsidig upplysning skall varje svensk medborgare ha rätt att taga del av allmänna handlingar. *Lag (1976:952)*.

716 ECtHR 2 November 2010, *Gillberg v Sweden*, paras 2–3.

717 ECtHR 2 November 2010, *Gillberg v Sweden*, paras 13–14.

self-determination, the underlying value of privacy and data protection.[718] Even if the right to self-determination is an important element of data protection, it is not absolute.[719] Therefore the personal data can in some cases be processed without the consent of the data subject, for instance, by disclosing it to third parties. These factors should be considered when examining the significance of the consent given by the data subjects.

In this case, the data subjects had given their consent for processing of their personal data. When doing so, they were under the impression that the data would not be further disclosed. An interesting question in connection with this is, of course, whether these data subjects would have given their consent knowing their data might be further disclosed and, even further, if the data subjects had not given their consent, whether there would have been any other means of obtaining this data.

Keeping in mind that the consent of the data subject cannot be considered an absolute prerequisite for the processing of personal data, the next question relates the scope of the consent. What is the exact scope of the consent that the data subject has given? What did he or she consent to? There were not at the time precisely defined guidelines for the data subject's consent in the European legislation, as seemed to be the case in the Swedish national legislation as well.[720] The reasonable expectations of the data subject, two elements of which can be distinguished, should play a significant role in seeking an answer to this question. Firstly, if the further disclosure could have been considered reasonably foreseeable when the original consent had been given, the formal absence of the consent alone should then not be considered as an obstacle to further disclosure. It does not seem as if there would have been any substantial changes in the legal framework relating to the public access legislation between the time the consents were given and the request for the documents was made. Any future request should therefore have been reasonably foreseeable at the time the consent was given. Secondly, if the further disclosure of the personal data can be considered consistent with the original processing of the data, the absence of consent should not necessarily be an impediment to the processing of personal data. It does seem that both E and K would have used

718 For more about self-determination, see, for instance, A. Rouvroy & Y. Poullet, "The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the importance of Privacy for Democracy", in S. Gutwith; Y. Poullet; P. De Hert; C. de Terwangne & S. Nouwt, *Reinventing Data Protection* (Springen, 2009), 45 – 76.

719 A. Rouvroy & Y. Poullet, "The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the importance of Privacy for Democracy", in S. Gutwith; Y. Poullet; P. De Hert; C. de Terwangne & S. Nouwt, *Reinventing Data Protection* (Springen, 2009), 45–76. See also instance Case C-524/06, *Heinz Huber*, ECLI:EU:C:2008:724.

720 Convention 108 does not contain any provisions relating to the data subject's consent. The Data Protection Directive and the Data Protection Regulation define consent as any freely given specific and informed indication of his or her wishes by which the data subject signifies his or her agreement to personal data relating to him or her. The Swedish legislation, *personuppgiftslagen* (1998 : 204), contains provisions relating to the consent of the data subject (for instance, 9 § and 10 §); however, it does not give more precise guidelines for the definition of consent.

the material for research purposes, i.e. for purposes similar to the original one. Disclosing the research material to other researchers under similar conditions of confidentiality could hardly be considered inconsistent with the original use of the personal data in question.

2.2.4 THE CONCLUSION IN GILLBERG V SWEDEN

Besides offering a broader European context for solving the dilemma of data protection and access to public documents, Gillberg v Sweden offers some useful tools for deciding when interference with privacy can be considered justified. It also suggests how to assess the meaning of prior agreement, the data subject's consent and legitimate interest.

Firstly, it seems that the prior agreement argument cannot overrule the right of public access to documents. It is also quite clear that two parties cannot conclude an agreement restricting a third party's fundamental rights with binding effect – the right of access to public documents in this case. The absurdity of the whole idea becomes even more glaring if the situation is compared with other restrictions on fundamental rights through agreements between two individuals. Two people agreeing that a third will not have the right to a private life or right to a fair trial would be just some examples. Thus, the agreement itself does not seem to create sufficient grounds for refusal to disclose documents; the assessment of the disclosure must be carried out based on the information that the documents contain. Nevertheless, the circumstances related to this prior agreement should have been closely scrutinized.

Secondly, the impossibility of prior agreement being decisive also derives from one of the basic principles of the right of public access, namely, from an individual examination of the content of the documents. This approach is clearly adopted in the Swedish legislation. It seems that the Third Section of the ECtHR confirmed this approach in stating that the criminal proceedings against Mr Gillberg were not disproportionate and that they were necessary in a democratic society. Moreover, as the entire case related to conflict between data protection and access to public documents, the judgment can also be read as recognizing that in a democratic society access to public documents can be a legitimate restriction to the right to the protection of one's personal data.

3. CENTRAL QUESTIONS RAISED BY THE EUROPEAN CASE-LAW

This section will now recap and draw together the main questions raised by the case-law examined in this chapter. First, the central dilemmas raised by the Bavarian Lager judgment will be discussed: stating reasons for the request for access to documents and the data subject's consent. The focus will then move to the significance of the role played by professional activities in this context. This second question is of paramount importance for the overall focus of this study as it gives indications on setting the criteria for the disclosure of personal data.

3.1 LEGITIMATE INTEREST AND STATING REASONS FOR THE REQUEST FOR ACCESS TO DOCUMENTS

The legitimate interest of the applicant has gained more importance as a consequence of the recent case-law of the Court of Justice.[721] The requirement to state reasons for the request leads naturally to assessment of the legitimate interest of the applicant. This being taken into account in assessing the disclosure of the document leads to a situation in which the same document might have been disclosed to different extents to different applicants. It also seems to follow that established Council practice of disclosing the documents on Council internet pages cannot continue as such. Also, as the Court of Justice stated in the Satakunnan Markkinapörssi and Satamedia case, published personal data remains within the scope of the data protection regulation regardless of previous publication.[722] This leads to the interesting question of how to assess situations in which personal data has been released based on access to document legislation.

Another interesting view, of course, is that according to Article 8(b) of the Data Protection Regulation, personal data shall only be transferred to recipients who establish the necessity for this transfer, and if there is no reason to assume that the data subject's legitimate interests might be prejudiced. However, when someone applies for access to a document, the applicant could be satisfied with the opportunity to examine the document *in situ*. If Article 8(b) is to be taken literally as regards the part concerning the data *transfer*, studying the document *in situ* would not fall under the Article. Therefore, strict interpretation of Article 8(1) would not hinder the applicant having access to this data as long as it is not transferred but is merely

721 See also Case C-139/07 P, *Technische Glaswerke Ilmenau GmbH*, ECLI:EU:C:2010:376.

722 See also Case C-131/12, *Google Spain and Google Inc*, ECLI:EU:C:2014:317 and Case C-73/07, *Satakunnan Markkinapörrsi and Satamedia*, ECLI:EU:C:2008:727.

saved and viewed in the original data bank. Consequently, a narrow interpretation of Article 8(b) seems to allow viewing this information as long as it is not transferred. Naturally, law must be interpreted in accordance with its intention. This question will be further elaborated in the concluding chapter together with the provisions of the new EU Institutions' Data Protection Regulation.

3.1.1 REASONING OF THE APPLICATION

In terms of actual rules, the legitimate interest of applicants is obviously relevant when the question of justifying the application arises. As has been noted above, requests for documents do not need to be argued under the Transparency Regulation. This is a quite natural approach as the Regulation governs public access to documents. Parallel to the Transparency Regulation, there are several Regulations governing party access.[723] These two partially linked concepts, public access and party access, must obviously be distinguished from each other.

It seems as if it follows from the Bavarian Lager judgment that the applicant should from now on state reasons for receiving the personal data possibly contained in the documents as well.[724] This seems to be contrary to the Court's earlier ruling, in which the Court stated "*the particular interest of an applicant in obtaining access to documents cannot be taken into account by the institution […]*".[725] It ought to be noted however that a different issue was at stake in that case. It is naturally not possible to assess whether there has been a legitimate interest which can be considered as creating the necessity required by the Data Protection Regulation if the application has not been reasoned. This approach does seem to create two significant problems. First, the applicant cannot be aware of this requirement to state reasons. An ordinary citizen filing an application under the Transparency Regulation can hardly be expected to be aware of the recent case-law of the Court of Justice. Second, it is very likely that the applicant is not even aware that the document requested contains personal data. In other words, the applicant is required to establish reasons for disclosure of data the content of which the applicant does not know. The situation has some similarities to the obligation on institutions to determine whether there is an overriding public interest in disclosure of a document under some of the exceptions of the Transparency Regulation.[726] In these cases, it

723 The inadequate framework of party access regulation means that Regulation 1049/2001 is often used as way to get information by parties to different cases as well.

724 For reasoning of application, see in particular Case C-615/13 P, *ClientEarth and PAN Europe v EFSA*, ECLI:EU:C:2016:489, paras 53–61.

725 Case C-266/05 P, *Sison v Council*, ECLI:EU:C:2007:75.

726 Joined cases C-39/05 P and C-52/05 P *Sweden and Turco/ Council*, ECLI:EU:C:2008:374, para 49.

is also indeed quite likely that the institution itself is in a better position to assess the possible reasons in favour of the disclosure of the names.

3.1.2 PUBLIC ACCESS TO A DOCUMENT OR ACCESS TO PUBLIC DOCUMENTS

Another interesting point about the question of legitimate interest concerns the question of public access to documents v access to public documents. When access to a document is open to the general public, legitimate interest can hardly play a significant role. The CJEU has concluded in its recent case-law though that reasoning cannot be too general. According to the CJEU public interest as such would be too general to justify transfer of personal data.[727] This being said, it ought to be noted that legitimate interest could have relevance at a general level in determining the existence of an overriding public interest, for example.

Once the legitimate interest of the applicant is to be examined, the right of public access to documents seems to turn into the right to access public documents. To make the difference clearer, it could be described as the individual's right of access to official documents.

To date, the Court of Justice has not examined whether some individual interest could be considered general by nature. Naturally, this would mean that these personal interests would reflect general interests which could be considered so substantial that they might constitute an overriding public interest. For instance, the Council has often noted that an applicant's personal interests are irrelevant to examining the applications.[728] If the document is to be disclosed, it will be so *erga omnes*, thus the public will have access to the document. Now, after the Bavarian Lager judgment, this approach will have a new twist. If one of the corner-stones of access to documents legislation is to be re-evaluated, it ought to be asked why it could not work in favour of the applicant as well.

3.2 CONSENT OF DATA SUBJECT

All four cases examined take a quite different approach to the data subject's consent. Both Schecke and Eifert and Satakunnan Markkinapörssi and Satamedia were related to publishing information indicating the income of ordinary citizens. While in Schecke and Eifert the Court of Justice noted that data subjects had been informed

727 Case C-127/13 P, *Strack v Commission*, ECLI:EU:C:2014:2250, para 108. However, Recital 28 of the renewed EU Institutions' Data Protection Regulation clarifies that the transparency of Union institutions can justify disclosure of data.

728 For Council's *erga omnes* practice, see B. Driessen, *Transparency in EU Institutional Law: A Practitioner's Handbook*, (Kluwer 2012) 44.

of the future disclosure of the information, this did not have relevance in the final outcome. The heart of the question was the legitimacy of certain Regulations and the processing of data was based on legislation, not on the consent of the data subjects. As for Satakunnan Markkinapörssi and Satamedia, the Court of Justice did hold that the data processing activities conducted by Satakunnan Markkinapörssi and Satamedia could be considered legitimate in the sense of the Data Protection Directive if the sole objective of those activities was disclosure for public information, opinions and ideas. The Court of Justice left it for the domestic court to determine whether the activities could be considered as falling under these headings. However, the consent of data subjects was not considered at any stage of the case.

In comparison to all of other cases examined in this chapter, the data subjects in Gillberg v Sweden would seem to have the strongest case when it comes to consent. Despite this, it played very little role. The European Court of Human Rights never assessed this aspect and it was apparently not examined by the domestic courts either. Of the four cases examined, the Gillberg v Sweden case seems to be the only one in which the data was collected purely on the basis of the data subjects' consent in the first place. In both Schecke and Eifert and Satakunnan Markkinapörssi and Satamedia, the collection was based on legislation; in Bavarian Lager, the data had been collected in the course of professional activities. It even seems possible to conclude that in the last three cases, anticipation of disclosure of the personal information of the data subjects would most likely have had no effect on their participation. However, the awareness of the future transmission of data in Gillberg v Sweden might have had an effect on the data subjects' willingness to participate. Another question is, of course, how the content of the consent should be assessed. This question was tentatively elaborated in the section relating to Gillberg v Sweden and will be further explored in the concluding chapter. In Bavarian Lager, the question was rather the data subjects' right to object to the processing of data related to them, even if consent did play a role in this case as well. This question is examined more closely in the concluding chapter, together with the question of the legitimate interest of the applicants, as these two questions are closely linked.

3.3 PROFESSIONAL ACTIVITIES

The question of the significance of data being collected while the data subjects are carrying out their professional activities was not answered in the four cases considered here, nor are there any other cases that could provide a clear answer this question. While this section will provide some first remarks on this question, it will be further elaborated in Chapter VII.

While the General Court took a firm stand, stating that mere disclosure of data relating to participation at a meeting in the course of professional activities did not

breach the data subjects' right to privacy, the Court of Justice did not confirm this approach.[729] While the Court of Justice did not examine the reasoning of the General Court in this respect, it did annul the General Court's decision in so far as this decision annulled the Commission's earlier decision in the case. As for the Schecke and Eifert, the Court of Justice simply noted that the fact that the information related to the professional activities of the farmers was not fundamental to the case. Schecke and Eifert differs significantly from the Bavarian Lager case in terms of the nature of the disclosed data. While the question in Bavarian Lager concerned data relating to participation in a meeting hosted by an institution, the information in Schecke and Eifert gave indications of farmers' income. The essential objective behind the disclosure also differs in these two cases. In Bavarian Lager, the main objective was to know who had participated in a meeting at which a decision was made that affected the applicants' rights. In Schecke and Eifert, the information was to be released to guarantee appropriate expenditure of public funds. To put it differently, the disclosure of the data in Bavarian Lager was in itself the objective and purpose of the request, whereas in Schecke and Eifert it was a means to achieve some other goals. Furthermore, in Schecke and Eifert the Court of Justice did not see obstacles to the disclosure of the data once some additional safeguards were imposed.

The European Commission gave its proposal for the Regulation of the European Parliament and of the Council regarding public access to the European Parliament, Council and Commission documents after the General Court's Bavarian Lager judgment. Even if it was specifically the Commission who appealed to the Court of Justice, it does seem as if the Commission approved the General Court's approach to the disclosure of personal data relating to the exercise of professional activities. The Commission noted in its proposal that the Data Protection Regulation had been considered too restrictive, specifically concerning persons acting in a public capacity. Furthermore, according to Commission proposal "*names, titles and functions of public office holders, civil servants and interest representatives in relation with their professional activities shall be disclosed unless, […]*".[730] Hence, it might not be clear how to assess the disclosure of personal data related to professional activities in light of the current case-law, but it does seem that most of the relevant institutional stakeholders agree that professional activities are relevant when it comes disclosing the information.

729 See also case C-615/13 P, *ClientEarth and PAN Europe v EFSA*, ECLI:EU:C:2016:489, paras 27–35.

730 Proposal for a Regulation of the European Parliament and the Council regarding public access to European Parliament, Council and Commission documents, COM (2008) 229 final, p. 19.

4. CONCLUSION

On the face of it, the four cases discussed in this chapter have significant differences and present very different legal dilemmas. Nonetheless, some common and recurring issues can be identified. First, the most important similarity is that all cases reflect a balance between two fundamental rights, or rights equivalent to fundamental rights. While balancing the underlying principles was apparent in all cases, in Bavarian Lager the dilemma emerged at the level of competing rules.

As the Bavarian Lager study has shown, even if the CJEU did take the full application of both Regulations as a starting point, this does not seem achievable. The dilemma does not seem to be solvable by defining its scope in the line with AG Sharpston's propositions either. As a result, the basic question raised in the aftermath of this judgment is to what extent the request for public documents should be reasoned.[731] This question is closely related to the applicant's legitimate interest. Another question of equal importance is how to assess the data subject's right to object to the processing of personal data or the weight given to the data subject's consent.

While stating reasons for the application and the data subject's consent have arisen as central dilemmas in applying the Transparency and Data Protection Regulations simultaneously, the case studies have also indicated how to resolve them. Rightful interference with the protection of personal data was at stake in the Schecke and Eifert and Satakunnan Markkinapörssi cases. As the case studies have shown, transparency and journalistic purposes, for example, can be considered legitimate reasons for limiting one's right to the protection of personal data. While the more detailed criteria justifying this interference vary in the cases examined, some elements of more general criteria can be distinguished, such as the significance of professional activities or public control over expenditure of public funds.

While similar conclusions on rightful interference with the protection of personal data can be drawn from the Gillberg case, another fundamental issue argued in this case study was the weight given to prior agreement. As it was shown, it should not hinder later disclosure of the information as such.

731 See also case C-615/13 P, *ClientEarth and PAN Europe v EFSA*, ECLI:EU:C:2016:489. The CJEU has clarified in that case that the public interest as such remains on too general a level to be considered adequate reasoning. In the said case the CJEU accepted quite detailed reasoning as a basis for the data transfer. However, this is a question which is likely to be further elaborated in the future case-law, in particular in light of Recital 28 of the EU Institutions' Data Protection Regulation.

CHAPTER VI

THE TENSION BETWEEN ACCESS TO DOCUMENTS AND DATA PROTECTION

This chapter will address the tension between transparency and data protection legislation in a more detailed and concrete manner, and it will introduce some practical examples in which this tension is apparent. The focus will be on conflicting data protection and transparency provisions in the European legal framework, and more precisely, the tension between the rules of the Transparency Regulation and the EU Institutions' Data Protection Regulation. Both of these Regulations are applied by the EU institutions and some of the situations which will be discussed in this chapter have already occurred in practice.

As discovered earlier in Chapter I, the potential conflict between rights and principles arises on the level of conflicting rules, and this chapter will now focus on such cases. While it is clear that these are only examples of issues pertaining to the surface level of law, at the same time it is equally clear that the solution for the conflict must be deducted from the deeper levels.[732] At this stage only the tension between rules will be studied. It must be borne in mind that the collision of rules does not necessarily indicate that there would be a collision of principles or rights, and even less a collision of fundamental rights.[733] The tension between the rights and underlying principles will be examined in more detail in the concluding chapter.

1. OVERLAPPING REGULATIONS

The Transparency and EU Institutions' Data Protection Regulations are partially overlapping. Before the entry into force of the EU Institutions' Data Protection Regulation none of the Regulations contained any provisions to stipulate how to assess the relationship of the Transparency Regulation and the former Data Protection Regulation. This did not reflect the legislator's lack of information; interrelated references to these Regulations can be found in the recitals of the said

732 For the three levels of legal order see Kaarlo Tuori *Critical Legal Positivism* (Dartmouth Publishing, 2002).

733 See Chapter I.

Regulations.[734] Some Member States have adopted an approach where personal data which is stored in official registers is disclosed on the basis of the public access to documents legislation.[735] However, such an approach has not been incorporated in European Union law, not by the Regulations nor by the case-law of the Court of Justice. Instead, the Court of Justice has underlined that, in principle, both Regulations should be fully applied.[736]

This being the case, the situations where both Regulations will be simultaneously applied has to be identified first. Only after that can an attempt to find a balance between the examined principles be made. Previously, situations of conflict examined by the European Courts were studied. Now, these situations will be complemented with other situations where the tension is apparent, even if not yet actualized in the form of concrete court cases. First, it will be examined to what extent the scopes of the said Regulations overlap, and thereafter, situations in which the rules collide will be construed.

1.1 SCOPE OF APPLICATION

When the Transparency Regulation and the EU Institutions' Data Protection Regulation are studied conjointly, the scope of application must be analyzed first.

The scope of Transparency Regulation covers "*all documents held by an institution, that is to say, documents drawn up or received by it and in its possession, in all areas of activity of the European Union*". Thus all documents held by Union institutions fall within the scope of the Transparency Regulation.[737] Article 2 of the EU Institutions' Data Protection Regulation clarifies that the scope of application covers "*the processing of personal data by all Union institutions and bodies*". Furthermore, some specified areas are excluded from the scope, such as the processing of operational personal data by Europol and the EPPO.[738]

For the purposes of this thesis, two elements of the scopes can be identified. The first element is what is covered by the Regulations, i.e. documents and the

734 Recital 15 of the Data Protection Regulation and Recital 11 of the Transparency Regulation. The EU Institutions' Data Protection Regulation stipulates that Union institutions and bodies shall reconcile the right to protection of personal data with the right of access to documents in accordance with the Union law (article 9(3)). The new Data Protection Regulation does not contain any rules providing supremacy for either of the Regulations either.

735 A. Wallin & P. Nurmi, *Tietosuojalainsäädäntö*, (Jyväskylä, 1991) 185–188; see also laki viranomaisen toiminnan julkisuudesta 21.5.1999/621.

736 Case C-28/08P, *Bavarian Lager*, ECLI:EU:C:2010:378, para 56.

737 Regulation (EC) No 1049/2001 of the European Parliament and the Council of 30 May 2001 regarding public access to European Parliament, Council, and Commission documents (OJ L 145, 31.5.2001, p. 43–48).

738 Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1–22).

processing of personal data. The second element is the stakeholders who have to apply the said Regulations. The first element will be examined together with a more precise assessment of personal data and the document in section 1.2. The stakeholder element will be examined now.

The scope of the Transparency Regulation currently covers only the institutions, while the Data Protection Regulation covers Community bodies as well. However, this difference is in effect minor, for two reasons. Firstly, the European Commission has encouraged all of its agencies etc. to adopt decisions regulating access to their documents. A great number of the different agencies and similar bodies have adopted such decisions.[739] Secondly, the Commission's proposal for the new Transparency Regulation includes different bodies and agencies in the scope.[740] The legal basis on which the Transparency Regulation is based did not allow the extension of the scope to other bodies and agencies, but this was changed with the Lisbon Treaty. The legal basis laid down in EU primary law, in the Treaty on the Functioning of the European Union, now enables the extension of the scope.[741] In the difficult negotiating process for the recast of the Transparency Regulation, the extension of the scope has been one rare thing on which an agreement has been reached.[742]

In conclusion, the scope of application of the two Regulations overlaps significantly. Even if there might be some minor differences, the simultaneous application of the both Regulations is inevitable as far as the material scopes of the Regulations overlap. This would be the case when an application for a document which contains personal data has been filed. The more interesting question is therefore how to distinguish personal data from a document, if it is even possible.

1.2 DEFINITION OF DOCUMENT AND PERSONAL DATA

Having established that the scopes of the EU Institutions' Data Protection Regulation and the Transparency Regulation overlap, the next step is to examine whether personal data, which forms only a part of a document should be considered personal data which falls within the scope of the EU Institutions' Data Protection Regulation and secondly, and even more interestingly, whether a register containing solely

739 See for example the decision (25 March 2009) by the European Chemical Agency on the implementation of Regulation (EC) 1049/2001 of the European Parliament and of the Council regarding public access to documents to European Parliament, Council and Commission documents.

740 Commission Proposal for a Regulation of the European Parliament and the Council regarding public access to European Parliament, Council and Commission documents, COM (2008) 229 final, p. 5.

741 Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union (OJ C 326, 26.10.2012, p. 1–390), article 15.

742 See document 14549/11, Brussels, 23 September 2011.

personal data could be considered a document and, as such, within the scope of the Transparency Regulation.

The scope of the EU Institutions' Data Protection Regulation has been defined widely. The second paragraph of Article 2 of the Regulation stipulates that it applies "*to the processing of personal data wholly or partly by automated means, and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system*".[743] This formulation makes the scope wide for two reasons. First, it seems that the only personal data that falls outside of the scope are some casual data in manually-maintained files. However, the mere fact that this manually-maintained file might form a part of filing system in the future suffices to render the personal data in scope of the EU Institutions' Data Protection Regulation. This leads to a situation where the exclusion of certain personal data from the scope the Regulation is a rather marginal question. The second reason for this relates to the processing of personal data by automated means, or even partly automated means. There is hardly any processing of personal data carried out in any other manner. The increasing use of different applications of new technology makes the references to manual processing a moot point. A Follow-up question is, of course, how to define automated data processing. Should word processing, for example, be considered automated processing of personal data? This is an issue which has been addressed and assessed for example by the Advocate General in the course of the Bavarian Lager case.[744] AG Sharpston had a fair try at solving the tension between the Transparency and the former Data Protection Regulations by focusing on the content of the concept of automatic processing of personal data.[745] However, the Court of Justice did not adopt AG Sharpston's approach. The Court did not confirm the suggestion that when "*dealing with a request for access to documents, […] [a] human brain is still directing the technology, just as the handyman still manipulates the electric drill that has replaced the brace and bit. In my view, such a sequence of operations, in which the individual human element plays such a preponderant part and retains control throughout, should not be considered to be 'the processing of personal data … partly by automatic means' within the meaning of Article 3(2) of Regulation No 45/2001. […]*"[746] Accepting this baseline would have had far-reaching consequences, going beyond the relationship between the Transparency Regulation and Data Protection Regulation. Nevertheless, the Court did adopt a different approach and

743 Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1–22).

744 Opinion of AG Sharpston in Case C-28/08, *Bavarian Lager*, delivered 15 October 2009.

745 Ibid., paras 104–147.

746 Ibid., paras 144–147.

it does not seem too bold to state that basically all personal data is covered by the EU Institutions' Data Protection Regulation in line with the Court's case-law.[747]

Two different types of situations where documents contain personal data are studied next. First, situations in which the document contains some casual personal data are studied. Thereafter, situations in which the document is formed nearly solely from personal data will be studied.

In the context of the first type of situations, the document refers to what is more traditionally considered a document. For this purpose, the baseline idea is that some names contained in a document are not the whole content of the document but only minor part, for example mentioned in the text. When a document contains personal data, the CJEU's case-law expects the principles of both the Transparency Regulation and the Data Protection Regulation to be fully applied.[748] As I argued earlier, it follows that in these cases the disclosure of the document must be assessed in a two-step process. First, other parts of the document must be examined solely under the Transparency Regulation. After this examination has been carried out, the disclosure of the personal data in the document must be examined under the Transparency Regulation and the EU Institutions' Data Protection Regulation. I must underline that this second step of the assessment cannot be based solely on the EU Institutions' Data Protection Regulation, as the Transparency Regulation must be applied simultaneously. Any other interpretation would be contrary to the Court's ruling. Thus, the document is divided into two sections, one which contains personal data and the rest of the document. The suggestion on how to do this will follow in the concluding chapter.

The second type of situation occurs when an applicant requests information which is basically only personal data. The Dennekamp case is an example of such a situation, and this request was tried before the General Court. Dennekamp had requested information on the MEPs who had participated in an additional pension scheme, which was available for Members of the European Parliament. The requested information covered only personal data. The question of whether this information was a document in the meaning of the Transparency Regulation was never addressed. Instead, the reasoning of the General Court culminated in the question of whether the applicant should have provided reasons for the disclosure of the document and whether the European Parliament had justified its refusal appropriately. Thus, the General Court decided the case on the basis of the Court of

747 See for example case T-121/05, *Borax Europe v Commission,* ECLI:EU:T:2009:64; Case T-166/05, *Borax Europe Ltd. v Commission*, ECLI:EU:T:2009:65; case T-436/09, *Julien Dufour v European Central Bank*, ECLI:EU:T:2011:634, para 90; case C582/14, *Patrick Breyer v Bundesrepublik Deutschland*, ECLI:EU:C:2016:779.

748 Case C-28/08P*, Bavarian Lager*, ECLI:EU:C:2010:378, para 56.

Justice's Bavarian Lager judgment and, in the absence of reasoning for the request, decided the case in favour of the European Parliament.[749]

When the Dennekamp judgment is read together with the General Court's Dufour judgment[750], it does seem clear that the definition of document covers all personal data, regardless of the manner which the data has been stored or saved. The Dufour judgment made it clear that even when such pieces of information would not form a coherent entity, the information is to be considered document. The information can be dispersed and still be considered a document in the meaning of the Transparency Regulation. The adopted approach is very broad, and it basically leads to the conclusion that all information is to be considered a document.[751] The General Court concluded that separate words, characters, lists, catalogues or figures, for example, can be considered a document. Furthermore, it underlined that length cannot be considered relevant when assessing whether the information at hand is to be considered a document.[752] Consequently, one name or set of names can be considered a document.

The General Court did not assess in the Dufour case whether a databank as such can be considered a document.[753] However, this question is irrelevant when it comes to the definition of personal data. European data protection legislation sees personal data as clearly separate from databanks. Examining the content of the concept of databanks would mostly relate to the processing of personal data, which is not the focus of this thesis.

In conclusion, two different types of requests for documents containing personal data can be distinguished. The first category contains the so-called traditional documents, i.e. documents which contain only some personal data. As argued earlier, these requests must be assessed in a two-step process. The documents in the second category essentially contain only personal data. These requests should be assessed in their entirety based on both Regulations, the Transparency Regulation and the Data Protection Regulation.

1.2.1 DISPERSED INFORMATION

It was earlier argued that even when information is fragmented and dispersed in different registers, this information should be considered a document in the meaning of the Transparency Regulation. The General Court confirmed this approach by

749 Case T -82/09, *Dennekamp v Parliament*, ECLI:EU:T:2011:688.

750 Case T-436/09, *Julien Dufour v European Central Bank*, ECLI:EU:T:2011:634.

751 Ibid., paras 91–94.

752 Ibid., paras 91–94, 108–115.

753 Case T-436/09, *Julien Dufour v European Central Bank*, ECLI:EU:T:2011:634.

stating that "*[…] the Kingdom of Denmark and the Republic of Finland are correct in their contention […] that anything that can be extracted from a database by means of a normal or routine search may be the subject of an application for access made pursuant to Decision 2004/258*".[754] Hence, storing information in a fragmented format would not enable the controller to avoid obligations deriving from the Transparency Regulation. In other words, storing the information in a dispersed format does not form a basis for refusing the disclosure of information. This is rather clear as far as the concept of document is examined solely based on the Transparency Regulation. However, assessing this situation simultaneously based on the EU Institutions' Data Protection legislation, some additional elements have to be acknowledged.

To start with, the EU Institutions' Data Protection Regulation specifies that "*personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes*".[755] Solely disclosing personal data based on the Transparency Regulation should not be considered incompatible with the original purposes for which the personal data was initially collected. This issue will be elaborated further later in this thesis. But when the personal data is collected from different databanks and then combined, the situation becomes more complicated. One of the driving forces behind the European data protection regime has been the fear of effective data processing technologies, and how, for example, combing different data from different registers would impact on the data subjects' privacy. When combining data from different registers the question would not relate only the disclosure of information but also how to assess the new information. I would be quite reluctant to argue that combining personal data as described was in line with the data protection regime.

1.2.2 LEGAL BASIS FOR THE PROCESSING OF PERSONAL DATA

All processing of personal data must have a legal basis. Even publicly available data can be processed only when there is a sufficient legal basis for the processing. To illustrate this on a more practical level, two examples from the CJEU's case-law can be studied: the so-called Google v Spain case and the Satamedia case.[756] In both of

754 Case T-436/09, *Julien Dufour v European Central Bank*, ECLI:EU:T:2011:634, para 153.

755 The Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39–98).

756 Case C-131/12, *Google Spain and Google Inc*, ECLI:EU:C:2014:317 and Case C-73/07, *Satakunnan Markkinapörrsi and Satamedia*, ECLI:EU:C:2008:727. For legal basis, see also Case C-13/16, *Rigas satiksme*, ECLI:EU:C:2017:336. For legal basis when personal data is disclosed, see case C-127/13 P, *Strack v Commission*, ECLI:EU:C:2014:2250, paras 101–103.

these cases the controller was processing personal data which was already legally in the public sphere.

In the first case, Google was searching information from the internet and made a list of links based on information which it had found mechanically. In its assessment the CJEU saw that even if the original source of information could not be ordered to delete or to rectify the information, the secondary processor, i.e. Google in this case, was liable to erase links which referred to outdated information. In the Google v Spain case, the original source of information was a newspaper. This newspaper had published information of seizure in accordance with the national legislation; the national law even required publication of such information. The Court's judgment leads to a situation where the original information is still available on the internet, but this information cannot be sought based on the name of the person. Only if someone is searching information of the seizure, which took place over 10 years ago, could this information be found. The Court's approach creates quite a heavy administrative burden on the controller. The controller has a duty to erase links to the information, which is available through other sources, and they even have to take the role of "guardian of the information". The Court's decision puts the controller in a position where they can essentially decide what information is available to the public. There might even be a danger of links being erased, which should be available to the public. And this is a flaw that is more difficult to detect than having incorrect or outdated information on the internet. Who would know to make a claim relating to information which cannot be found easily on the internet? Setting these pragmatic questions aside and looking solely at the balancing carried out by the Court between the protection of one's personal data on the one hand, and freedom of speech and information on the other, one must accept that the Court did find quite a delicate and yet fair balance between these rights.[757] The data subject does have the right to have outdated or incorrect information rectified. On the one hand, outdated information is not always incorrect, yet from the data subject's viewpoint it would be disproportionate to be assessed based on very old information. On the other hand, history should not be rewritten. Thus, the original source of information should not be abolished nor changed, but finding this information can be made harder.

In the second case, Satamedia published vast amounts of taxation information. Taxation information is in the public sphere in Finland. All the newspapers publish taxation information, but Satamedia's publications contained more taxation information, with a very low yearly income limit and contained hardly any journalistic content. It was indisputable that the personal data which Satamedia processed was in the public sphere. It ought to be noted that it was *legally* publicly

757 For a systematic analysis on reconciliation of data protection rules with freedom of speech in EU member states, see D. Erdos "European Union Data Protection Law and Media Expression: Fundamentally off Balance" in *International and Comparative Law Quarterly* 65 (2016), 139–183.

available, i.e. it was not information which would have been leaked and thereafter published. The outcome of the Court's judgment was that Satamedia was able to process the personal data if it was carried out for journalistic purposes. The national Supreme Administrative Court saw that processing of personal data carried out by Satamedia could not be considered journalistic and therefore Satamedia could not process the personal data.[758] Thus even if it was clear that anyone has the right to have taxation information from the taxation office, this did not create a sufficient legal basis for further processing of the said data. The conclusion drawn in this case is very much like the outcome in the Google case when it comes to the availability of the information. Finding the said information in the taxation office does take more effort than simply googling it or sending an SMS to a certain phone number. It is clear that for someone to go to a taxation office to search for his neighbour's income information, for example, differs from simply searching for it on the internet.

Both examined cases reflect situations where publicly available personal data must be processed in accordance with the data protection legislation. The first requirement for data processing is a sufficient legal basis. Lawfulness of the data processing is regulated in Article 6 of the GDPR. Processing of personal data is lawful only when some of the legal bases which are defined in the said Article are met. Processing of personal data in the public sector would be mostly based on points (c) and (e) of the said Article.[759] In other words, "*processing is necessary for compliance with a legal obligation to which the controller is subject*" or "*processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller*". When controller is processing sensitive data, some of the qualifications laid down in Article 9 also have to be met.[760] The EU Institutions' Data Protection Regulation contains corresponding legal bases.

The requirement to have a legal basis for the processing of personal data does not create a conflict between the data protection requirements and the public's access to documents. The GDPR provides the Union or national legislator with the possibility to set a legal basis in national (or Union) law for data processing carried out in the public interest. Public access to documents, is to a great extent, in the public interest.[761] In other words, the applicant does have a legal basis for the data processing when seeking the information from the institutions. However, this legal basis does not suffice for further processing of the personal data. In other words, the applicant may not for example combine this information with other information.

758 See KHO 2009: 82.

759 For public sector processing of personal data and T. Pöysti, Trust on Digital Administration and Platforms, in *Scandinavian Studies in Law* 65(2018), 339, 353.

760 Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1–88).

761 Joined cases C-39/05 P and C-52/05 P *Sweden and Turco/ Council,* ECLI:EU:C:2008:374.

Google v Spain clearly illustrates this. Unless, of course, there is another legal basis for the further processing of the personal data; this could be, for example, journalistic purposes. This being said, the question arises whether it is the institution which should assess if grounds for further processing exist. I see that an institution's duties are fulfilled when it has ensured that the disclosure meets the requirements set by the Transparency and the Data Protection Regulation. Supervising the later data processing falls under the responsibility of the Data protection authorities.

2. COLLIDING RULES

This section elaborates different situations where there is an apparent tension between data protection and transparency provisions. Some of these situations have been touched upon when the most central judgments delivered by the European Courts were examined earlier. This section will now address these situations in more detail. This section will first discuss access to one's own personal data. This is followed by more fundamental questions, namely purpose limitation and further transmission of personal data, and the data subject's right to object. After these fundamental issues have been covered, the question of stating reasons for the application will be addressed.

2.1 ACCESS TO ONE'S OWN PERSONAL DATA

The Transparency Regulation does not contain specific party access rules. Nor does it contain specific provisions regarding the data subject's right to obtain information regarding him or herself. This leads to a situation where the EU Institutions' Data Protection Regulation provides wider access to the information than the Transparency Regulation when the applicant is the data subject. In other words, the applicant has wider access to his own personal data based on the EU Institutions' Data Protection Regulation than in the Transparency Regulation.

The tension between the said provisions occurs when a person requests access to a document containing the applicant's own personal data and has filed the request based on the Transparency Regulation. Transparency Regulation does not address this situation differently from any other situations where the requested document contains personal data, i.e. someone else's personal data. Thus, the data subject does not have privileged access to his own data. However, based on the EU Institutions' Data Protection Regulation, one has privileged access to his or her own personal data. Even if the applicant would not be entitled to have access to the document

based on the Transparency Regulation, they might have that right under the EU Institutions' Data Protection Regulation.[762]

This leads to a situation where applying the EU Institutions' Data Protection Regulation instead of the Transparency Regulation, would lead to a more transparent approach. Furthermore, the Charter of Fundamental Rights endows data subjects with the "*right of access to data which has been collected concerning him or her*". Thus, the data subject should not be refused access to his personal data solely because they have filed the application based on the Transparency Regulation. Instead the data subject should be provided with an effective manner to execute his or her fundamental right.

When assessing how to handle the situations described above and how the principle of good administration influences this assessment, a comparison could be drawn from the institutions' obligation to evaluate whether there is an overriding public interest.[763] In other words, the institutions could be expected to actively guide the applicant to ask for the information under the EU Institutions' Data Protection Regulation instead.

2.2 PURPOSE LIMITATION PRINCIPLE AND FURTHER TRANSMISSION OF PERSONAL DATA

The second example of colliding rules, namely the further transmission of personal data, has been touched upon in the case-law, but not addressed as such. This is a question which occurs repeatedly, for example, when the confirmatory applications for access are examined by the Council. An often-repeated argument is that access to a document – or more precisely to the personal data in the said document – cannot be granted because releasing the data would violate those provisions of the Data Protection Regulation which concern further transmission of personal data.[764]

Before examining this question in more detail, some fundamental remarks have to be made. First, if this argument was accepted as such, it would lead to a situation where all requests for access to documents containing personal data could be refused based on this argument alone. Regardless of the nature of the personal data, it would never be released based on the Transparency Regulation, and only partial access could be granted to documents containing personal data. Second, one of the founding principles of the Transparency Regulation is the non-existence

762 Case T-3/08, *Coedo Suarez v Council*, (OJ C 64, 8.3.2008, p. 54–55); Case C-553/07, *Rijkeboer*, ECLI:EU:C:2009:293.

763 See for example Case T-529/09, *In 't Veld v Council*, ECLI:EU:T:2012:215, para 20; Case T36/04, *API v Commission*, ECLI:EU:T:2007:258, paras 54, 94.

764 See for example document 12973/07, Brussels, 19 October 2007.

of block exemptions. All requests for documents have to be examined individually and based on the content.[765] Hence, accepting this argument would be contrary to one of the founding principles of the Transparency Regulation, which requires that refusal to disclose documents is based on the content of the said documents, not purely on the nature of the documents.[766]

Next, these points are elaborated further. When arguing that disclosing personal data to the public based on the Transparency Regulation would be contrary to the EU Institutions' Data Protection Regulation, the core idea is that public access to personal data would be incompatible with the specified purpose for which the personal data had been initially collected. In line with Article 4 of the Regulation the "*personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes*". In other words, the purpose limitation principle sets limits for the further processing of personal data when the initial processing purposes turn into a new purpose.

Before engaging in a discussion of further processing and purpose limitation, it should be noted that the purpose limitation principle is one of the corner-stones of the European data protection regime. This is well illustrated, for example, in the so-called Schrems case[767] and the very difficult negotiations between the European Union and the United States that followed the Court ruling.[768] One of the core issues in these negotiations was the access by American public authorities to personal data which was transferred initially for commercial purposes from the European Union to the United States. Setting a heavy weight on the data protection principles when significant commercial interests are at stake shows the profound importance of the said principle.[769] Thus, the significance of the purpose limitation principle cannot be overlooked. However, it has to be examined in relation to public access to documents.

It was previously established that one of the most profound principles of the Transparency Regulation would be violated if public access to documents was refused solely based on the purpose limitation principle. When assessing the

765 See for example joined cases C-514/07 P, C-528/07 P and C-532/07 P *Sweden and Others v API and Commission*, ECLI:EU:C:2010:541, para 72; Case T36/04, *API v Commission*, ECLI:EU:T:2007:258, paras 55–56.

766 For similar interpretation, see for example joined cases C-39/05 P and C-52/05 P *Sweden and Turco/ Council*, ECLI:EU:C:2008:374. According the Court of Justice, it did not suffice to ensure that document contained legal advice. It had to be established that the disclosure of legal advice would actually harm the interests protected by the said exception.

767 Case C-362/14, *Schrems,* ECLI:EU:C:2015:650.

768 See for example the Press release (29.2.2016) by the European Commission *Restoring trust in transatlantic data flows through strong safeguards: European Commission presents EU-U.S. Privacy Shield* available <http://europa.eu/rapid/press-release_IP-16-433_en.htm >

769 See for example the Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision by the Article 29 Data Protection Working Party (13.4.2016).

situation simultaneously from the data protection angle, the following two remarks can be made.

First, certain processing purposes where further processing of personal data are deemed not to be incompatible with the original purpose of the data processing are laid down in law. The Data Protection Regulation did allow further processing for historical, statistical or scientific research purposes.[770] The GDPR allows further processing also for archiving purposes, and this the case with the EU Institutions' Data Protection Regulation as well.[771] Hence when these articles are read together with Article 86 of the GDPR, which provides the possibility to reconcile public access legislation with data protection legislation either in Union or national legislation, it must be concluded that the fundamental right to public access to documents represents a similarly significant interest as scientific research or statistical purposes.

Second, the nature and the processing context of the personal data ought to be addressed. When processing of personal data is carried out by public sector controllers, this is often done in the context of decision-making. Naturally, there are also situations where the personal data processed by public sector controllers might be sensitive. An example of this would be health data and processing of such data carried out by the hospitals. Another example can be drawn from social welfare. Nonetheless, these are situations which would mostly occur on the national level, not at Union level. Furthermore, the privacy interests of the data subjects in these type of situations are often protected in the national legislation by secrecy rules.[772] It must be underlined that this data is protected because it is sensitive, not because it is personal data. When assessing this in the Union context, it ought to be noted that the scope of the Transparency Regulation does not typically cover these type of activities carried out by the public sector in the national context. The European Union does not have a similar healthcare or welfare system to national states. Hence, the focus on the actions covered by the Transparency Regulation is rather on the institution in their decision-making capacity. In other words, the personal data processed by the Union institutions is very often related to persons who have either participated in a meeting or who are, for example, the beneficiaries of certain benefits.[773] The information could concern civil servants who have participated in a

770 Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1–22), Article 4(1)(b).

771 Regulation (EU) No 679/2016 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) (OJ L 119, 4.5.2016, p. 1–88); The Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39–98).

772 For example in Finland Laki potilaan asemasta ja oikeuksista 1992/785.

773 See for example Joined cases C-92/09 and C-93/09 *Volker und Markus Schecke GbR and Hartmut Eifert*

meeting, lobbyists who have had meetings with the civil servants or, for example, information on Members of the Parliament who are entitled to some benefits which are financed with taxpayers money. The personal data which is covered by the Transparency Regulation rarely relates data subjects in their private capacity. In such cases where it does, the exceptions laid down in Article 4 of the Transparency Regulation protect the interest of the data subjects, for example, the data subjects' privacy.

Bearing in mind the examined elements which characterize data processing in the Union institutions, it can be concluded that purpose limitation and the further transmission of personal data are at the heart of European data protection legislation. These core principles can, however, be derogated for legitimate reasons. It will be argued later that reconciling public access to documents with data protection represents such a legitimate interest.

2.3 DATA SUBJECT'S RIGHT TO OBJECT

One of the rights endowed to the data subject with the EU Institutions' Data Protection Regulation is the data subject's right to object to the processing of his or her personal data. In Article 23 of the Regulation the data subject has been given the right "*to object, on grounds relating to his or her particular situation, at any time to processing of data concerning him or her, which is based on point (a) of Article 5(1)...*". When the objection is deemed justified, the said personal data may no longer be processed. The same article also contains provisions on the data subject's right to be informed. These provisions reflect the underlying aims of self-determination of the data subject.[774]

There are no explicitly contradictory provisions in the Transparency Regulation, but the underlying interests represented by the right to object and the Transparency Regulation in general aim in different directions. The most profound issue in this respect relates to the data subject's possibility to influence the exercise of another person's fundamental right. To elaborate this little further, access to documents is a fundamental right guaranteed by the Charter of Fundamental Rights. If the data subject wishes to exercise his or her right to object to the transfer of their personal data to a third party who is asking to access to it based on the Transparency Regulation, the data subject would be able to stipulate how the third party can exercise his or her fundamental right of access to documents.

v Land Hessen, ECLI:EU:C:2010:662; C-28/08P*, Bavarian Lager*, Judgment of the Grand Chamber of 29 June 2010 (not yet published).

774 See Chapter IV, section 1.3. The new EU institutions' Data Protection Regulation contains a similar provision.

Next, the scope of this right will be defined in more detail and once the scope has been established, the right will be placed in the context of the democratic decision-making process and the public's right of access to information.[775] First the data subject's objection should be justified. And the objection must relate to the particular situation of the data subject. Hence a mere refusal does not meet the criteria laid down in the EU Institutions' Data Protection Regulation. The GDPR, like the EU Institutions' Data Protection Regulation, also provides the possibility to restrict the right to object in Union or Member State law.[776] Furthermore, the right to object is applicable only when the legal basis for the data processing is the public interest (or the controller's legitimate interest). Thus, there are many limitations to the right to object.

Now that it has been established that the right to object is not absolute, and that its application might require balancing from the controller, different circumstances that might have an influence in the balancing can be recognized.[777] As a first example, the data subject might want to object to the processing of his or her personal data for direct marketing purposes. When such a situation arises, there do not seem to be reasons to allow such processing in spite of the data subject's objection. There does not seem to be such a public interest at stake that the balancing would lead to any other outcome than the termination of the data processing. As a second example, the data subject might have participated in a public decision-making process and does not want his or her personal data to be disclosed. The requester could be, for example, a newspaper or a non-governmental organization. When the criteria set for the right to object are met, i.e. certain legal bases, the controller must balance different interests. In the latter case, the controller has to consider whether the public's right to know outweighs the data subject's right to object. This issue will be elaborated further in the concluding chapter when the underlying principles and aims of access to documents legislation and data protection legislation will be balanced.

2.4 STATING REASONS FOR THE APPLICATION

Chapter III examined the applicant's obligations to state reasons for the application. It was concluded that the Transparency Regulation aims at providing the widest possible access to documents and as such, the applicant is not required to reason his or her application. Therefore, the reasons for the request cannot have any relevance

775 See for instance Case T-412/05, *M v European Ombudsman*, ECLI:EU:T:2008:397; Case T-383/08, *New Europe v Commission*, ECLI:EU:T:2009:114; Case C-553/07, *Rijkeboer*, ECLI:EU:C:2009:293.

776 Articles 21 and 23 of the GDPR.

777 For circumstances of the case, see Chapter I, section 2.

as such.[778] The possibility to request documents anonymously also supports this view. Contrary to this approach, if the request for information is based on the EU Institutions' Data Protection Regulation, the applicant has to provide reasons for the request.[779]

Not only do the requirements for stating reasons for the request vary depending on the applied Regulation, but how the reasoning is taken into account also differs depending on the applied legislation. The Council has also sometimes partly based its refusal to disclose some information by noting that the personal reasons of the applicant cannot have any relevance in the assessment because the Council is releasing the document on an *erga omnes* basis. Thus, the Council gives access to the public in general.[780]

The General Court tried to solve this conflict by deciding that requests for personal data do not need to be reasoned when the access to personal data is sought based on the Transparency Regulation and disclosure of the said information would not undermine the protection of the data subject's privacy. However, the Court of Justice later reversed the General Court's decision.[781] Thus the General Court's approach clarifying that the applicant did not have to provide reasons for the disclosure of personal data was set aside. The personal data in this case related to some interest representatives, i.e. lobbyists, who had attended meetings organized by the Commission.[782] The Court of Justice stated that both Regulations are to be applied in their entirety.[783] This decision leads to a situation where the applicant has to state reasons for the disclosure as far as the document contains personal data.

Hence, there are two clearly colliding rules which should be applied simultaneously.[784] While Article 6 of the Transparency Regulation clearly stipulates that there is no obligation to state reasons for the application, Article 9 of the EU Institutions' Data Protection Regulation states in turn that the recipient should establish that the data is necessary for certain tasks. When examining these colliding rules, the scope of application of the conflicting provisions should be addressed first.

778 See also for example B. Driessen, "The Council of the European Union and access to documents" in *European Law Review* 30 (2005), 690.

779 See for example Case T-164/09 Kitou v European Data Protection Supervisor, pending case.

780 B. Driessen, "The Council of the European Union and access to documents" in *European Law Review* 30 (2005), 690.

781 Case T-194/04, *Bavarian Lager v Commission*, ECLI:EU:T:2007:334; Case C-28/08P, *Bavarian Lager*, ECLI:EU:C:2010:378, para 56.

782 Ibid.

783 Case C-28/08P, *Bavarian Lager*, ECLI:EU:C:2010:378, para 56.

784 See Chapter I, section 1.1.

2.4.1 SCOPE OF ARTICLE 6 OF THE TRANSPARENCY REGULATION

When studying the scope of the said rules, the focus is first on Article 6 of the Transparency Regulation, which stipulates that "*the applicant is not obliged to state reasons for the application*". When this rule is examined together with the underlying principles of the Transparency Regulation, such as the widest possible access to information, a narrow interpretation of exceptions and the non-existence of block exemptions, it does not seem likely that Article 6 intends to hinder the applicant from providing reasons for his or her application. Rather, the aim of Article 6 seems to be to limit unnecessary obstacles to releasing the information. Keeping these bases in mind, it actually seems that Article 6 does indeed allow the applicant to state reasons for the application. Another question is of course, whether the institution is allowed to require the applicant to state reasons. This question will be tackled soon. Before examining this question in more detail, though, another aspect of stating reasons is considered. While it is not clear whether the institution can require reasons when examining the disclosure of personal data based on the Transparency Regulation, there do not seem to be obstacles to the institution taking into consideration reasons provided by an applicant, even if this has not been the practice, for example in the Council.[785] At this stage, reasons given by the applicant are not considered in relation to the overriding public interest test, but rather on more general terms, also taking into account the possibility for more individual reasoning.

Even if there do not seem to be hinderances to taking into account reasons provided by the applicant, the Council has often noted that it is unable to take such reasons into consideration. In these cases, the given reasons have been rather individual in their nature and, as such, not in the scope of the overriding public interest test.[786] Hence, the bottom line in the Council's argumentation is that individual reasons cannot be considered significant when assessing the disclosure, because the document has to be released to the public in its entirety. This follows from the European Union legislative framework, where access to documents legislation is considered public access to documents, not access to public documents.

However, in the aftermath of the Bavarian Lager decision, the institutions seem to be obliged to take the applicant's individual reasons into account. Regardless, the European Commission did argue in the Valero Jordana case that it cannot take into consideration the reasoning provided by the applicant and the applicant should have filed the application under the Data Protection Regulation to a different unit

785 B. Driessen, "The Council of the European Union and access to documents" in *European Law Review* 30 (2005), 690.

786 See for example B. Driessen, "The Council of the European Union and access to documents" in *European Law Review* 30 (2005), 690.

in the Commission.[787] However, the General Court did not adopt the view proposed by the Commission, but rather saw that the Bavarian Lager judgment did oblige the Commission to assess the reasoning provided by the applicant when deciding on the disclosure of the document under the Transparency Regulation.[788]

The General Court did not specify whether the reasons provided by the applicant should be in the public interest or whether they could be individual in their nature.[789] Nevertheless, when applying the EU Institutions' Data Protection Regulation, the reasons provided by the data requester do not necessarily have to serve the public good in general; instead the reasons can be individual in their nature. Another interesting question is whether the necessity to take into consideration the private reasoning of the applicants should be extended to other areas of information as well. Particularly taking into consideration the principle of widest possible access to information, it does not seem far-fetched to suggest that individual reasons could also be of relevance when assessing whether the document could be disclosed.

To conclude the above discussion, the voluntary reasoning for an application does not seem to be excluded from the scope of Article 6 of the Transparency Regulation. If such reasons are provided, the institution should take them into consideration, if for no other reason than in the name of good administration. This could lead to partly individualized disclosure of documents, but one of the aims of the Transparency Regulation is to provide the widest possible access to documents. It does seem to be in the spirit of the Transparency Regulation to allow access to a limited group of people when the alternative is to entirely refuse access.

Furthermore, in moving towards the partly individualized disclosure of documents, EU practice approximates with the ECtHR practice, which has underlined the reasons given by the applicant throughout its case-law.[790] Thus when it comes to personal data, access should be granted to public documents rather than to the public, as such, also in the framework of the European Union.

Hence, it was established that Article 6 does not exclude the possibility to state reasons for an application on a voluntary basis, And also that taking into consideration the widest possible access to documents, the institutions should consider such reasons when they are provided. The question that naturally follows is whether the institution is entitled to require reasoning in order to disclose personal data in light of Article 6 of the Transparency Regulation.

When reading Article 6 of the Transparency Regulation in more detail, it becomes evident that in some cases the institution is entitled to ask for further information from the applicant. According to the second paragraph of Article 6 when "*an*

787 Case T-161/04, *Valero Jordana v Commission*, ECLI:EU:T:2011:337, paras 24, 87–89, 92, 94, 96, 100, 106.

788 Case T-161/04, *Valero Jordana v Commission*, ECLI:EU:T:2011:337, paras 24, 87–89, 92, 94, 100, 106.

789 Case T-161/04, *Valero Jordana v Commission*, ECLI:EU:T:2011:337.

790 See Chapter V, section 2.

application is not sufficiently precise, the institution shall ask the applicant to clarify the application and shall assist the applicant in doing so, for example, by providing information on the use of the public registers of documents". In these cases, the institution needs to have some further information to be able to search for the documents the applicant is requesting. Hence the institution cannot deny access to a document solely because it is unable to identify the document or documents that the applicant has requested, if it has not first carried out consultations with the applicant in order to specify the request.

To examine the rationale behind this provision, the first step is to take a look at the core principles of the Transparency Regulation, starting with the widest possible access to documents. It seems natural that the applicant is not required to give detailed information when filing the first request. If this was the case, the right of access to documents would be narrowed significantly. However, it is essential for the institution to have sufficient information for the identification of the document.

Even if the Transparency Regulation does allow interaction between the institution and the applicant, the examined situation differs from a situation where the institution would directly ask for reasons in order to disclose the document. First, the latter is explicitly closed from the scope of Article 6 of the Regulation. Secondly, engaging in consultation with the applicant would be quite different from simply asking reasons for the disclosure of the information.

Though the institution's entitlement to require the applicant to state reasons for the disclosure seems to fall outside of the scope of Article 6 of the Transparency Regulation, it does not seem to lie in the hard core of the said article. Firstly, the article does recognize the possibility for twofold communication between the institution and the applicant. Secondly, while the article lays down some basic guidelines for the administration of access requests, one of the core aims besides good administration seems to be the widest possible access to documents. Thus, one could say that it would be in the spirit of the said provision to set the obligation for the institution to ask for reasons in cases where this would lead to wider transparency.

2.4.2 SCOPE OF ARTICLE 9 OF THE EU INSTITUTIONS' DATA PROTECTION REGULATION

As was the case under the previous data protection regime, the current EU Institutions' Data Protection Regulation sets the onus on the requester to establish the necessity to have personal data transferred.[791]

The renewed wording of the article on the transmissions of personal data clarifies the relationship between the Transparency Regulation and the data protection provisions, but does not entirely solve it. It still remains open how detailed the reasoning the applicant provides should be in order to meet the requirements set by the case-law. However, the wording of Article 9 together with the related recital introduces four significant elements to unbuckle the tension examined in this thesis. It even solves one issue entirely; namely the controller's responsibility to carry out the balancing test. This is strongly interrelated with the last sentence of Article 9(1)(b), which stipulates that the controller must balance various competing rights. In other words, the new article clarifies that 1) it is the controller who carries out the balancing test, and 2) various competing interests must be balanced when the said test is carried out. This issue will be discussed in the next chapter.

The two other elements relate to the weight given to transparency in this context. First, Article 9(3) clearly stipulates that Union institutions must reconcile the protection of personal data with public access to documents. Furthermore, Recital 28 clarifies that the specific interest for which the data is transferred could relate to the transparency of Union institutions and bodies. These amendments in comparison the previous Data Protection Regulation crystallize that personal data which falls under the Transparency Regulation can be disclosed.

The rules regarding the further processing of personal data are drawn from the purpose limitation principle. Thus, the solution for how to apply this rule together with the public access to documents rules must be sought from the underlying principles of the said rules and an attempt to reconcile these principles will be made in the concluding chapter.[792]

---

791 "*Article 9 – Transmission of personal data to recipients established in the Union other than Union institutions and bodies*

1. Without prejudice to articles 4 to 6 and 10, personal data shall only be transferred to recipients established in the Union other than Union institutions and bodies if:

(a) the recipient established that the data are necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the recipient; or

(b) if the recipient establishes the necessity to have the data transmitted for a specific purpose in the public interest and the controller, where there is any reason to assume that the data subject's legitimate interests might be prejudiced, established that I is proportionate to transmit the personal data for that specific purpose after having demonstrably weighted the various competing interests.

2. […]

3. Union institutions and bodies shall reconcile the right to the protection of personal data with the right of access to documents in accordance with the Union law".

792 For colliding rules and principles, see Chapter I.

2.4.3 INSTITUTION'S OBLIGATION TO EXAMINE THE EXISTENCE OF THE REASONS FOR THE DISCLOSURE OF PERSONAL DATA

Under the previous data protection regime there were no rules nor case-law providing a clear answer as to whether the institution has a duty to examine the specific reasons for the disclosure of personal data provided by an applicant. Guidance could then have been drawn from established case-law, which had set the onus on the institution to examine whether an overriding public interest exists when the applied provision contains the overriding public interest test.[793] The institution was, after all, in the best position to assess whether an overriding public interest exists, as it had the best information about the content of the document. Naturally, it might help the applicant's cause if he or she refers to circumstances that could be considered an overriding public interest.[794]

Before setting the focus on the current data protection regime, it ought to be noted that when the institution examines the existence of the reasons creating the basis for the disclosure of personal data on its own initiative, the different nature of the public interest and personal data must be taken into account. Reasons for the disclosure of personal data are more often related to individual circumstances than to the public interest. Thus, the institution is not necessarily in a position to evaluate such reasons unless the applicant has put forward some justification. It follows that the institution is not in a position to carry out the required assessment as far as it is not provided with the reasons.

The case-law has clarified that that the applicant must provide reasons for the application when the document contains personal data. Therefore, it is taken that this responsibility is on the applicant and this point does not need to be further elaborated.

Further clarification on this topic was provided by the EU Institutions' Data Protection Regulation. It specified that it is the controller's, i.e. the institution's, duty to assess whether the data can be disclosed. Article 9(1)(b) stipulates that the "*controller, where there is any reason to assume that the data subject's legitimate*

793 See for example Case T-529/09, *In 't Veld v Council*, ECLI:EU:T:2012:215, para 20; Case T36/04, *API v Commission*, ECLI:EU:T:2007:258, paras 54, 94.

794 It must be noted that the Court's approach when it comes to the onus on the institution to assess whether an overriding public interest exists has not been solid. In the so-called TGI case the Court laid down other type of general presumption. In this case, the Court first laid down a general presumption of non-disclosure for certain types of documents and thereafter stated that this presumption can be challenged by the applicant. The applicant can either show that a certain document is not covered by the exemption or that a public interest which justifies the disclosure exists. See Case C-139/07 P, *Technische Glaswerke Ilmenau GmbH*, ECLI:EU:C:2010:376, para 62. This approach was criticized. It has been underlined that the applicant is not in place to demonstrate whether the presumption applies or not. When the applicant does not know the content of the document, it is indeed quite challenging to show that the presumption does not apply. Consequently, this right endowed to the applicant by the Court might well remain moot. See for example D. Adamski "Approximating a workable compromise on access to official documents: The 2011 developments in the European courts" in *Common Market Law Review* 49 (2012), 526.

interests might be prejudiced, establishes that it is proportionate to transmit the personal data for that specific purpose after having demonstrably weighted the various competing interest". This is a welcome evolution introduced by the new legislation. While it does not solve the tension examined in this thesis entirely, it will clarify one important element in the complex issue.

2.4.4 CONFLICTING PROVISIONS

Having examined the scope of Article 6 of the Transparency Regulation and Article 9 of the EU Institutions' Data Protection Regulation, it is evident that there are conflicting rules at stake. While Article 6 seems to leave some room for the applicant to state reasons for the request on a voluntary basis, it does not seem to give leeway for the institution to request such reasoning from the applicant. Article 9 of the EU Institutions' Data Protection Regulation in turn sets the duty on the applicant to establish the necessity to have the personal data transferred, and it is not possible to assess if the application meets this requirement unless the applicant provides some reasoning.

Even though the EU Institutions' Data Protection Regulation was adopted very recently, nothing in the wording suggests that the principle set by the Court in Bavarian Lager should be reassessed. Instead, the new Regulation stresses the need to take into account the Union legislation on public access to documents when personal data is transferred. This is a conflict that cannot be solved based on well-settled judicial institutions either, such as *lex superior*. Both the protection of personal data and access to public documents are fundamental rights protected by the Charter of Fundamental Rights. The solution to the colliding rules must therefore be sought from the underlying levels of law and the dimensions of the corresponding principles. Colliding rules do not necessarily signify a collision of the related rights.[795] This will be further elaborated in the next chapter.

795 See Chapter I.

CONCLUSION

CHAPTER VII

FROM SIMPLY SHARING THE CAGE TO LIVING TOGETHER

RECONCILING THE RIGHT OF PUBLIC ACCESS TO DOCUMENTS WITH THE PROTECTION OF PERSONAL DATA

The challenges when public access to documents needs to be reconciled with the protection of personal data have increased over the years. The challenges are taking new forms, and this is heavily influenced by current developments in society. Two elements characterize this development; the shift from information being stored in registers or files to data floods, and the new means of communication which have become part of ordinary life.

Regarding the first element, in early data protection legislation, the weight was often on personal data registers or data files.[796] It follows that data protection was primarily seen to govern rather vast amounts of personal data. Simply mentioning someone's name in a certain context was not necessarily addressed under the data protection legislation. This has changed with new technologies which enable data to be saved in a dispersed format. Even when the data is saved or stored in various different locations, personal data can be easily searched for and fetched. Combining the data with other personal data has also become effortless. It follows that there is a need to protect personal data in such cases where the data does not form part of file or register, as far as the data is being processed by automated means.[797] When a mere name in a document is personal data in the sense of European data protection legislation, the protection of personal data has been brought into a new era.

Regarding the second element, new means of communication have put private persons in a position from which they can reach an unlimited number of people in a very short time period. When personal data was communicated – for example as a part of a document – to a private person 20 years ago, it was most likely to stay in the private sphere of the requester or applicant. The situation is very different today, when all private persons can easily distribute information to an unlimited number of people on the internet and on social media. When it is assessed whether

796 See for example A-R. Wallin & P. Nurmi, *Tietosuojalainsäädäntö,* (Lakimiesliiton kustannus, 1990).

797 Directive 95/46/EC of the European Parliament and 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 (OJ L 281, 23.11.1995, p. 31–50). Directive 95/46, article 3.

the data subject's right to privacy might be breached as a result of the disclosure of the personal data, new means of communicating the information must set the threshold lower than before.

This thesis first set out the theoretical framework for the research, and this was followed by a discussion of European transparency and data protection legislation. These chapters have covered the relevant provisions, rules and underlying principles of both sets of legislation. These rules and principles will play a central role when the balancing of the right of access to documents with the protection of personal data is carried out. This was followed by an elaboration of the actual situations of colliding rules; both the relevant case-law and also more theoretical situations were examined. Next, this concluding chapter will draw together the earlier discussions and seek asolution to the reconciliation of public access to documents with the protection of one's personal data.

First, the legislative setting will be briefly covered. The need to reconcile public access to documents with the protection of personal data does take concrete form when the EU Institutions' Data Protection Regulation and the Transparency Regulation are applied simultaneously. After establishing that situations occur where both Regulations are to be applied simultaneously, an assessment of the underlying objectives and aims of the transparency legislation and data protection legislation will follow. The underlying objectives and aims are an essential part of the balancing, and they will be taken into account when the balancing exercise is carried out. However, the underlying objectives and aims cannot supersede the underlying principles. Before finally engaging in a discussion of the identification of the essence of the said rights, a brief reminder of the earlier discussion on limiting fundamental rights will be given. Lastly, an attempt to maintain the hard core of both rights, while they are simultaneously applied, will be made.

1. SIMULTANEOUS APPLICATION

The collision of principles can materialize only when the respective rules collide on the surface level of law. The collision of rules takes place when there are two contradictory requirements following from legislative acts. Thus, before engaging in a discussion on how to balance different principles, it must be examined when both the data protection legislation and the transparency legislation are applied simultaneously. This discussion will complete the earlier analysis of the overlapping Regulations in Chapter VI. Thereafter will follow some brief remarks of the consequences of the Bavarian Lager judgment.

1.1 MATERIAL SCOPE

Next, two elements which must be taken into account when the material scopes of the data protection legislation and the transparency legislation are examined will be discussed. First, the question of who is in a position to disclose information must be assessed. This question was elaborated in more detail in Chapter VI, and some short remarks on this issue will be given to refresh the memory. Second, the question of how the definition of document relates to the definition of personal data will be elaborated further.

The Transparency Regulation applies to all documents held by an institution in all areas of activity of the European Union.[798] The EU Institutions' Data Protection Regulation in turn applies to the processing of personal data by all Union institutions and bodies.[799] Transmission of personal data, i.e. disclosure of personal data, is processing of personal data. Hence, it is clear that the Union institutions might have to assess disclosure of certain information based on the Transparency Regulation and the EU Institutions' Data Protection Regulation, provided that the definitions of document and personal data overlap.[800]

When assessing the situations in which the definitions of a document and personal data overlap, it must be first noted that both concepts are wide.[801] To start with the least complex situations, the situations where a document contains personal data will be discussed next. This would be the case, for example, when some names are mentioned in a document. Such situations clearly fall within the sphere of public access to documents legislation. The most intriguing question in these cases is the nature of the personal data. The personal data which appears in institution documents could be roughly divided into two categories. The first category would contain the personal data of those who participate in public decision-making. This data could be, for example, signatures on a decision, or names of people participating in meetings etc. The second set of personal data contains more trivial information. It could be, for example, information about a person to whom the decision relates, or the personal data could have ended up in a document for other

798 Regulation (EC) No 1049/2001 of the European Parliament and the Council of 30 May 2001 regarding public access to European Parliament, Council, and Commission documents (OJ L 145, 31.5.2001, p. 43–48), Article 2(3).

799 The Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union in institutions, bodies, offices and agencies and on the free movement of such data, repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39–98), Article 2.

800 According to second paragraph of Article 3, The data protection regulation applies "*to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system*". However, this limitation of the scope is insignificant for the purposes of this thesis.

801 See Chapter III, section 1.1 and Chapter IV, section 2.1.

even quite random reasons. An example of such information would be decisions taken by the human resources department regarding additional compensation for children's schooling. I draw the distinction between the two categories of personal data from the level of participation in public decision-making. The first category of personal data relates to the position of the data subjects, and the second category covers all other situations. For personal data to fall in the first category, it suffices that person is in a position to influence public decision-making. It would not require that the person has actually made a decision.

Proceeding from the easiest to more challenging questions, the cases covered next are the situations where the document contains mainly personal data. A list of names and e-mail addresses would provide an example of such a case. When this type of situation occurs, the applicant might ask for, for example, information about the people who have participated in a certain meeting, as was the case in Bavarian Lager.

All of these situations have taken place on practical level, both at the EU level and also on a national level. Increasing the level of challenge, the next situation would cover cases where the applicant is requesting only one name, for example, or an IP address for that matter. Based on the case-law, one name or number could constitute a document.[802] Thus the applicant could request one piece of information based on the public access to documents legislation, and this information could be personal data.

If the previous examples have seemed challenging combinations of the scopes of the examined Regulations, there is another layer to add to this. As noted, the concept of personal data is wide. Besides the clear cases, i.e. names, telephone numbers etc., the definition of personal data also more widely contains information such as IP addresses, licence plate numbers, etc.[803] For information to be considered personal data, it suffices that the person is indirectly identifiable. The wide definition of personal data is one of the corner-stones of European data protection legislation. It also forms an element which underlines the need to assess the disclosure of personal data based on public access to documents legislation in line with the underlying principles of the data protection legislation. This issue will be further elaborated later in this chapter.

Lastly the question of databanks is briefly tackled. Despite the importance of the question of whether, and to what extent, data banks should be considered documents, profound analysis of this is beyond the scope of this thesis. However, this is a highly relevant issue, and this might well arise in some form in the future. Information is stored increasingly in dispersed form in databanks. This should not create an obstacle to public access to documents. Setting the content of the data

802 Case T-436/09 *Julien Dufour v European Central Bank*, ECLI:EU:T:2011:634.

803 See Chapter III, section 2.1.1.

banks aside, it must be noted that databanks do contain information about the structure and functioning of the databanks.

Thus, there are various different scenarios where the definitions of a document and personal data overlap. The specific features of each situation form the circumstances of the case. Thus, the outcome of an individual balancing case must always be assessed in the said context, taking the circumstances appropriately into account.

1.2 AFTERMATH OF THE CJEU'S BAVARIAN LAGER RULING

The studies in the previous chapters have shown that the provisions of the Transparency Regulation and the EU Institutions' Data Protection Regulation are contradictory to a certain extent.[804] Nevertheless, the Court of Justice stated in the Bavarian Lager judgment that in principle, both Regulations are to be applied in their entirety when access is requested based on the Transparency Regulation and the document contains personal data.[805] The Court of Justice decided this after the General Court had first concluded that, in certain cases, the Data Protection Regulation was not applicable and even personal data could be released solely based on the Transparency Regulation.[806]

The General Court has elaborated CJEU's Bavarian Lager ruling further in its decisions in the Valero Jordana and Dennekamp cases.[807] In the Valero Jordana case the European Commission had suggested that the access to personal data in the requested document should be entirely assessed based on the Data Protection Regulation, and therefore instructed the applicant to file a new request based on the Data Protection Regulation. However, the General Court did not accept this interpretation of the simultaneous application of the said Regulations.[808]

The Kingdom of Sweden noted that the approach suggested by the Commission would have led to situation where the whole framework of the Transparency Regulation would have vanished and as such the core principles of the public access legislation would become inapplicable.[809] This concern is quite justified, in particular because the Court of Justice had not decided the Bavarian Lager case solely in favour of the Data Protection Regulation. The Commission's view as presented in

804 See in particular Chapters V and VI.

805 Case C-28/08P, *Bavarian Lager*, ECLI:EU:C:2010:378, para 56.

806 Case T-194/04, *Bavarian Lager v Commission*, ECLI:EU:T:2007:334, paras 107–109.

807 Case T-161/04, *Valero Jordana v Commission*, ECLI:EU:T:2011:337; Case T-115/13, *Dennekamp v Parliament*, ECLI:EU:T:2015:497.

808 Case T-161/04, *Valero Jordana v Commission*, ECLI:EU:T:2011:337, paras 24, 87–89, 92, 94, 96, 100, 106.

809 Case T-161/04, *Valero Jordana v Commission*, ECLI:EU:T:2011:337, para 67.

the Valero Jordana case does not seem to mirror the Commission's initial approach either. In Bavarian Lager, the Commission had specifically argued that it was unable to assess the disclosure of the document under Article 8(b) of the Data Protection Regulation, because the applicant had not submitted reasons for the request.[810] In other words, if the applicant had reasoned their application, the Commission would have assessed the application based on both the Transparency and Data Protection Regulations.

The General Court seemed to formulate a presumption for a narrow interpretation of Article 8(b) of the former Data Protection Regulation in the Dennekamp case. However, the formulation of the interpretation instruction is cryptic to some extent. But when read together with the last sentence of the said paragraph, which underlines that the "*Transparency Regulation must not be rendered devoid of purpose by an interpretation of the relevant provisions that would mean that legitimate disclosure could never have the aim of full disclosure to the public*", it can be only be read as creating the presumption of a narrow interpretation of Article 8(b) of the Data Protection Regulation, when applied together with the provisions of the Transparency Regulation.[811] The General Court also stated that the reasoning related to disclosure of personal data and provided by an applicant may be general in nature.[812]

In the Valero Jordana case, the applicant had stated reasons for his application and the Commission modified its earlier approach by demanding an entirely new application based on a different Regulation. However, the General Court finally decided that the Commission had erred in law when requiring a new application based on a different Regulation from the applicant.[813]

Thus, the CJEU's statement that in principle both data protection and transparency legislation should be fully applied is still the leading guideline when balancing data protection rules with public access to documents. The CJEU has not itself elaborated this approach. The available specification of the requirement for simultaneous application is drawn from the General Court's case-law. Keeping the CJEU's position and the elements stemming from the General Court's case-law in mind, it needs to be examined whether the balancing could be carried out without interfering with the hard core of the related rights. The CJEU's instruction can only be applied if the simultaneous application can take place without violating the essence of the rights at stake.

---

810 Case C-28/08P, *Bavarian Lager*, ECLI:EU:C:2010:378, para 78.

811 Case T-115/13, *Dennekamp v Parliament*, ECLI:EU:T:2015:497, para 68.

812 Ibid.

813 Case T-161/04, *Valero Jordana v Commission*, ECLI:EU:T:2011:337, paras 24, 87–89, 92, 94, 100, 106.

2. IDENTIFYING AND RECONCILING THE UNDERLYING PRINCIPLES, AIMS AND OBJECTIVES OF DATA PROTECTION AND PUBLIC ACCESS TO DOCUMENTS LEGISLATION

When the balance between the right of public access to documents and the protection of personal data is sought, the underlying aims and objectives of the said rights can and will be taken into consideration. However, the underlying aims and objectives cannot supersede the underlying principles, which form the basis for the concrete rights. In other words, aims and objectives are taken into consideration, but they cannot form an independent counterpart to the principles. This approach reflects the Dworkinian separation between policies and principles.[814]

To elaborate further the distinction between the underlying aims and objectives and the underlying principles of the rights, the following remarks can be made. The underlying aims and objectives will be seen as more general factors than underlying principles. I derive this conclusion from the following premises. Firstly, the underlying objectives and aims are bound with the whole Regulation. The principles instead form a ground for more specific rights. One Regulation might well contain fractions to protect several different rights.[815] This is clearly the case with the Data Protection Regulation for example. As previously discussed, among some other elements, the features of the right to non-discrimination can be distinguished in the data protection legislation.

Furthermore, separating principles from the objectives and aims culminates in the Dworkinian doctrine of institutional support. While the requirements for institutional support have not been clearly defined, institutional support still implies that a principle needs rather strong support to ultimately be considered as a principle. For example, the reference to such a principle in the case-law of the Court of Justice would seem to create a sufficient basis on which to conclude that a certain concept is a principle. Principles are sought from the deep structure of law and therefore the recent changes at the surface level have not yet properly influenced the deep structure of law and established their place there. Thus, when the objectives and aims of the said Regulations are studied, they would partly seem

814 See Chapter I section 2.2 R. Dworkin, *Taking Rights Seriously*, (London, 1977) 90–122

815 See Chapter I section 3.2.2; See in particular T. Ojanen, "Making the essence of fundamental rights real: the Court of Justice of the European Union clarifies the structure of fundamental rights under the Charter" in *European Constitutional Law Review 2* (2016), 321–323; see also for example M. Scheinin, *Ihmisoikeudet Suomen oikeudessa*, (Jyväskylä, 1991) 32.

to exist on the surface level of law and, as such, have not become independent principles just yet. [816]

To take the separation of aims and objectives from principles to a more practical level, it is quite interesting to approach the current debate taking place in Finland. The previous government was under heavy pressure to defend some of its political decisions leading to national legislation. These acts were said to be unconstitutional. One could claim that aims and objectives more easily reflect current political orientations, and this not the case with principles. Principles are more fundamental, they exist in the deep structure of law and no aim or objective can supersede them.

Finally, it should be underlined that the aims and objectives of the rights might in some cases approach the underlying principles. It was earlier established that there is no clear formula for how to recognize principles. It is equally difficult to draw a clear distinction between aims and objectives and principles.

2.1 OBJECTIVES AND AIMS OF THE EUROPEAN TRANSPARENCY AND DATA PROTECTION LEGISLATION

The common presumption is that the Transparency and the Data Protection Regulations have different aims and objectives. While one should provide the widest possible access to government documents, the other draws from the protection of data subject's privacy. This presumption has been strengthened by the CJEU's case-law. The case-law has underlined the contradictory aims of the right of public access to documents and data protection. Just as an example, the General Court reiterated in the Dennekamp case that the said Regulations have different objectives. It underlined that the Court of Justice had stated that "*Regulation No 1049/2001 is designed to ensure the greatest possible transparency of the decision-making process of the public authorities and the information on which they base their decisions. It is thus designed to facilitate as far as possible the exercise of the right of access to documents and to promote good administrative practices. Regulation No 45/2001 is designed to ensure the protection of the freedoms and fundamental rights of individuals, particularly their private life, in the handling of personal data*".[817] This approach has not been contested, and it currently forms a part of settled case-law.

This baseline is not contested in this research either, but it must be examined whether this approach is too simplistic, in particular when the appropriate balance

816 For institutional support, see for example Chapter I, section 1.1 and in particular Dworkin, *Taking Rights Seriously*, (Duckworth 1977) 39–45, 64–68.

817 Case T -82/09, *Dennekamp v Parliament*, ECLI:EU:T:2011:688, para 23; Case C-28/08P, *Bavarian Lager*, ECLI:EU:C:2010:378, para 49.

between transparency and data protection is sought. I will later argue that besides the differing aims and objectives, the said pieces of legislation have also shared objectives. Good governance will be of particular interest in this respect.

Next the aims and objectives of transparency legislation will be assessed, and this is followed by a similar analysis of the data protection legislation. Thereafter the outcome of the analyses will be drawn together.

2.1.1 UNDERLYING OBJECTIVES AND AIMS OF EUROPEAN TRANSPARENCY LEGISLATION

When the underlying aims and objectives of European transparency legislation are studied, democracy is justifiably number one on the list, followed tightly by good governance. If data protection can be seen as a means to protect privacy and some other related fundamental rights, transparency and access to documents could be described as a precondition for a well-functioning democracy, freedom of press and good administration. Good administration and freedom of press are also closely connected, but this aspect is beyond the scope of this thesis.

While the aims and objectives are apparent in the recitals of the Transparency Regulation, democracy together with good governance are also strongly present in the explanatory report of Council of Europe Convention 205.[818] According to the report, "*transparency of public authorities is a key feature of good governance and an indicator of whether or not a society is genuinely democratic and pluralist*". The explanatory report goes further, specifying that access to public documents enables citizens to participate in matters of public interest and opens up the possibility to criticise those who are in power. Similarly with the European Union legal instruments relating to transparency, the explanatory report underlines that transparency makes administration more legitimate and increases confidence towards public authorities. Besides these points, the explanatory report sees that transparency strengthens the self-development of people and promotes human rights.

Reducing corruption is not mentioned in the European Union legislative instruments as an objective. However, the explanatory report of Convention 205 specifically mentions that transparency works in favour of decreasing corruption.[819] Furthermore, different surveys have also shown the connection between transparency and corruption; the more transparent the system, the less likely the

818 Council of Europe Convention 205 on Access to Official Documents 18.VI.2009, Trömsö / Explanatory Report. For the good governance and information governance, see Pöysti, T. "Hallintoeettiset toimintasäännöstöt hyvä hallinnon toteuttamisessa" in I. Koivisto; T.Ojanen; O.Suviranta & M.Sakslin (eds.) *Olli Mäenpää 60 vuotta*, (Edita, 2010), 143–157.

819 Council of Europe Convention 205 on Access to Official Documents 18.VI.2009, Trömsö / Explanatory Report.

occurrence of corruption.[820] In some of the European Union legislative instruments, a corresponding aim has taken the formulation of guaranteeing better control of use of public funds.[821]

Next, the relationship between democracy and transparency will be examined. Transparency is an essential element of democracy. Firstly, it provides a means for participatory democracy or deliberative democracy. Secondly, a transparent system enables public control over public sector functions. Once the different connections between democracy and transparency have been elaborated, the question of good governance vis-à-vis transparency will be tackled. Lastly, the control over public funds together with the relationship between transparency and corruption will be discussed. Other aims, such as promoting fundamental right and self-development of people, will not be discussed in more detail.

2.1.1.1 Transparency as a prerequisite for well-functioning democracy

When addressing the relationship between democracy and transparency, it must acknowledged that there are also several other tools to strengthen democratic society, such as free elections, a multi-party system, freedom of information, separation of powers etc.[822] These tools or requirements will not be examined further; the focus will be on transparency. Also, the aim of democracy can be seen as a hypernym to other aims of transparency legislation, such as participation in the decision-making process and scrutinizing and controlling the decision makers.

The connection between well-functioning democracy and transparency is quite obvious. In most of the European Union Member States this is a baseline, which is explicitly acknowledged.[823] It does not seem too daring to state that democracy – or strengthening democracy – is the core aim of European transparency legislation. As was noted, the idea of democracy, and awareness of the public in general, was the driving force behind the first European transparency legislation more than two hundred years ago, and this same aim was behind the adoption of the first transparency legislation in the EU context.[824] This is strongly supported by the

820 See for instance G. Robertson, "the Media and judicial corruption", in D. Rodriguez and L. Ehrichs (eds.) *Global Corruption Report 2007, Corruption in Judicial Systems – Transparency International* (Cambridge, 2007), 108–115.

821 Commission Regulation (EC) No 259/2008 of 18 March 2008 laying down detailed rules for the application of Council Regulation (EC) No 1290/2005 as regards the publication of information on the beneficiaries of funds deriving from the European Agricultural Guarantee Fund (EAGF) and the European Agricultural Fund for Rural Development (EAFRD) (OJ 19.3.2008 L76, p. 28–30).

822 See Chapter I section 3.

823 H Kranenborg and W. Woermans *Access to Information in the European Union – a Comparative Analysis of EC and Member State Legislation* (Europa Law Publishing, 2005), 10.

824 After the Danish rejection of the Maastricht Treaty in 1992, the discussion regarding public access to information flourished in the European Union. The Danish rejection was seen as a sign of the gap between

current legal instruments regulating transparency in the European Union and the case-law of the Court of Justice of the European Union.

Democracy in general – and also some more detailed elements of democracy – has been very centrally placed in the second recital of the Transparency Regulation. This approach has been treasured, and it is also apparent in the Commission's proposal for the recast version of the Transparency Regulation.[825] Besides the more general statement of openness strengthening the principles of democracy, the possibility to participate in the decision-making process, as well as the legitimacy enjoyed by the administration, are apparent aims mentioned in the second recital.[826]

The impact that transparency has on democratic structures, together with the possibility to participate in the decision-making process, has been elaborated in the Court's case-law. This was also apparent in the so-called Turco case.[827] The Court's Turco decision is of utmost importance, if not the most important in the CJEU's case-law. Turco had argued that "*the principle of democracy and citizen participation in the legislative process constitutes an overriding public interest in […] disclosure.*"[828] While the Court drew some clear guidelines on how to evaluate whether a document containing legal advice should be released, it also made a clear statement on the relationship between access to documents and democracy. The Court noted that the institution should balance the particular interest in question in light of the intention of increased transparency, and reiterated that according to the recitals of the Transparency Regulation "*increased openness […] enables citizens to participate more closely in the decision-making process and guarantees that the administration enjoys greater legitimacy and is more effective to the citizen in a democratic system*". The Court went further by underlining that these considerations being particularly important when an institution is using its legislative powers. The Court stated that "*openness in that contributes to strengthening democracy by allowing citizens to scrutinize all the information which has formed the basis of legislative act. The possibility for citizens to find out the considerations underpinning legislative action is a precondition for the exercise of their democratic rights*". This statement clearly recognizes the influence which transparency has in the democratic structures of society.

European Union and its citizens. And this discussion in turn had a close relationship with the discourse relating to the democratic decision-making processes in the European Union. See for example Ian Harden, "The Revision of Regulation 1049/2001 on Public Access to Documents" 2 (2009) *European Public Law*, s. 239–256 and Commentary of the Charter of Fundamental Rights of the European Union June 2006.

825 Proposal for a Regulation of the European Parliament and the Council regarding public access to European Parliament, Council and Commission documents, COM (2008) 229 final.

826 Regulation (EC) No 1049/2001 of the European Parliament and the Council of 30 May 2001 regarding public access to European Parliament, Council, and Commission documents (OJ L 145, 31.5.2001, p. 43-48).

827 Joined cases C-39/05 P and C-52/05 P *Sweden and Turco/ Council*, ECLI:EU:2008:374.

828 Joined cases C-39/05 P and C-52/05 P *Sweden and Turco/ Council*, ECLI:EU:2008:374, para 12.

The core question in the Turco case was whether documents containing legal advice should have been disclosed. In the three-step process put in place by the Court, the last step is to assess whether there is an overriding public interest justifying the disclosure of the legal advice. When such an interest exists, disclosure can be justified even if it would prejudice the interests protected by the said exception. Here the Court stated that "*such an overriding public interest is constituted by the fact that disclosure of documents containing legal advice of an institution's legal service on legal questions arising when legislative initiatives are being debated increases the transparency and openness of the legislative process and strengthens the democratic right of European citizens to scrutinize the information which has formed the basis of a legislative act*". [829] The significance of this statement cannot be overestimated. Not only did the Court give the very first guidelines for the interpretation of the overriding public interest test. It also set a very strong presumption in favour of the disclosure of the Council legal service's opinions when given in relation to a legislative act. And this principle was based on strengthening the democratic rights of the European citizens. Later, the General Court has extended this approach by stating that scientific opinions delivered in the course of legislative process should also be disclosed as a rule.[830] The General Court also underlined that this is the general principle, "*even if [the opinions] might give rise to controversy or deter those who expressed them from making their contribution to the decision-making process*".[831] These cases illustrate how highly democracy is valued by the Luxembourg courts, and how transparency is clearly seen as a tool to promote this aim; even any nuisance that the disclosure might cause should not be considered a definite obstacle to access to information.

The Turco judgment was not left in a vacuum. It was followed by other cases in which the relationship between democracy and transparency has played an equally important role. Interestingly, even though AG Maduro eminently served the Court with the opportunity to confirm the nature of the right of access as a fundamental right, the Court never took advantage of it.[832] Instead, the Court rather decided the case by emphasizing the vital meaning transparency has for democracy.[833]

At the heart of the Turco ruling, the general principle of disclosure of the information given in the course of the legislative process was formed, and, to be

829 Joined cases C-39/05 P and C-52/05 P *Sweden and Turco/ Council*, ECLI:EU:2008:374, paras 57, 67.

830 Case T-166/05, *Borax Europe Ltd. v Commission*, ECLI:EU:T:2009:65.

831 Ibid., 105.

832 Opinion of AG Maduro in joined cases C-39/05 P and C-52/05 P *Sweden and Turco/ Council*, ECLI:EU:C:2007:721, delivered 29 November 2007, para 32 and Joined cases C-39/05 P and C-52/05 P *Sweden and Turco/ Council*, ECLI:EU:2008:374. Similarly, see also Case C-353/99 P *Council of the European Union v Heidi Hautala*, ECLI:EU:C:2001:661. For an analysis of the said case, see P. Leino, "*Case annotation of Case C-353/99 Council v Heidi Hautala*" in *Common Market Law Review* 39 (2002), 621–632.

833 Joined cases C-39/05 P and C-52/05 P *Sweden and Turco/ Council*, ECLI:EU:2008:374.

more precise, the disclosure of legal advice given in the course of the legislative process.[834] The General Court extended this approach significantly in the Access Info case.[835] The General Court concluded that not only should the information delivered during the process be released, but also information relating to the delegations given their contribution to the process. And this information was to be disclosed while the negotiation process was still ongoing.[836]

This case had its roots in the recast process of the Transparency Regulation and the related negotiations in the Council. A non-governmental organization, Access Info, had asked for access to some of the documents drawn up in the course of these negotiations. While the Council gave quite vast access to these documents, it withheld some parts of the information, namely the identification information relating to the delegations that had given their contributions in the course of the said negotiations.[837] The core argument of the Council was that releasing this information would make it more difficult to find an agreement in the Council. It saw that disclosure of the information would narrow the negotiation space of the Member States.[838] The Council argued that proposals narrowing the wide interpretation of the principle of transparency adopted by the Court would be exceptionally difficult to defend "*in the face of public opinion*". Furthermore, the Council also argued that disclosure of the said documents had led to a "hostile media reception" or "sharp criticism on the part of the public".[839]

While the General Court saw that the Council had not been able to demonstrate that public opinion was hostile, it also held that it is characteristic for democratic debate that both negative and positive comments relating to the ongoing legislative process are made in the media and by the public. Giving some weight to the fact that the process in question leads to binding legislation directly applicable in Member States and having effect on citizens, the General Court stated that "*if citizens are to be able to exercise their democratic rights, they must be in a position to follow*

834 Joined cases C-39/05 P and C-52/05 P *Sweden and Turco/ Council*, ECLI:EU:2008:374, para 68.

835 Case T-233/09, *Access Info Europe / Council of the European Union*, ECLI:EU:T:2011:105.

836 Case T-233/09, *Access Info Europe / Council of the European Union*, ECLI:EU:T:2011:105. The Court of Justice has developed its approach even further. The CJEU set recently a presumption for the disclosure of the four column trilogue documents, see case T-540/15 *De Capitani v Parliament*, ECLI:EU:T:2018:167.

837 For more information see Access Info report *The Secret State of EU Transparency Reforms*, 21 March 2011, available from: http://www.access-info.org/documents/Access_Docs/Advancing/EU/Secret_State_of_EU_Transparency.pdf

838 The exception applied in this case was Article 4(3)(1) of the Regulation 1049/2001, according to it "*access to a document, drawn up by an institution for internal use or received by an institution, which relates to a matter where the decision has not been taken by the institution, shall be refused if disclosure of the document would seriously undermine the institution's decision-making process, unless there is an overriding public interest in disclosure*". While this article relates to the ongoing negotiation process, the question at stake in the Turco case was the protection of legal advice. It ought to be noted however that in line with Council practice, the full versions of the documents including the indications to Member States have often been released following the conclusion of the negotiations.

839 The requested document was available on the Statewatch webpages.

in detail the decision-making process within the institutions taking part in the legislative procedures and to have all the relevant information". Furthermore, the General Court emphasized that in a democratic system, the delegations should be publicly accountable for the proposals they had submitted.[840] While the Turco case circulated very much around the question of how to assess whether there is an overriding public interest and the criteria based on which the existence of an overriding public interest can be assessed, the General Court did not touch upon this question when it decided the Access Info case. The exception which was applied in the Access Info case, namely the exception relating to the ongoing negotiation process, contains an overriding public interest test, but the General Court decided the case in favour of Access Info without examining the case from this angle.[841] As such, the General Court saw that the exception relating to an ongoing decision-making process was not applicable at all in the said case.

In both cases the Court of Justice of the European Union assessed the role that transparency and access to documents play in the democratic decision-making process, or more precisely, in the legislative process. Based on the outcome of these judgments, the role must be considered significant. In the Turco case the focus was on the disclosure of the information building a foundation for a legislative act. In the latter decision, the General Court held that besides the relevant information on the decision-making process, the identification information relating to delegations should also be released.[842] While access to information on the decision-making process enables people to participate in the public debate, the identification information enables people to hold the ones making the actual decisions accountable for their actions and also to address them directly.[843]

2.1.1.2 Transparency's two democracy tools

Looking at the existing European legislation and the recent case-law, it can be stated that transparency – and in this case more particularly the right of access to documents – is essential for a well-functioning democracy. For the purposes of this thesis, two different ways in which transparency serves to strengthen the democracy in a society is identified. Firstly, it provides the opportunity to participate

840 Case T-233/09, *Access Info Europe / Council of the European Union*, ECLI:EU:T:2011:105, paras 69, 70, 78; Case C-280/11 P *Council v Access Info Europe*, ECLI:EU:C:2013:671, para 31.

841 Case T-233/09, *Access Info Europe / Council of the European Union*, ECLI:EU:T:2011:105, para 85.

842 The Council supported by the United Kingdom, Greece, Spain, Czech Republic and France have appealed this judgment to the Court of Justice.

843 The General Court's decision covers the identifying information about the delegations that had expressed their opinions and given proposals in the course of a legislative procedure in the Council. This question will be examined in more detail at later stage in this thesis, together with the disclosure of personal information in the course of the democratic decision-making process.

in the decision-making process. Secondly, it enables citizens to control their representatives. The significance of these tools is not diminished even with the fact that the relationship transparency–corruption–democracy is excluded from the considerations of this thesis.

Regardless of the form of democracy, the core idea is always that of the people as the sovereign.[844] Therefore it seems utterly essential that the sovereign is provided with relevant information; how could the sovereign otherwise form an opinion? The question that follows from that is how the sovereign should be involved in the decision-making process, and should the form of participation reflect how much information the sovereign is entitled to? In the very purest form of democracy, the sovereign is directly involved in the decision-making process. However, even if direct democracy did exist in Ancient Greece and, for example, the Swiss system contains some elements of direct democracy, representative democracy seems to dominate in the Western world. At this stage, the question of whether the sovereign is entitled to detailed information in a representative democracy is left aside. Instead the focus will be on deliberative democracy.

While participatory democracy gets its authorization from free elections and voting, deliberative democracy draws it from citizens' participation in the process of drafting laws through free, public debate.[845] This is exactly the context in which transparency and access to public documents should be placed. It does not seem too courageous to state that transparency enables citizens, for example in the form of non-governmental organizations, to participate in public discussion.

The value of public debate in the democratic decision-making process and its contribution to the outcome of such a decision-making process is not always taken for granted. As previously noted, it has been argued, for example, that that the hostile media reception and sharp criticism on the part of the public forms – among other arguments – a basis for the refusal to disclose information.[846] It has also been noted that the possibility to participate in the public debate does not yet imply that the views expressed would dictate the outcome of the law drafting process.[847] It might well be that in the first case there would be a risk of sharp criticism on the part of

844 G. Smith, *Democratic Innovations*, (Cambridge, 2009) 22; see also for example See E. Maes, Constitutional Democracy, Constitutional Interpretation and Conflicting Rights, in Brems (ed.) *Conflicts between Fundamental Rights*, (Intersentia, 2008), 71–72.

845 A. Ieven, "Privacy Rights in Conflict: In Search of the Theoretical Framework behind the European Court of Human Rights' balancing of private life against other rights", in E. Brems (ed.), *Conflicts between Fundamental Rights* (Intersentia, 2008), 62.

846 Case T-233/09, *Access Info Europe / Council of the European Union*, ECLI:EU:T:2011:105, paras 44, 70, 78.

847 A. Ieven, "Privacy Rights in Conflict: In Search of the Theoretical Framework behind the European Court of Human Rights' balancing of private life against other rights", in E. Brems (ed.), *Conflicts between Fundamental Rights* (Intersentia, 2008), 64.

the public[848], and also the latter observation seems quite correct. This should not, however, be held against of the importance of the public debate. The benefits of public debate are obvious even in light of these comments. The sole fact that the outcome of the proceedings might differ from some of the views expressed during the process, should not lead to the conclusion that public debate was in vain. The dissenting views expressed during the process cannot, or at least should not, be simply disregarded. Unpleasant views ought to be considered as well as – or even in more detail than – the more pleasant ones. To justify the final outcome of the decision-making process, dissenting opinions should be taken into consideration and "reasoned away". Even if it might seem a lot to ask to put forward reasoning that would convince the opposite side, the reasoning should at least convince a "reasonable man". This obviously contributes to the final outcome of law-making processes by guaranteeing better justification for the acts. Thus, public debate should lead to better decisions and better law-making.

Besides offering a tool for the sovereign to participate in the decision-making process, transparency provides the means to scrutinize the information on which the decisions have been based and to hold the ones making the decisions accountable. This serves the people, as it provides the possibility to control the functioning of the public sector.

A significant difference between participation in the decision-making process and scrutinizing the process lays in the timing of the disclosure of the information. The General Court held that the settled Council practice of releasing the identification information of the delegations once the negotiation process was concluded did not suffice.[849] Participation in the negotiation process requires that access to information is provided while the process is still ongoing. The settled Council practice would have enabled controlling and scrutinizing the decision-making process. While this could be sufficient in a representative democracy, deliberative democracy sets the bar higher vis-à-vis the decision makers, and assumes the more active participation of the citizens. Nevertheless, scrutinizing and controlling still remains significant tools in building a democratic society and one of the core aims of the transparency legislation is to provide the means for that.

The Court underlined the importance of the public being able to scrutinize the information forming the basis for legislation in its Turco judgment. But having accurate information about ongoing legislative processes also enables citizens to participate in the public discussion relating to these matters, provided that these documents are released while the legislative process is still ongoing. If the information is disclosed after the legislative process has been concluded, the only purpose the disclosure can serve is the possibility to scrutinize.

848 Proposals for restricting public access to documents could easily lead to that.

849 Case T-233/09, *Access Info Europe / Council of the European Union*, ECLI:EU:T:2011:105.

2.1.1.3 Good governance

Good governance and democracy are partly overlapping concepts. Good governance and the legitimacy of the governance are also particularly mentioned as an aim of European transparency legislation and good governance can be distinguished as an independent aim of the Transparency Regulation.[850] Such characteristics as accountability, effectiveness and transparency are often used to describe good governance.[851]

It was earlier established that transparency can be seen as a tool for accountability. This was earlier examined from the perspective of strengthening democracy, but the same applies vis-à-vis good administration. This can be considered as one of the connecting points between good administration and democracy.

Besides providing tools for overseeing administration and therefore pushing the government to make the best of its administration, transparency should also make administration more effective. Quite interestingly, unbearable administrative burden is often used as reasoning not to examine requested documents individually.[852] On the face of it, it might seem that instead of making the administration more effective, transparency actually causes unpleasant extra work for civil servants. It would be too simplistic to leave it at that. It is an issue which must be elaborated further. First, it must be stressed that the burden these requests might cause cannot be underestimated, in particular if an element of malpractice is mixed with the request. However, the disclosure of documents should on a general level improve the quality of the preparation of different proposals, decisions and documents from the very start. For example, the reasoning behind different proposals or decisions should be drafted from the start in such a convincing way, that different decisions and proposals would also seem accountable in the eyes of the citizens. This, in turn, should make the whole administration more effective.[853]

850 Regulation (EC) No 1049/2001 of the European Parliament and the Council of 30 May 2001 regarding public access to European Parliament, Council, and Commission documents (OJ L 145, 31.5.2001, p. 43–48).

851 See for example United Nations Economic and Social Commission for Asia and the Pacific – What is Good Governance, available on the internet <http://www.unescap.org/sites/default/files/good-governance.pdf > [last visited 21.2.2017].

852 Commission Proposal for a Regulation of the European Parliament and of the Council regarding public access to European Parliament, Council and Commission documents COM(2008) 229 final (30.4.2008), p.5.

853 For the role of transparency in good governance, see also F. Weiss & S. Steiner, "Transparency as an element of Good Governance in the Practice of the EU and the WTO: Overview and Comparison" in *Fordham International Law Journal*. 30(2006), 1545–1586.

2.1.1.4 Reducing Corruption

Besides being linked together, strengthening democracy and good governance form a joint venture with the aim of reducing corruption. Bad governance and corruption are often linked together.[854] For example, the anti-corruption Council of Europe body, GRECO[855], is currently urging its member states to enhance transparency over political funding.[856]

The Council of Europe Convention on Access to Official Documents recognizes reducing corruption as one of its aims.[857] However, this aim is not apparent in the European Union's Transparency Regulation. Despite of the absence of this general aim in the most important legal instrument regulating public access in the European Union, some other instruments have explicitly mentioned the relationship between transparency and the proper use of public funds. This is the case for example in the Council Regulation on Agricultural Funds. According to Recital 6 of Regulation No 259/2008, "*making the information accessible to the public enhances transparency regarding the use of Community funds in the common agricultural policy and improves the sound financial management of these funds, in particular by reinforcing public control of the money used*". The recital goes further, assessing that the measures set up by the Regulation to prevent irregularities are justified and proportional in a democratic society.

The reasons why plain formulation such as "reducing corruption" is missing in the EU context can only be guessed. Maybe this is because the focus has been on strengthening the democratic structures of the Union, or maybe it has seemed politically more correct to dress this aim as prevention of irregularities. Nevertheless, the relationship between transparency and corruption has been established in many international surveys; transparency decreases corruption.[858] The same presumption applies to proper use of public funds and prevention of irregularities; more transparency equals fewer irregularities.

---

854 See for example Transparency International, available on the internet <https://www.transparency.org/what-is-corruption/#what-is-transparency> [last visited 21.2.2017]; see also Oikeuskansleri Tuomas Pöysti, *Korruptiontorjunnan voitettavat vaikeudet Suomessa*, 11.12.2018, Available on the internet < https://www.okv.fi/fi/tiedotteet-ja-puheenvuorot/494/korruptiontorjunnan-voitettavat-vaikeudet-suomessa/ > [last visited 22.2.2019].

855 Group of States against Corruption.

856 Available on the internet < http://www.coe.int/t/dghl/monitoring/greco/default_en.asp > [last visited 21.2.2017].

857 According to 1 preamble of the *Explanatory Report – CETS 205 – Access to Official Documents*, Transparency of public authorities is a key feature of good governance and an indicator of whether or not society is genuinely democratic and pluralist, opposed to all forms of corruption, capable of criticizing those who govern it, and open to enlightened participation of citizens in matters of public interest.

858 See for example G. Robertson, "the Media and judicial corruption", in D. Rodriguez and L. Ehrichs (eds.) *Global Corruption Report 2007, Corruption in Judicial Systems – Transparency International* (Cambridge, 2007), 108–115.

2.1.2 UNDERLYING OBJECTIVES AND AIMS OF THE EUROPEAN DATA PROTECTION LEGISLATION

This section will assess the underlying aims and objectives of the European data protection legislation. The background for the data protection legislation is twofold. While the protection of one's privacy has always been a significant element of data protection, the free flow of personal data and, as such, commercial interests were initially at least of equal importance.[859] For example, the OECD Guidelines on the protection of privacy and transborder data flows were adopted in 1980.[860] The Explanatory Memorandum confirms that the guidelines were drawn with the view to balancing two different objectives, namely the protection of one's privacy and individual liberties and the free flow of personal data.[861] The free flow of personal data was seen as a contributor to economic growth. The different objectives of privacy and free flow of data were seen as somewhat contradictory and it was agreed that a balance between them had to be found.[862] The underlying aim was to create a basic framework for some restrictions to data processing and, as such, unify the situation in different contracting parties. The differences in national legislation were seen as hinderances to free data flows and unifying the situation in different contracting parties would then ease the flow of personal data.[863] Summa summarum, even though the need to protect privacy was recognized in these Guidelines, the actual interest seems to lie in the need to avoid the creation of unnecessary obstacles to the free flow of data.[864]

Quite interestingly, it seems that very similar approach was adopted when the first instrument regulating data protection in the European Union was negotiated. It was quite clearly stated in the Commission's Explanatory Memorandum regarding the Data Protection Directive that the objective of the Data Protection Directive was to allow personal data to flow freely from one Member State to another.[865] To achieve

859 See for example OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Explanatory Memorandum. See also Commission of the European Union, Amended proposal for the Council Directive on the protection of individuals with regard to the processing of personal data and the free movement of such data, COM(92) 422 final – SYN 287, Brussels 15 October 1992. For case law, see joined cases C-465/00, C-138/01 and C-139/01 Österreichischer Rundfunk and Others, ECLI:EU:C:2003:294, paras 39–42; case C-101, *Lindqvist*, ECLI:EU:C:2003:596, paras 79–81; Case C-73/07, *Satakunnan Markkinapörrsi and Satamedia*, ECLI:EU:C:2008:727, paras 51–53.

860 Recommendation of the Council concerning guidelines governing the protection of privacy and transborder flows of personal data (23 September 1980).

861 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Explanatory Memorandum. The OECD Guidelines were revised in 2013. Revised Guidelines are available on the internet < http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm > [last visited 30.8.2019].

862 Ibid.

863 Ibid.

864 Ibid.

865 Commission of the European Union, Amended proposal for the Council Directive on the protection of individuals with regard to the processing of personal data and the free movement of such data, COM(92) 422 final – SYN 287, Brussels 15 October 1992.

this aim, a high level of protection of personal data had to be ensured together with the security of data protection. The protection of one's privacy or personal data did not seem to be the goal itself; while the actual aim was the free flow of personal data, the high level of protection of one's personal data could rather be described as a means to attain this goal. This argument can be reasoned on the basis of the Explanatory Memorandum, but the final formulation adopted in the Directive does not seem to mirror this approach. It clearly defines both the protection of personal data and the free flow of this data as its objectives.[866]

When examining the objectives of the data protection legislation from this angle, it is also of utmost importance to note that the legal base for the Data Protection Directive was Article 95 EC (now 114 TFEU).[867] This article lays down the grounds for measures which have as their object the establishment and functioning of the internal market. Consequently, it can even be questioned whether the said legal base would have provided sufficient grounds for harmonization measures regarding the protection of fundamental rights, such as protection of privacy, at that time. When raising this question, it must be kept in mind though, that based on the settled case-law, when the aims pursued by certain measures are twofold, the act can and must be adopted based on solely one legal base if the other aim can be identified as incidental.[868]

It seems clear that the objectives of the EU's data protection legislation are twofold: the protection of one's privacy and the free flow of personal data. Thus, it is important to keep in mind that while the protection of personal data is a fundamental right, it can also be regarded as a commercial asset with significant economic value. Even if the functioning of the internal market and, as such, commercial interests are clearly one of the main objectives of the European data protection legislation, this aspect was not and will be not examined in this thesis. As the overall theme of this thesis is balancing two fundamental rights, the commercial aspect of personal data is not significant in this respect.

2.1.2.1 Data protection and privacy

The relationship between privacy and data protection was studied in more detail in Chapter IV, and the purpose of this section is to provide a picture of how privacy serves as an aim of the data protection legislation.

866 For case law on the twofold objectives, see joined cases C-465/00, C-138/01 and C-139/01 Österreichischer Rundfunk and Others, ECLI:EU:C:2003:294, paras 39–42; case C-101, *Lindqvist*, ECLI:EU:C:2003:596, paras 79–81; Case C-73/07, *Satakunnan Markkinapörrsi and Satamedia*, ECLI:EU:C:2008:727, paras 51–53.

867 Article 95 falls under Title VI concerning the common rules on competition, taxation and approximation laws.

868 Case C-211/01, *Commission v Council*, ECLI:EU:C:2003:452, paras 38–40.

Convention 108, the very first binding international instrument governing the protection of personal data, names the protection of one's privacy as its main aim.[869] This Convention was concluded in the framework of the European Council and it also paved the way for the EU instruments regulating data protection. The objective of protecting one's privacy was indeed mentioned in the European Union data protection instruments under the previous data protection regime, but they also mention more generally the protection of fundamental rights as their objective.[870]

Moreover, the Commission proposal for the GDPR did not further mention the protection of one's privacy as its objective in Article 1, and this approach was not changed during the four-year-long negotiations in the Council and European Parliament. Instead the GDPR mentions the protection of one's personal data together with a more general reference to protection of fundamental rights as its objective.[871] This might reflect the transition process of the protection of personal data that has culminated in its recognition as fundamental right. While it was previously considered an element of privacy, it has now established its place as an independent right among other fundamental rights.

The other fundamental rights which might become affected through data protection legislation are listed in the Commission's proposal, and are as follows: freedom of expression, freedom to conduct business, the right to property and in particular the protection of intellectual property, the prohibition of any discrimination amongst others on grounds such as race, ethnic origin, genetic features, religion or belief, political opinion or any other opinion, disability or sexual orientation, the rights of the child, the right to high level of human health care, the right of access to documents and the right to an effective remedy and a fair trial.

The Commission's proposal does not suggest that the protection of these rights would be the aim of the Regulation, but merely notes that these fundamental rights might be affected. These rights could be categorized as freedom of expression/information, commercial rights, non-discrimination, right to health care, children's rights and the right to a fair trial.[872]

869 Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg 1981 28.1.2981.

870 Directive 95/46/EC of the European Parliament and 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 (OJ L 281, 23.11.1995, p. 31–50) and Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1–22).

871 Commission Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) COM(2012) 11 final (25.1.2012) and Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1–88).

872 Commission Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) COM(2012) 11 final (25.1.2012).

Interestingly, the right to privacy was not even mentioned on the Commission's list of rights.[873] Arguably, this might have been done to underline the independent status of data protection as a fundamental right. As for the rights listed in the Commission's proposal, commercial rights were excluded from the scope of this thesis and freedom of expression/information relates most likely to the situations where these rights are in conflict with data protection, i.e. the overall theme of this thesis. As for the children's rights, they are seen as a part of the right to privacy in the context of this thesis. Health care and procedural rights related to a fair trial will not be discussed in more detail.

Even if privacy has been excluded from the Commission's list, its significance in relation to data protection cannot be overlooked. It is still an integral part of the data protection regime through its provisions. Furthermore, if the original aim of the data protection legislation is to be dimmed, there is a serious risk of unintended consequences; when interpreting relatively technical legislation in particular in relation to other Regulations, the overall aim of the legislation should be kept clear in mind. If not, the final outcome might not correspond to the original objectives of the legislator.

When returning to the roots of the Data Protection Directive, it is of significant importance to note that besides the original aim of the protection of privacy, the Commission did specifically note that "*it is not so much the content of data which may endanger privacy as the context in which the data is processed*".[874] Thus the protection of personal data must always be seen in the relevant context, i.e. Alexy's circumstances must be taken appropriately into account.

2.1.2.2 Integrity as an element of privacy

Neither the GDPR, the EU Institutions' Data Protection Regulation and its predecessor, the Data Protection Regulation, nor Convention 108 contain any provisions relating to the protection of one's integrity, nor was this mentioned among the objectives of these instruments. Regardless, the protection of one's integrity is an essential element of the European data protection regime. How to justify this assertion?

To begin with, the Transparency Regulation approaches the protection of one's personal data through integrity. The Regulation specifically mentions the protection

873 See also comments on the reluctance of using the term privacy in the data protection legislation, I. Lloyd, "From ugly duckling to Swan. The rise of data protection and its limits", in *Computer Law and Security Review* 34 (2018), p. 780.

874 Commission of the European Union, Amended proposal for the Council Directive on the protection of individuals with regard to the processing of personal data and the free movement of such data, COM(92) 422 final – SYN 287, Brussels 15 October 1992, p. 17.

of integrity in the context of an exception relating to the protection of one's personal data. The protection of the individual's integrity is also specifically mentioned in some of the domestic legislation.[875] Furthermore, integrity is often seen as reflecting the underlying values of self-determination.[876] The protection of integrity might not have been specifically mentioned as an objective in the said instruments, nor mentioned in the recitals or explanatory memorandums. Nevertheless, both the Data Protection Directive and the Data Protection Regulation have several provisions which clearly illustrate the values of self-determination of the data subject, and as such, also integrity. The same applies to the GDPR and the EU Institutions' Data Protection Regulation. An example of articles which reflect self-determination are provisions mentioning the data subject's consent as a prerequisite for processing of personal data.[877] Furthermore, Recital 30 of the Data Protection Directive underlined the importance of the data subject's consent when processing personal data.[878] Other provisions reflecting the idea of self-determination are, for instance, different provisions which regulate access to one's own personal data and provisions which provide the data subject with the possibility to rectify information concerning him or her.[879]

2.1.2.3 Non-discrimination

Non-discrimination was particularly mentioned as one of the aims of data protection legislation in the Commission's new proposal.[880] More correctly, it was mentioned as a human right which might be affected by the data protection legislation. This is not a new aim for the data protection legislation. This aim was also recognized for example in the OECD Guidelines.[881]

The objectives of non-discrimination might not be clearly mentioned in the recitals or articles of the current European data protection legislation. However, this aim is apparent in the legislation itself. For example, some special categories of personal data were defined as sensitive in the Data Protection Directive, as is the

875 For example, according to Swedish Personuppgiftslagen, 1998:204, 29 April 1998, 1§ "*the purpose of this act is to protect individuals against the violation of their personal integrity by processing of personal data*".

876 D.W. Schartum, Norway, in Blume (ed.) *Nordic Data Protection,* (Kauppakaari Oyj, 2001), 86.

877 For example, Articles 7 and 8 of the Data protection Directive.

878 Directive 95/46/EC of the European Parliament and 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 (OJ L 281, 23.11.1995, p. 31–50), Recital 30.

879 See for example Article 10 of the Data Protection Directive.

880 Communication from the Commission to the European Parliament, The Council, the Economic and Social Committee and the Committee of Regions, A comprehensive approach on personal data protection in the European Union, COM 2010 (609) final.

881 OECD WP the Protection of Privacy and Transborder Flows of Personal Data.

case in the GDPR and EU Institutions' Data Protection Regulation. This data can be processed only under strict conditions. Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership as well as data relating to health or sex life are considered sensitive.[882] The Commission's Explanatory Memorandum does not seek the justification for the special treatment of sensitive information through non-discrimination, but solely the risk of endangering the data subject's privacy.[883] Regardless, it is apparent that the type of information which is considered sensitive in the sense of data protection legislation is that which is commonly considered grounds for discrimination.[884] When Article 21 of the European Charter of Fundamental Rights on non-discrimination is placed next to the list of sensitive personal data, the resemblance is clear.[885] Thus it seems safe to conclude that non-discrimination has been one the objectives of European data protection legislation from the very initial phases of the said legislation.

2.1.2.4 Good processing practices – good governance

One of the objectives of the European Union data protection legislation is good processing practices. This is not clearly expressed as an objective in the articles or the preambles of the said legislation, but there are several features in the legislation itself that reflect such aims. Good processing practices are also an element of good governance – or good administration. For example, the following features – which are present in the European Union data protection legislation – are considered components of good processing practices.[886] First, the European data protection legislation contains the principle of purpose limitation. This principle is also closely related to transparent processing of personal data in the sense that data subjects should be informed how, and for what purpose, their data is used. Also, for example, data security can be considered a reflection of good processing practices.[887]

882 Directive 95/46/EC of the European Parliament and 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 (OJ L 281, 23.11.1995, p. 31–50), Article 8. As of 25.5.2018 also biometric data is considered sensitive given that certain qualifications are met. For biometric data, see also joined cases C-446/12 to C-449/12 *Willems and Others*, ECLI:EU:C:2015:238.

883 Commission of the European Union, Amended proposal for the Council Directive on the protection of individuals with regard to the processing of personal data and the free movement of such data, COM(92) 422 final – SYN 287, Brussels 15 October 1992, p. 17.

884 See also Article 22 of the GDPR, which sets restrictions for profiling based on special categorities of personal data (such as race).

885 According to Article 21 of the European Charter of Fundamental Rights "*any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation shall be prohibited*."

886 S. Singleton, *Tolley's Data Protection Handbook*, (LexiNexis, 2004) 22.

887 Ibid.

Besides containing provisions on good processing practices, in some domestic legislation promoting good processing practices is explicitly mentioned as an objective of the law.[888] In some other Member States promoting such good practices might be part of the data protection authorities' duties, even if this is not explicitly mentioned as one of the objectives of the data protection legislation.[889]

The requirements of good processing practices apply both to the private and public sectors. However, the focus of this thesis is on the European Union public sector and when good processing practices are assessed in the context of public sector data processing, they very quickly develop the link with good governance and good administration. Furthermore, the former Data Protection Regulation did set up the independent data protection supervisory authority, the European Data Protection Supervisor (EDPS).[890] The EDPS monitors in particular the EU institutions' and bodies' data processing practices[891] and promoting good processing practices in the institutions is one of the EDPS's main tasks.[892] These factors are all, of course, strong indications that good processing practices do form a part of good governance.

Furthermore, some public sector specific characteristics do also underline the element of good governance when public sector data processing takes place. For example, some authors have expressed concerns in particular over public sector data collection, storage and use.[893] While data processing in private sector would probably often have economic influences, data processing in the public sector could open up possibilities for strict state control over citizens. This is another reason why good processing practices have a particular significance in the public sector and, as such, are an important element of good administration.

Next, I will place good processing practices in the wider context of good administration. To start with, the objective of good governance is not clearly stated as an aim in the European data protection regime. Nor is good governance or one's right to good administration an unambiguous concept in the European legal field.[894] One reason for this might be that EU citizens' right to good governance is a

888 Henkilötietolaki 22.4.1999/523, Article 1.

889 S. Singleton, *Tolley's Data Protection Handbook*, (LexiNexis, 2004) 22. In accordance with the UK's Data Protection Act 1998, section 51, the Commissioner is charged with issuing codes of good practice to be followed by data controllers.

890 Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1–22).

891 Article 2(1) of the Regulation 45/2001.

892 Tasks of the European Data Protection Supervisor, available on the internet < http://www.edps.europa.eu/EDPSWEB/edps/EDPS?more=moins > [last visited 21.2.2012].

893 P. Blume, Denmark, in Blume (ed.) *Nordic Data Protection,* (Kauppakaari Oyj, 2001), 18. See also P. Seipel, Sweden, in Blume (ed.) *Nordic Data Protection,* (Kauppakaari Oyj, 2001), 120.

894 For example, it has been criticized that the Commission did not define the concept of good governance in its White Paper. See for example H. Addink, Principles of Good Governance: Lessons from Administrative Law, in Curtin and Wessel (eds.) *Good Governance and the European Union, Reflections on Concepts, Institutions and Substance*, (Intersentia, 2005), 24.

relatively new concept in the European legal framework. While some authors raised the question of whether good administration should be considered a human right in 2008[895], its status as a fundamental right in the European Union was clarified when the Charter of Fundamental Rights entered into force in December 2009.[896]

Even if there is no clear European definition of good governance, different elements of good governance can be captured. These can be sought from the practice of Member States and EU institutions. For example, the British and Irish Ombudsman Association lists the principles of good governance as follows: independence, openness and transparency, accountability, integrity, clarity of purpose and effectiveness.[897] Some of the elements of the principles of openness and transparency would include that policies and procedures are openly and clearly defined. Another key element of this principle is free access to information. The principle of clarity of purpose aims at three different goals. Firstly, it should be clear why a certain scheme exists. Secondly, it should be clear what this scheme does. Thirdly, it should be clear what can be expected from the scheme.[898]

As for the Union institutions, the European Commission has considered the following principles relevant for good governance: openness, participation, accountability, effectiveness and coherence.[899] The European Ombudsman in turn has defined several different elements of good administrative behaviour. These elements are described in the 27 articles of the European Code of Good Administrative Behaviour.[900] Data Protection is clearly mentioned in Article 21 in the European Code of Good Administration. However, the article does not give further guidance on how data protection should be considered as part of good governance. It simply states the evident, namely the requirements of the civil servants to process personal data in accordance with the former Data Protection Regulation. Furthermore, the Secretary-General of the Council adopted a decision regarding good administrative behaviour. In this decision, the requirements of data protection legislation are specifically noted in Article 11.[901]

---

895 M. Niemivuo "Good Administration and the Council of Europe" in *European Public Law* 4 (2008), 563.

896 Charter of Fundamental Rights of the European Union (OJ C 303, 14.12.2007, p. 1–16).

897 Good Governance Guide, available on the internet < http://www.bioa.org.uk/docs/BIOAGovernance-GuideOct09.pdf > [last visited 21.2.2012].

898 Good Governance Guide, available on the internet <http://www.bioa.org.uk/docs/BIOAGovernance-GuideOct09.pdf> [last visited 21.2.2012].

899 European Transparency Initiative (ETI), Communication from the Commission of 21 March 2007, Follow-up to the Green Paper 'European Transparency Initiative'[COM 2007 (127) final]; Commission's white paper, Code of Good Administrative Behaviour, Relations with the public, adopted on 1 March 2000 (OJ 20.10.2000 L267).

900 Decision of the Secretary-General of the Council/High Representative for Common Foreign and Security Policy of 25 June 2001 on a code of good administrative behaviour for the General Secretariat of the Council of the European Union and its staff in their professional relations with the public (OJ 5.7.2001 C189/1); The European Ombudsman, The European Code of Good Administrative Behaviour, 2005.

901 Decision of the Secretary-General of the Council/High Representative for Common Foreign and Security Policy of 25 June 2001 on a code of good administrative behaviour for the General Secretariat of the Council of the European Union and its staff in their professional relations with the public (OJ 5.7.2001 C189/1).

As said previously, good governance is is an ambiguous concept and as such, it leaves a wide margin for elaboration when what forms the content of good administration is assessed. However, it seems quite safe to suggest that good processing practices are part of good administration in the European legal framework. Specifying the exact elements of good processing practices is much more difficult. While data protection is clearly mentioned in the European Code of Good Administrative Behaviour, there are no clear indications of how to define different components of data protection as a part of good administration, apart from one's right to access his or her own file.

Further, the European Code of Good Administration refers to data protection legislation as a whole, but some elements which are more important in relation to good administration can be distinguished. Based on the principles defined in some domestic practice, the common principles for good administration and data protection legislation could be found in certain provisions. This is particularly the case with the principles of openness and transparency, and also clarity of the processing purpose. As mentioned earlier openness and transparency have a different meaning in the internal dynamics of data protection legislation vis-à-vis access to document legislation.

Some of the articles giving more precise frames for good processing practices are laid down in the European data protection legislation. An example of this is the requirement for purpose limitation in the processing of personal data. As noted by some authors, this requirement promotes the transparent processing of personal data.[902] As such, it also works in favour of good governance.

Thus, even if good processing practices or good governance are not explicitly mentioned as the aims of the data protection legislation, I argue that they do form an integral part of the aims and objectives of the European data protection legislation.

2.1.2.5 Democracy

Having discussed the different objectives of the data protection legislation, it is also essential to look at privacy's relationship with democracy. The relationship between transparency and democracy was examined earlier[903] and it was concluded that transparency can be considered a prerequisite for well-functioning democracy. However, according to some[904] privacy can also be considered a prerequisite, or at least an element of, democratic society and for the freedom of speech.

902 Ibid.

903 See Chapter III, section 1.2.

904 See for instance A. Rouvroy & Y. Poullet, "The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the importance of Privacy for Democracy", in S. Gutwith; Y. Poullet; P. De Hert; C. de Terwangne & S. Nouwt, *Reinventing Data Protection* (Springen, 2009), 45–76.

The relation between privacy and democracy might not at first sight seem as clear as the relationship between transparency and democracy. The connection between privacy and democracy is based on the assumption that in order to be able to form and freely express personal opinions, one should have privacy to develop and elaborate these thoughts.[905] In this context it is of interest to note that the driving force behind the development of the data protection regime was the fear of the potential effects of uncontrolled use of new information technologies. On the one hand the new technologies were seen as a threat to privacy, and on the other hand the new possibilities they offered for controlling and supervising people were considered dubious[906] That is to say that the control of the state over its citizens was considered worrying.

Nonetheless, when access to documents is inserted into the equation with democracy and privacy, we immediately notice that without first having the relevant information, the meaning of the privacy becomes void via-á-vis democracy. Thus, the opportunity to elaborate one's thoughts without interference is rendered fruitless quite quickly if one is not first provided with sufficient information. To conclude, even if there might be some grounds to regard privacy as a prerequisite or an element of democracy, it still seems quite a far-fetched construction. Other fundamental rights could also be linked with democracy with similar constructions.

2.1.3 SOME REMARKS ON THE UNDERLYING AIMS AND OBJECTIVES OF TRANSPARENCY AND DATA PROTECTION LEGISLATION

It was earlier established that the contrast between the different objectives of transparency and data protection legislation have dominated the discussion on the balancing of the said rights. This is too simplistic an approach. Both similarities and differences exist between the underlying objectives and aims of transparency and data protection legislation. This section will first draw together the discussions from the previous chapters and sections, noting the differences between the aims and objectives of the said rights. Thereafter the shared objectives and aims of the transparency and data protection regime will be discussed.

There are differences between the underlying objectives and aims, but I would lay even more weight on the differences which exist in the structures of the said concepts. The protection of personal data is a more complex and multilateral concept than the right of access to documents. Different sub-elements of data protection

905 A. Rouvroy & Y. Poullet, "The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the importance of Privacy for Democracy", in S. Gutwith; Y. Poullet; P. De Hert; C. de Terwangne & S. Nouwt, *Reinventing Data Protection* (Springen, 2009), 45–76.

906 Wallin & Nurmi, *Tietosuojalainsäädäntö*, (Helsinki, 1990) 1–7.

reflect different underlying objectives and aims of the data protection legislation. For example, when particular provisions relating to the processing of sensitive data reflect the aims of non-discrimination, certain provisions reflect the objectives of good governance instead. An example of such provisions are the rules governing diligent planning of the processing operations. The dispersed structure of data protection could be elaborated further, but it suffices to note that while different objectives are not apparent in all aspects of data protection legislation, they are clearly visible in some areas and in some legislative provisions. This underlines the significance of the contextual interpretation. It is therefore of utmost importance to establish Alexy's circumstances for the balancing. These circumstances will be drawn from the objectives and aims of the said rights. Seeking the proportional balance in Hesse's terms must be based on contextual interpretation.[907]

Setting the structural differences aside and focusing on the aims and objectives themselves, an interesting difference between the underlying objectives of the examined rights is how they have been developed over the years. While the core objectives and aims of the transparency and public access to documents legislation have remained the same for centuries, the original aim and objective of the protection of personal data has faded and turned into a more pluralistic set of objectives. While transparency legislation has realised the values of democracy from the very beginning, the original objective of protecting one's privacy has not even been mentioned in the GDPR.[908] One reason for this might be the changing nature of the right to protection of personal data. When the first data protection laws were adopted in Europe, data protection was seen as an element of privacy. Only after the Charter of Fundamental Rights entered into force has the protection of personal data been unanimously recognized as an independent fundamental right. Maybe the Commission dimmed the reference to privacy to underline this development, rather than to blur the original objectives and aims of the data protection legislation.

Now, it was established that the objectives of transparency regulation have remained the same throughout hundreds of years. It was argued earlier in this chapter that principles exist in the deep level of law while objectives and aims are often found on the surface level of law. When the underlying aim to increase democracy has existed over decades, it can hardly be argued that democracy cannot be considered a principle because it cannot be draw from the deep level of law. Going back all the way to the first transparency legislation and Chydenius' explanatory

907 See Chapter I, section 2.2.1.

908 Commission Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) COM(2012) 11 final (25.1.2012) and Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1–88).

texts, and then putting them together with the introductory part of the current legislation, it must be concluded that the connection between transparency and democracy is solid. Thus, the reasoning must be sought from elsewhere. Principles can be seen as propositions which describe rights; "*arguments of principle are arguments intended to establish an individual right*".[909] The discussion on whether the right to democracy exists will not be touched upon. For the purposes of this thesis, the collective nature of democracy is underlined. Consequently, it is not seen to establish an individual right and therefore cannot be considered a principle.[910]

Once it has been established that democracy is rather an objective or aim of the transparency legislation than an underlying principle, the question that follows is whether this would lead to a situation where arguments of democracy could not supersede arguments of principle. In a Dworkinian world, policies can never trump principles.[911] Hesse's practical concordance in turn takes policies into account as a part of a proportionality test and the European Court of Human Rights sees limitations to certain rights justified when they are necessary in democratic society.[912] Drawing on what was said, it appears clear that democracy can and even must be taken into account as an underlying objective when transparency is balanced with other rights. But could it trump arguments of principle, which are intended to establish individual rights? For the purposes of this thesis this question does not need to be answered. Thus, it remains unanswered. Instead, the focus will be on two other related issues. First, the hard core, the essence of public access to documents, will be derived from the grounds of democratic decision-making. This will be based on the right to receive information about the decision-making processes that take place in the democratic structures of society. Second, democracy will be an essential element when Hesse's and Alexy's optimization is practiced while looking for the balance between data protection and transparency.

Now some differences between the underlying objectives have been assessed. The most obvious difference between the protection of privacy and access to data is not addressed at this stage. This issue will be focused on when the solution for reconciling the different principles is carried out.

Next, the most significant similarity between the said objectives and aims will be briefly discussed. This is the objective to promote good governance. The objective of good governance has long been considered as one of the core aims of transparency regulation. This aim can be sought all the way from the Chydenius' explanatory

909 R. Dworkin, *Taking Rights Seriously,* (Duckworth 1977) 90–91.

910 See Chapter I, section 1.1 and section 1.2.

911 R. Dworkin, *Taking Rights Seriously,* (London, 1977) 90–122.

912 See Chapter I section 2.4, in particular K. Hesse, *Grundzüge des Verfaussungsrechts der Bundesrepublik Deutschland*, (Heidelberg, 1990) 142; T. Marauhn and N. Puppel, Balancing Conflicting Human Rights: Konrad Hesse's notion of "*Praktische Kokordanz*" and the German Federal Constitutional Court, in Brems (ed.) *Conflicts between Fundamental Rights*, (Intersentia, 2008), 279–281.

memorandum. It is more rare to see the connection made between the protection of personal data and good governance. Regardless, it was shown earlier in this chapter that there is a connection between data protection rules and good governance. This objective might not be apparent in all provisions of the data protection legislation, but it clearly exists. When good governance forms part of the circumstances where rights are balanced, this similarity is of particular interest. Furthermore, the shared objectives and aims of the Transparency and Data Protection legislation will be of particular interest in such cases where the application of the rules of the said Regulations would lead to different outcomes.

3. FROM SIMPLY SHARING THE CAGE TO LIVING TOGETHER; RECONCILING PUBLIC ACCESS TO DOCUMENTS WITH THE PROTECTION OF PERSONAL DATA

This section will focus on the colliding rules on the surface level of law and seek the balance by weighing the underlying principles of data protection and public access to documents. When the dimensions of the principles are sought, the limits of the respective rights will be heavily tested. The question of whether the underlying principles can be reconciled or whether the simultaneous application of the examined Regulations actually leads to a violation of the hard core of one the rights will be addressed in the second part of this section. The second part of this section will first examine the essence of the said rights and thereafter assess whether the hard core of both rights can remain untouched when the underlying principles of the rights are reconciled. Or will it be inevitable that one of the rights will supersede other? Finally, a suggestion for a procedural provision will be made.

Before engaging in the discussion of balancing the said rights, a short reminder of some basic elements when fundamental rights are limited will be provided. It was established earlier that limiting one fundamental right in order to realize another fundamental right does not necessarily lead to violation of the said right and, as such, to a genuine collision of rights.[913] Thus fundamental rights can be limited without violating the said rights. However, the restrictions cannot be arbitrary or disproportionate.

913 Se Chapter I, section 2.

3.1. RIGHTFUL INTERFERENCE OF PROTECTION OF PERSONAL DATA

It was earlier established that neither of the examined rights is absolute.[914] It follows that these rights can be restricted without violating the said rights.[915]Both examined rights are recognized as fundamental rights in the legal framework of the European Union. Therefore the potential limitations to these rights must meet the criteria laid down in Article 52(1) of the Charter of Fundamental Rights.[916]As was established earlier, the said article sets some basic requirements for the limitations, i.e. that they must be provided for by law, respect the essence of the right and be proportional. For the proportionality test, the Charter provides some further guidance. To be proportionate, the limitation must be necessary, i.e. the aim pursued cannot be achieved without the said limitation. If same result can be achieved by measures which interfere less with the said fundamental right, those measures must be selected.[917] Second, the limitations must pursue general interests recognized by the Union.

3.1.1 PROVIDED FOR BY LAW AND RESPECT THE ESSENCE

Thus, the limitations must be 1) provided for by law and 2) respect the essence of the said rights. When limitations are set by the legislator in the course of legislative procedure, it does not take much of an effort to establish whether the first requirement is met. The limitation could for example take form as an exemption to the other right.

The question of whether the first requirement is met does not need to be further elaborated. Both rights are regulated by law and this thesis will provide a suggestion on how to reconcile the tension between the two principles by reading

914 For the protection of personal data not being an absolute right, see also Opinion of the Court (Grand Chamber) of 26 July 2017 pursuant to article 218(11) TFEU, ECLI:EU:C:2016:656, para 181.

915 For rightful interference with the right to protection of personal data, see also Opinion of the Court (Grand Chamber) of 26 July 2017 pursuant to article 218(11) TFEU, ECLI:EU:C:2016:656, paras 181–210.

Very detailed and rather technical methods for assessing the privacy and data protection risks have been developed. See for example EUI working paper, *Report on system effectiveness, efficiency and satisfaction assessment; Data Protection* by Erik Krempel, Fraunhofer IOSB and Dr. Coen van Guljik, TU Delft, available on the internet < https://surveille.eui.eu/wp-content/uploads/sites/19/2015/04/D3.3bSystem-Effectiveness-and-Efficiency-Data-Protection.pdf > [last visited 15.5.2017].

916 Charter of Fundamental Rights of the European Union (OJ C 303, 14.12.2007, p. 1–16). For restricting the principle in the Finnish context, see O. Mäenpää, *Julkisuusperiaate* (Helsinki, 1999), 15–19.

917 See for example joined cases C-293/12 and C-594/12 *Digital Rights Ireland and Kärtner Landesregierung*, ECLI:EU:C:2014:238 and joined cases C-92/09 and C-93/09 *Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen*, ECLI:EU:C:2010:662.

the Transparency Regulation and the EU Institutions' Data Protection Regulation together without violating the essence of either of the examined rights. Before offering the suggestion for the interpretation, the essences of the rights need to be studied in more detail. Only after this analysis has taken place, it can be assessed whether reconciliation is possible while the cores of the said rights remain untouched. Before studying this issue in more detail, the circumstances of the case will be studied.

3.1.2 PROPORTIONALITY

To assess whether a certain measure limiting the protection of personal data or public access to documents is to be considered proportional, it is necessary to identify the essence of the said rights. When reconciling two fundamental rights, the hard core of both rights should remain untouched. Measures invading the hard core of the right can hardly be considered proportional. Therefore, the proportionality test will be carried out simultaneously with the identification of the hard core of the rights. At this stage, the proportionality test is studied on a more general level and some general remarks about the relevant circumstances will be given in the next section.

The core idea of the proportionality principle is that the measures taken are suitable for the objectives they are aiming at.[918] Drawing from the CJEU's case-law, the requirements to be met in the proportionality test have been elaborated in more detail. Self-evidently, these requirements reflect also the wording of the Charter of Fundamental Rights. The proportionality test could be formulated as follows: "*The measure must (1) pursue objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others; (2) be suitable to meet these objectives; (3) be "necessary" in the sense that it is the least invasive suitable measure; and (4) is proportionate in the strict sense*".[919]

The first element of the proportionality test can be examined already at this stage, even if the essence of the rights has not yet been identified. The first element is to assess whether the intended measures will meet the objectives of general interest recognized by the Union. The rights balanced in this research are recognized by the Charter of Fundamental Rights. Both rights have also clearly established their place in the Union's primary law. Thus, this is an issue that does not need to be further elaborated. The objectives are of general interest in Union law. And also, the intended measures pursue rights of other.

The other elements of the proportionality test will be carried out while identifying the essence of the examined rights. What is to be considered proportional might vary

918 T. Tridimas, *General Principles of EU Law*, (Oxford, 2005) 136–142.

919 L. Feiler, "The Legality of the Data Retention Directive in Light of the fundamental Rights to Privacy and Data Protection" in *European Journal of Law and Technology* 3 (2010).

based on the aims pursued. The limitations of one right must be strictly necessary in order to realize the other right. It follows that what is to be considered proportional depends of the circumstances of the case. The circumstances of the case may vary, and the legislator cannot predict all possible scenarios that might occur in the future. An attempt to capture the circumstances can be given by elaborating the conditions under which one principle takes over another.

3.2 THE CIRCUMSTANCES OF THE CASE – CONDITIONS

When two multidimensional principles are reconciled, contextual-based balancing is unavoidable.[920] It was earlier established that contextual-based evaluation is not arbitrary. One could tentatively name such factors as legal certainty, predictability, rule of law, constitutional state, significance in democratic society etc. as elements which should be met in contextual-based analysis.

Drawing from the circumstances of the case, the conditions providing the tools for a case-by-case analysis can be identified. When it is examined how to balance two competing principles, "*the judicial function is to establish the conditions under which one principle takes over another*".[921] This section will elaborate the circumstances which will have relevance when an assessment of whether personal data should be disclosed takes place. In other words, elements which create the conditions for contextual-based analysis will be provided in this section.[922]

I divide the circumstances of the case into two categories: the data processing environment and the nature of personal data. Both the processing environment and the nature of personal data can be further developed and structured in more detail. First the environment where the data is being processed will be elaborated, and this will be followed by an analysis of the nature of the personal data.

3.2.1 PROCESSING ENVIRONMENT

The risk elements involved in data processing vary in different processing environments. It is clear that the risk involved in data processing differs significantly in offline and online worlds. First, I will elaborate how information in the public sphere relates to the online world. This will be followed by a more general analysis

920 For case-by-case balancing in the CJEU's case-law, see also Brkan, M. The Court of Justice of the EU, privacy and data protection: Judge-made law as a leitmotif in fundamental rights protection, in Brkan, M. & E. Psychogiopoulou (eds.) *Courts, Privacy and Data Protection in the Digital Environment*, (Edward Elgar, 2017), 19–22.

921 R. Alexy, *A Theory of Constitutional Rights*, (Oxford, 2010) xxviii.

922 See Chapter I, section 2.2.1.

of situations where processed data is publicly available. It must be underlined that this assessment will not touch upon the question of making this information publicly available in the first place.

3.2.1.1 Publicly available information and online information

One of the core issues which needs to be tackled when seeking the balance between the two rights, is whether the information should be available to all, or whether there may be limitations to this. This is also a question which has great significance when placing this scenario in an online world. I see that at least two elements make the online world very different from the offline world. First, the most obvious difference is that online information is available to everybody. Second, combining information from different sources by using – for example – search engines, makes reuse of this information effortless. Furthermore, it could even be argued that this type of search based on personal data creates profiles, and could therefore be subject to particular data protection rules concerning profiling.

Once this is said, it should be kept in mind that one of the core ideas of the transparency legislation is that requests for the information can be made anonymously. In other words, the identity of the applicant requesting the information should not be relevant when assessing whether the document can be disclosed. When assessing the disclosure of personal data against that background, the question of the online / offline environment seems irrelevant.[923] However, I see that this approach must be elaborated further in particular in light of the Bavarian Lager judgment.[924] And not only Bavarian Lager, but also other judgments, such as Schecke and Hartmut Eifert and so-called Data Retention I play a role in this assessment.[925] These judgments have stressed that the protection of personal data is a fundamental right. Besides this element, these judgments have underlined the importance of the proportionality requirement in relation to the data protection provisions. In other words, interference with one's right to the protection of personal data must be limited to what is *strictly necessarily*. The Court's approach follows very much Hesse's doctrine, which underlines the necessity element when restricting fundamental rights.[926] I argue that such factors as general availability and the possibility to

923 See also H. Nissenbaum, *Privacy in context – Technology, Policy, and Integrity of Social Life*, (Stanford University Press, 2010) 53–58. Nissenbaum notes that it has hardly caused any heated debated when public records are made accessible through the internet.

924 Case C-28/08P, *Bavarian Lager*, ECLI:EU:C:2010:378.

925 Joined cases C-92/09 and C-93/09 *Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen*, ECLI:EU:C:2010:662 and joined cases C-293/12 and C-594/12 *Digital Rights Ireland and Kärtner Landesregierung*, ECLI:EU:C:2014:238.

926 See Chapter I, section 2.4.

combine personal data with the information from various other sources, have a great significance when assessing whether such processing of personal data is to be considered proportional with the aims pursued. The circumstances for balancing can be drawn from these elements.

To take these propositions to a more practical level, the following example can be given. Minutes from city council meetings are publicly available information in some Member States.[927] These minutes might contain at least two types of personal data. First, the minutes would most likely have information about the municipal decision makers. Besides this information, there could also be occasional information about municipal citizens, for example in the context of their construction permits. When the city council's minutes are publicly available, this information –including the personal data – would be accessible for the public from the outset. When this situation is considered in the offline world, it seems to meet the requirements of proportionality. First, the information about political decision makers should be publicly available, including at the municipal level. Second, the information about the construction permits might be relevant to some municipal citizens, and there does not seem to be any reason to assess the situation differently. In other words, there is no need for secrecy in such cases. However, when this situation is transferred into a different environment, in an online world, the setting looks very different. When the information about someone's construction permit is available to the whole world for an unlimited time period, the proportionality requirement kicks in, and the necessity of such a measure can be questioned when taking into account the aims of the said measure. Even if in principle the situation does not change – the said information is available to everyone – the limitations of one's privacy rights and the level of interference with privacy is on a very different level in these two situations. In an online environment, the existence of search engines and the possibility to google someone allows the searcher to combine vast amounts of information from different sources. Thus, the information about someone's construction permit combined with other information available on the internet, could reveal more private information about the said data subject. Furthermore, this information could be entirely irrelevant to the person searching for the information.

To draw together the previous discussion, the general availability of the information is relevant when assessing whether the measures taken to safeguard the right of access are proportional in relation to the limitation of one's privacy. The difference between self-determination and privacy will be further developed soon, but I underline that the focus in this question is on privacy. Due to modern technology, availability cannot be considered solely based on public availability of the information. Because of the different nature of the online world and the offline

927 This is the case for example in Finland.

world, I suggest that publicly available information should be distinguished from online availability. While I see that this can offer part of the overall solution, it must be acknowledged that this distinction has its own difficulties, for example, how to place freedom of speech in this construction or how to assess situations where information is gained in the offline world and then transferred into the online world.[928]

3.2.1.2 Processing publicly available personal data

In this section I will elaborate further the question touched upon in the previous section and set it in the current context. The red line is to separate online information from publicly available information. This is an essential element when seeking the solution to the research question. The distinction cannot be derived from the applicant who requests the information, i.e. the person who has the right of access. The right would still belong to all. Instead, this distinction is based on how the publicly available personal data can be processed in the online environment and in other environments. When personal data is available in the online environment, personal data can be processed further without any restraints. In other words, the distinction of the processing environment should not imply that fewer persons would be entitled to have access to the documents. The right of access would still belong to all, but the restrictions regarding the processing environment would set natural boundaries for the processing of personal data.

It is clear in light of the Court's case-law that even when personal data is publicly available, data protection rules and principles apply to the processing of such personal data. It was clarified in the Spain v Google case that when personal data is legally available from one source, it does not necessarily signify that this information could be made available for unlimited number of people.[929] The Court's decision echoes its earlier Satamedia judgment, where the Court concluded that excluding personal data which has been published from the scope of the Data Protection Directive infringes EU law.[930] Thus, it clearly follows from the CJEU's case-law that even when personal data is in public sphere or publicly available, it must be processed in accordance with the data protection legislation.

It follows that when publicly available personal data is processed, it must take place in accordance with the data protection legislation. For the processing to meet

928 An answer to the latter question can be sought from the Spain v Google case (Case C-131/12, *Google Spain and Google Inc*, ECLI:EU:C:2014:317). The environment was different, but same principles could apply to situations where access to information is gained in the offline world.

929 Case C-131/12, *Google Spain and Google Inc*, ECLI:EU:C:2014:317.

930 Case C-73/07, *Satakunnan Markkinapörrsi and Satamedia*, ECLI:EU:C:2008:727.

the requirements of the data protection legislation, first the data processing must have a legal basis set out in the data protection legislation or alternatively fall outside the scope of the data protection legislation. This would be the case, for example, if personal data was processed solely for household purposes.[931] An example of the legal basis for the data processing could be controller's legitimate interest.[932]

When personal data is publicly available, there are not any natural limitations to, for example, collecting the personal data. However, this does not imply that the data protection rules do not apply to publicly available personal data. The question that follows is who should then ensure that personal data is being processed appropriately. This task falls naturally on the national data protection authorities or, in the case of the Union institutions, the EDPS.[933]

Besides ensuring that personal data is processed based on an appropriate legal basis, the supervisory authorities must ensure that other requirements of the data protection legislation are also met. While certain requirements – such as an appropriate legal basis[934] – must always be met, many of the other requirements which need to be fulfilled depend on the type and nature of the processing situation. The greater the risk involved in the processing, the stricter the requirements for the controller.[935]

3.2.2 THE NATURE OF THE PERSONAL DATA

As I suggested earlier, the type or nature of personal data forms the other category of circumstances. The definition of personal data is wide.[936] When the definition covers information from IP addresses and licence plate numbers to genetic information, it seems clear from the outset that the nature of the data must be taken into account when the circumstances of the case are assessed.

---

931 For the household exemption, see also European Law Blog, News and comments on EU law, *European Data Protection and Freedom of Expression After Buivids: An Increasingly Significant Tension*, February 21 2019, available on the internet < https://europeanlawblog.eu/2019/02/21/european-data-protection-and-freedom-of-expression-after-buivids-an-increasingly-significant-tension/ > [last visited 23.2.2019]. See also case T-345/17 *Buivids,* ECLI:EU:C:2019:122.

932 For more on legitimate interest, see for example the Article 29 Data Protection working party, "Opinion 6/2014 on the notion of legitimate interests of the data controller under article 7 of Directive 95/46/EC", 844/14/EN WP 217.

933 For the competent national data protection authority, see case C-230/14, *Weltimmo*, ECLI:EU:C:2015:639 and case 191/15, *Verein fur Konsumentioninformation v Amazon*, EU:ECLI:C:2016:612.

934 See also case C-127/13 P, *Strack v Commission*, ECLI:EU:C:2014:2250, para 108.

935 See for example Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1–88).

936 See Chapter IV, section 2.1.

3.2.2.1 The status of the person – public persons, public decision -making

I argued earlier that there should be a strong presumption of disclosure of personal data which relates to those who are in a position to influence public decision-making. If the right to protection of personal data was to be restricted in order to realize public access to documents, the restriction should be limited to what is strictly necessary in order to realize public access to documents.[937] These measures should also be proportional taking into account the objectives of the limitation. Whether limiting the right to the protection of personal data is proportional in such cases where the data relates to public decision-making will be assessed next.

Guidance on solving this issue can be sought from the case-law of the European Court of Human Rights. The Strasbourg Court has drawn some guidelines for assessing whether a person is a so-called "public person". Before engaging in the ECHR's practice in more detail, it must be underlined that ECHR's practice has developed in the course of freedom of expression cases. In other words, in such situations where the information related to a certain person has been published and distributed to public. When such situations are compared with public access to document cases, the restriction to one's privacy must be considered heavier in the former case. In the latter, personal data is not actively disseminated to an unlimited number of people.[938]

The ECHR has categorized two sets of public persons. These categories are politicians and figures of public importance. In accordance with the ECHR's practice, politicians should tolerate interference with their privacy to a certain extent. The ECHR has recognized, however, that other persons who also appear in public might be in a position where the breach of their privacy is allowed to a certain extent. Examples of this group of people would be civil servants and judges.[939] The ECHR's approach seems justified in the sense that when a person is involved in a decision-making process and the outcome of that decision has an effect on the society on more general level, the threshold to withhold information about the said decision makers should be quite high. I see that in the case of politicians the threshold should be even higher; this is for two reasons. Political decision-making allows more margin for discretion than the decision-making carried out by civil servants. The parameters for political decision-making can be drawn from fundamental rights, but it is precisely political decision-making which might amend other rights or

937 See Chapter I, section 2.4.

938 For the media being capable of inflicting the gravest damage on individual as a result of personal information processing, see for example D. Erdos "European Union Data Protection Law and Media Expression: Fundamentally off Balance" in *International and Comparative Law Quarterly* 65 (2016), 140.

939 See for example R. Gisbert, The Right to Freedom of expression in a democratic Society (Art. 20 ECHR), in Garcia Roca & Santolaya (ed.) *Europe of Rights: A Compendium of the European Convention of Human Rights*, (Leiden, 2012), 395.

obligations based on legislation. In other words, the rules on the surface level of law are amended by political decisions. When politicians have such a heavy influence on the rules applicable to society in general, the public in general should know how political decision makers use their influence. Civil servants, in turn, are bound to interpret the existing legislation. Therefore, the margin of discretion carried out by civil servants is limited to cases where the rules on the surface level of law do not provide a direct answer. In other words, while the decisions made by politicians cover all the elements needed for the decision-making, civil servants do not have a margin of discretion; rules are either applicable or not.[940] Naturally in certain cases the question of whether the rule becomes applicable or not might arise. Thus, the civil servant's margin of discretion – if it can be called discretion – is limited to identifying the hard core of the right when assessing the case and seeking an answer from the underlying levels of law.

Not only public figures but also civil servants conducting public duties have been considered differently from ordinary people when it comes to the right to privacy.[941] This baseline was tried in the Valero Jordana case. Both the applicant and the Kingdom of Sweden suggested that the exception to public access to documents laid down in Article 4(1)(b) concerning the protection of personal data should not have applied in the said case. It was argued that the said information did not interfere with the private life of the data subjects, because the applicant was asking only for information which related to the data subjects as civil servants.[942] This argumentation goes alongside with General Court's Bavarian Lager judgment.[943] The General Court did however reject this approach in particular, even if, in the end, it decided the case based on different merits. The General Court underlined that civil servants also have the right to privacy.[944]

3.2.2.2 The status of the person – private actors in the public sector – Reasonable expectations

To elaborate the second category of circumstances, i.e. nature of personal data, further it does not suffice study the concept of public person. To start with, there have been some concerns about the blurring lines between the private and public

940 See Chapter I, section 1.1.

941 See for example R. Gisbert, The Right to Freedom of expression in a democratic Society (Art. 20 ECHR), in Garcia Roca & Santolaya (ed.) *Europe of Rights: A Compendium of the European Convention of Human Rights*, (Leiden, 2012), 395.

942 Case T-161/04, *Valero Jordana v Commission*, ECLI:EU:T:2011:337.

943 Case T-194/04, *Bavarian Lager v Commission*, ECLI:EU:T:2007:334.

944 Case T-161/04, *Valero Jordana v Commission*, ECLI:EU:T:2011:337. See also case C-615/13 P, *ClientEarth and PAN Europe v EFSA*, ECLI:EU:C:2016:489, paras 27–35.

sector. These have mainly related to the lack of transparency in the private sector and, for instance, the inapplicability of freedom of information legislation in the private sector.[945] These concerns are justified in such cases where private sector actors are confided with public sector duties. Furthermore, there are situations where private sector actors are not directly confided with public sector duties, but the private sector actors have influence, one way or another, on public decision-making. As a third example, private sector actors might receive significant aid funded with tax payers' money.

It follows that the assessment of proportionality cannot be carried out solely based on the distinction between public and private persons. This is where the reasonable expectations of the data subject become relevant. Guidelines for this assessment can be drawn from the GDPR.[946] Article 6 of the GDPR sets good frames for this assessment because Article 6 addresses the situations where personal data is processed for a different purpose from that for which it was originally collected. That is to say that further processing is in line with the European data protection legislation when criteria in Article 6 are met; in other words, the data subject should reasonably expect that the data will be further processed in accordance with Article 6.

The GDPR and the EU Institutions' Data Protection Regulation set a non-exhaustive list of elements to be taken into consideration when personal data is processed for a purpose other than the initial processing purposes.[947] The first element on the list is "*any link between the purposes for which the personal data have been collected and the purpose of intended further processing*". When personal data is collected or stored on such an occasion which relates to the position of a person influencing public decision-making, the link between disclosure based on public access to documents and the original processing purposes exists. In such a case, the access request related to the position of the person. The same information would be requested regardless of who the individual participating in the public decision-making was.

The second element on the list id "*the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller*". When personal data is collected in the course of a process which leads to a decision and the data relates to those who are in a position to influence the said public decision-making, the requirements of this element are met.

---

945 J. Freeman, "Extending public accountability through privatization: From public law to publicization", in M.W. Dowdle (ed.) *Public Accountability*, (Cambridge, 2006), 83–111.

946 According to Recital 47 of the GDPR "*the legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller*".

947 Article 6 of the GDPR and article 6 of the EU Institutions' Data Protection Regulation.

The third and fourth elements on the list relate to the nature of personal data and the possible consequence for the data subject. When public access is given to such personal data, which relates to data subject in their capacity to influence public decision-making, consequences which are not necessarily only pleasant might arise. Disclosed information might, for example, reveal how influential a lobbyist organization was in a legislation process. The feedback which follows such a disclosure will not necessarily be pleasant.[948] This is, however, at the very heart of the structures of the democratic society and public's right of access to documents.

When these elements are assessed together with the case-law of the European Court of Human Rights, which clearly requires that public persons tolerate a higher degree of limitation to their privacy, it is safe to conclude that when someone is in a position which enables him or her to influence public decision-making, and access to personal data is requested in this context, there is hardly grounds to argue that the data subject might have reasonable expectations of non-disclosure of the said data. Naturally some other exception laid down in the Transparency Regulation might apply in such a case, for example the exception laid down in Article 4(3) to protect the institution's decision-making process.

3.2.2.3 Sensitive data – Nature of personal data

As a last element to be taken into consideration when the circumstances of the case are assessed, the sensitive nature of the personal data must be assessed. This assessment must be carried out with a view to such data being made publicly available. It is clear that there are such types of personal data which require a high degree of protection. The processing of certain types of personal data is considered more risky from the outset. For example, the processing of special categories of personal data is prohibited by default and allowed only in certain, specified cases. An example of such data is health data, but also other types of data are considered sensitive, such as data concerning religious or philosophical beliefs, sex life or sexual orientation.[949]

To elaborate this further, such personal data which does not fall in the scope of special categories of personal data, but is still somehow sensitive must be examined. The sensitivity does not then follow from the nature of the data itself, but from the wider processing context. The data could reveal for example information about data subject's whereabouts, information which is in many cases harmless. A practical

948 In Case C-280/11 P *Council v Access Info Europe*, ECLI:EU:C:2013:671, para 15, CJEU's reference to General Court's conclusion, "*that it is in the very nature of democratic debate that a proposal for amendment of a draft regulation can be subject to both positive and negative comments on the part of the public and the media*".

949 See for example Article 9 of the GDPR.

example of the importance of the processing context of such data is provided by information which was leaked by Wikileaks. According to newspaper information, the leaks by Wikileaks had put certain people in serious danger.[950] I see that this example demonstrates two things. First, disclosure of personal data requires a context-based assessment. Unintentionally wide disclosure of personal data might lead to serious consequences. It follows that disclosure of personal data almost always requires a certain level of consideration. The circumstances that create the conditions for disclosure of personal data can be formulated with a certain specificity in law, but the legislator cannot take all future situations into account in a detailed manner, and the provisions drafted in law must provide a certain amount of flexibility for the later application of the said provisions.

The second point demonstrated by the given example is how access to all personal data cannot be given by default and the need for protection might derive from other elements than those at the hard core of the right to data protection legislation. Revealing personal information which is not sensitive per se could, for example, hamper international relations or complicate institutions' decision-making processes. At the EU level these other interests are, however, protected by the exceptions laid down in the Transparency Regulation.

Consequently, special categories of personal data cannot be placed at the hard core of the right to the protection of personal data by default. Information about someone's philosophical view on life might be much less sensitive than, for example, information about someone's whereabouts. However, the nature of personal data must be taken into consideration as Alexy's circumstances of the case when the balancing between different rights is carried out.

3.3 HEADING TOWARDS THE HARD CORE

The tension between rights must be balanced with a view to reach the optimal effect of both rights. [951] When the optimal effect is achieved, the essence of the both rights is maintained. The limitations may not be broader than what is strictly necessary.[952] Next, the underlying principles of both rights will be examined. First an analysis is carried out on whether, and to what extent, certain principles need to

950 See for example Helsingin Sanomat, 29.8.2016, A 22.

951 For optimal effect, see K. Hesse, *Grundzüge des Verfaussungsrechts der Bundesrepublik Deutschland*, (Heidelberg, 1990) 142 and T. Marauhn and N. Puppel, Balancing Conflicting Human Rights: Konrad Hesse's notion of "*Praktische Kokordanz*" and the German Federal Constitutional Court, in Brems (ed.) *Conflicts between Fundamental Rights*, (Intersentia, 2008), 279–281.

952 For the proportionality test in the data protection context, see also I. Cameron, "Balancing data protection and law enforcement needs: Tele2 Sverige and Watson", in *Common Market Law Review* 54 (2017), 1470 and case C-203/15, *Tele2 Sverige*, ECLI:EU:C:2016:970.

be limited in order to realize the other right, while simultaneously heading towards the identification of the hard core of the said rights. Thereafter, a conclusion on whether the prescribed limitations will lead to collision of rights will be provided.

3.3.1 PURPOSE LIMITATION AND FURTHER TRANSMISSION OF PERSONAL DATA V WIDEST POSSIBLE ACCESS, NO BLOCK EXEMPTIONS AND NARROW INTERPRETATION OF EXCEPTIONS

It was established earlier that personal data must be collected and processed for specified purposes. The purpose limitation principle is one of the founding principles of European data protection legislation. It is enshrined by the Charter of Fundamental Rights and it was also an essential element in the CJEU's Schrems case assessment, where the CJEU elaborated the essence of the protection of personal data.[953] When personal data is collected for a certain purpose, it may not be further processed for incompatible purposes.[954]

While the purpose limitation principle is very clearly formulated in the Union legislation, the colliding principles of the transparency legislation must be recognized and sought from the deeper levels of law. However, once they have been established, they are equally clear. The principles which collide with the purpose limitation principle have been elaborated in Chapter III. These are the principles of no block exemption[955], narrow interpretation of exceptions and widest possible access.

If the purpose limitation principle was applied as such to situations where the data has been requested based on public access to documents legislation, personal data could hardly ever be disclosed. This cannot be the aim of the purpose limitation principle. It seems that situations where the applicant would process the personal data for the same purposes as the original controller are quite rare. For example, information about the participants of a meeting in the course of public decision-making – or an example from national level, municipal decision-making concerning building permits – would hardly be processed for the initial processing purposes by the applicant. However, the change in the processing purposes would not necessarily signify that the secondary processing is illegitimate. Furthermore, this information could be relevant and sometimes even necessary for the applicant. The relevance could be quite general in its nature too, such as journalistic purposes. Thus, the personal data could be processed for very legitimate purposes even if the initial purpose differentiated from the secondary purpose.[956]

953 Case C-362/14, *Schrems,* ECLI:EU:C:2015:650, para 90.

954 See Chapter IV, section 3.1.

955 For block exemption, see case C-615/13 P, *ClientEarth and PAN Europe v EFSA*, ECLI:EU:C:2016:489, para 70.

956 See for example Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1–88), Recital 50.

Hence, strict interpretation of the purpose limitation principle would create an obstacle to the right of access and deprive the Transparency Regulation of its effect. A vast amount of personal data would never be disclosed, even in such cases where the disclosure would not endanger the interests protected by the exceptions laid down in the Transparency Regulation.[957] In other words, certain information would not be disclosed purely based on the nature of the said information, i.e. for the reason that it is personal data***. This would lead to a situation where the data is protected, not the data subjects or the data subjects' interests. I argue that the ultimate goal or aim of the data protection legislation is, however, to protect data subjects and their interests. Not the data***.

The CJEU's elaboration of the essence in the Schrems case does not lead to different conclusion. Even if the CJEU did set a particular weight on the purpose limitation principle in its assessment, the CJEU did eventually conclude that the essence of the right to private life had been violated due to the wide and general access by public authorities to the content of electronic communication. An aggravating fact was that this access to electronic communication took place in a context in which there were no legal remedies available to the individuals. Hence, the CJEU saw wide access by public authorities and a lack of legal remedies as violating the essence of Article 7 and respectively Article 47 of the Charter.[958]

The circumstances creating the tension studied in this research differ significantly from the circumstances examined by the CJEU in the Schrems case. First, the European legal framework does provide legal remedies for the data subjects. Second, when personal data is collected by the public sector in the course of the exercise of public duties, and should be publicly available from the outset, it can hardly be claimed that the disclosure of personal data was not reasonably foreseeable at the time it was collected. This differs from the circumstances of the Schrems case, where personal data had initially been collected for commercial purposes. When data subjects actively share their own personal information on Facebook and use the said platform as a channel for personal communication, they have the right to expect this information to be shared only with recipients with whom they choose to share it.

Furthermore, strict interpretation of purpose limitation principle would create a block exemption. It was earlier established that one of the underlying principles of the transparency legislation is no block exemptions.[959] It was also acknowledged

957 See Chapter III, section 6.

958 Case C-362/14, *Schrems,* ECLI:EU:C:2015:650, paras 90–95. It ought to be mentioned that access by public authorities in the Schrems case differs significantly from public access, which is examined in this thesis. Public access is sought to official documents, not private communication information between individuals. Also, the context where this takes place differs significantly from the one where personal data was processed in the USA under the Privacy Shield. The redress mechanism is built in the EU data protection framework.

959 For the presumption of non-disclosure, see D. Curtin & P. Leino, "In search of transparency for EU law-making: Trilogues on the cusp of dawn" in *Common Market Law Review* 6 (2017), 1078–1079. The CJEU has established this also in more recent case, see for example in the case C-615/13 P, *ClientEarth and PAN*

that the CJEU has accepted certain presumptions regarding non-disclosure of information. However, these presumptions do not correspond to the situation at hand, where the disclosure relates to personal data, not enormous amounts of information, for example related to infringement procedures.

Simultaneously, strict interpretation of the purpose limitation principle would be contrary to the widest possible access principle and the principle of narrow interpretation of the exceptions. As was noted earlier in Chapter III, both of these principles are well established in the case-law. To conclude, strict interpretation of the purpose limitation principle would be contrary to many of the core principles of the transparency legislation and would create a presumption that personal data could not be disclosed from public documents.[960]

It follows that the purpose limitation principle must be restricted in order to realize the right of access to documents. As Hesse puts it, "*conflicting rights and interest must be subject to limitations, so that each one attains its optimal effect*".[961] Whether the need to restrict the purpose limitation principle would lead to a genuine collision of the rights examined in this thesis can be assessed only after it is clear whether the essence of the said right can be maintained despite of the restriction.[962]

3.3.2 STATING REASONS FOR THE APPLICATION

The next step towards the hard core is to elaborate how stating reasons for the application fits into the overall picture. The question of stating reasons for an application filed under the Transparency Regulation was at the very heart of the Bavarian Lager case. The General Court had concluded that there was no need for reasoning, but the CJEU turned it around. The CJEU underlined that there are no provisions granting one Regulation primacy over the other and that in principle, their full application should be ensured.[963] The CJEU stressed that the Data Protection Regulation must be applied simultaneously with the Transparency Regulation. If this was not the case, personal data would be disclosed from official documents solely based on the Transparency Regulation. In such cases personal data would

Europe v EFSA, ECLI:EU:C:2016:489, paras 69–70. The CJEU did not accept EFSA's argument as this would have led to a situation where a similar argument could have been used as grounds to refuse access to personal data generally in all similar situations.

960 Case T-115/13, *Dennekamp v Parliament*, ECLI:EU:T:2015:497.

961 See Chapter I, section 3. K. Hesse, *Grundzüge des Verfaussungsrechts der Bundesrepublik Deutschland*, (Heidelberg, 1990) 142; T. Marauhn and N. Puppel, Balancing Conflicting Human Rights: Konrad Hesse's notion of "*Praktische Kokordanz*" and the German Federal Constitutional Court, in Brems (ed.) *Conflicts between Fundamental Rights*, (Intersentia, 2008), 279–281.

962 For genuine collision of rights, see Chapter I, section 3. L. Zucca, Conflicts of Fundamental Rights as Constitutional Dilemmas, in Brems (ed.) *Conflicts between Fundamental Rights*, (Intersentia, 2008), 3–126.

963 Case C-28/08P*, Bavarian Lager*, ECLI:EU:C:2010:378, para 56.

be protected solely based on the privacy exception laid down in Article 4(1)(b) of the Transparency Regulation. The CJEU saw that this was not sufficient.

The CJEU's decision renders the tension in a situation where the rules collide on the surface level of law inevitable. The Transparency Regulation stipulates that requests for public access to documents do not need to be reasoned, while the EU Institutions' Data Protection Regulation requires the recipient of the data to establish the necessity for the data transfer.[964] From the outset, these rules cannot be applied simultaneously. This does not, however, necessarily reflect the collision of the underlying principles.

It is given that the requests must be reasoned. This was the core of the CJEU's judgment. This baseline was not amended with the EU Institutions' Data Protection Regulation either. Whether this leads to a collision on the level of principles can be deduced by identifying the essence of the right of access. I will do this by carrying out an assessment of three elements related to the reasoning of an application. The first and second elements are interconnected. First, it will be assessed whether the right to receive public sector information without stating reasons falls within the hard core of the right, and thereafter whether there are certain situations in which personal data should always be disclosed. The third element culminates in the question of how to interpret the requirement to state reasons for the application; in other words, how general or detailed the reasoning should be.

It was earlier established that the aims and objectives of the Transparency Regulation are strengthening democracy, good governance and reducing corruption. These aims are achieved by granting access to information. It was argued earlier that having access to information strengthens democracy in two different ways. First, it creates grounds for participatory, or deliberative, democracy. Second, it provides the general public with the means to supervise decision-making and decision makers.[965] To achieve this goal, it is essential that the applicant has the information. It is secondary if the applicant gives some reasoning in order to receive the information, provided that it will not de facto lead to denial of access to the information.

The right to request information without stating reasons is not widely elaborated in the recitals of the Transparency Regulation. It can be argued that this rule draws from the principle of widest access and on the other hand from public access. To begin with public access, when access is given to the public in general, the reasons for the further use of the requested information are insignificant. This is how public access differs from party access. Therefore, the applicant should not be asked to reason the application – in other words, to provide particular reasons related to

964 See Chapter VI, section 2. The necessity to establish that it is necessary to have the data transmitted follows from the new EU Institutions' Data Protection Regulation as well (Article 9), but other elements included in the Regulation will clarify the situation.

965 See Chapter VII, section 2.1.1.

the specific circumstances.[966] Secondly, widest possible access is ensured when disclosure of the information does not require reasoning. If stating reasons would instead lead to wider access in some rare cases, for example when the requested document contains personal data, providing reasons would not seem to violate the hard core of the right of public access, but rather work in favour of enhancing transparency.

The second interrelated element is whether there are such situations where access to personal data – personal data which is part of an official document – would fall within the hard core of the right of access to information. In other words, whether there is such personal data that the nature of the data sets a presumption for the disclosure, and whether the presumption of access to this data would invade the hard core of the competing right, that is the right to the protection of personal data. It was earlier established that official documents may contain different types of personal data. There is data which relates to decision makers and there is data which relates to other data subjects.[967] I see that access to personal data should be treated differently when access is requested to data which relates to those who are in a position to influence public decision-making. In a democratic society, citizens should have the right to know who influences the decisions which have an effect on citizens. This presumption could be superseded by the exemptions provided by the Transparency Regulation when disclosure of such personal data would endanger some of the interests protected by the said exemptions, such as privacy or international relations.[968] It is clear, however, that the said information is personal data, even if it relates to a certain post or role in public decision-making.[969]

The third element in this assessment sets weight on the processing of personal data. I see that stating reasons to receive personal data derives from two core elements of data protection legislation. The processing of personal data must have a legal basis and personal data may not be further processed for incompatible purposes.[970] First, processing of personal data is only allowed when there is an appropriate legal basis for the processing, or if the processing could fall outside the scope of the GDPR and be carried out, for example, for household purposes. This is an element, which separates data protection from the right to privacy. It was earlier established that the right to the protection of personal data has become an independent fundamental right, separate from the right to privacy. The requirement

966 Particular reasons should be taken into account on a more general level when assessing, for example, the existence of the overriding public interest.

967 See Chapter VI, section 2.1.1.2.

968 See Chapter III, section 6.

969 See for example Case T-94/16, *Psara v. European Parliament,* ECLI:EU:T:2018:602, paras 50–52.

970 The latter element does ultimately come back to the purpose limitation principle.

for a legal basis is the feature that is characteristic for data protection in general and simultaneously clearly separates it from the right to privacy.

In this context, it ought to be underlined that I see that the requirement to have a legal basis for the processing of personal data differs from the more general requirement of Article 52(1) of the Charter of Fundamental Rights which sets the parameters for restricting fundamental rights,[971]namely that the requirement that restrictions to fundamental rights must be provided by law. First, Article 8 of the Charter states that everyone has the right to the protection of personal data concerning him or her; this does not signify that the processing of personal data is banned. In other words, the processing of personal data does not itself constitute a restriction of the data subject's right. This is apparent in the European data protection framework. I give two further examples to illustrate this. Starting with the manual processing of personal data, which is excluded from the scope of the GDPR; it does not follow from this exclusion that the said data may not be processed at all because the processing is not based on law. Instead it may be processed without any limitations as long as the data does not form a data file. This is logical, because the said data processing does not endanger the interests of the data subject, with the scale of the processing being always quite moderate. Further, Article 9 of the GDPR forbids the processing of special categories of personal data. If data processing was banned from the outset, there wouldn't be a need to separately legislate on the said prohibition. Thus, the processing of personal data does not itself constitute a restriction of the data subject's right. Furthermore, if the processing of personal data was considered a restriction to the data subject's right, it would lead to a situation where the data itself was protected, not the data subject or data subject's interests. Even if in everyday language it is very common to use terminology that refers to protection of personal data, the aim is not to protect the data, but rather the data subjects. The GDPR's name quite clearly illustrates this; it is "*a regulation on the protection of natural persons*" with regard to the processing of personal data.

Moving back to assessing the requirement to state reasons for the application, another element included in the requirement to establish the necessity of the data transfer is the purpose limitation principle. The purpose limitation principle is one of the core elements of data protection, but it was earlier established that it is necessary to limit the purpose limitation principle in order to realize one's right of access to documents. This leads to a situation where the applicant should not be required to demonstrate that the further processing of personal data will be carried out for purposes compatible with the original data processing. This argument draws

971 For similar conclusion in the context of analyzing the CJEU's rulings related to protection of personal data, see also G. González Fuster, "Fighting For Your Right to What Exactly? The Convoluted Case Law of the EU Court of Justice on Privacy and/or Personal Data Protection" in *Birbeck Law Review*, 2(2) (2014), 271–278; G. González Fuster & R. Gellert, "The fundamental right of data protection in the European Union: in search of an uncharted rights" in *International Review of Law, Computers & Technology* 1(2012), 78–81.

support also from the recent case-law of the General Court; the Court does not lay emphasis on the purpose limitation principle in its reasoning when it is assessing whether the applicant has provided sufficient reasons.[972] Further backing for this approach can be sought from the recently adopted EU Institutions' Data Protection Regulation. Recital 28 of the Regulation clarifies that the specific purpose, referred to in the article on transmission of personal data, can relate to the transparency of EU institutions and bodies. The recital clarifies that when personal data is transmitted to recipients in the Union, and the recipient needs to establish the necessity for the data transfer, the specific purpose in the public interest for which the data is transferred can relate to the transparency of the Union institutions. This should not, however, be read as if personal data could be further processed for whatever purposes when the recipient has received it based on the said provisions. General parameters for data processing also apply to the processing of personal data received based on Transparency Regulation.[973]

It has been established that public access to documents cannot be realized when the purpose limitation principle applies. It hasn't been examined yet, whether the requirement to have an appropriate legal basis for the data processing would lead to a similar conclusion. The requirement to process the data legitimately either based on an appropriate legal basis or for the purposes which are excluded from the data protection regime would create an obstacle to public access to documents in such cases where the applicant does not have an appropriate processing purpose. In other words, the applicant would receive the information in such cases where the processing of personal data can be considered legitimate. This would differ from establishing the necessity to have the personal data transferred. The suggested approach sets the threshold to provide information for the further processing lower. It would suffice to give information about the intended legal basis applied in the processing, in other words, ***a simple informational notice would fulfil the requirement.*** This must be separated from party access where the position of the applicant is a significant element when assessing whether the information can be released. ***Legitimate processing purposes would not necessarily need to contain the actual, particular processing purposes; a more general reference to appropriate processing purposes should be considered sufficient.*** This approach would enable the applicant to request public access to documents anonymously and thereby meet the right to file an application anonymously based on the Transparency Regulation.

---

972 Case T-94/16, *Psara v. European Parliament,* ECLI:EU:T:2018:602 ; case C-615/13 P, *ClientEarth and PAN Europe v EFSA*, ECLI:EU:C:2016:489.

973 For case law, see in particular ase C-131/12, *Google Spain and Google Inc*, ECLI:EU:C:2014:317 and case C-73/07, *Satakunnan Markkinapörrsi and Satamedia*, ECLI:EU:C:2008:727.

The suggested solution reflects the existing case-law of the Luxembourg court. The CJEU has established that publicly available information must be processed in accordance with data protection legislation.[974] In other words, information that is legally publicly available must be processed in accordance with data protection legislation. The General Court has in turn agreed that general reasoning is sufficient, when data is applied for based on the Transparency Regulation.[975] Some further indications of how to assess adequate reasoning have been developed in later CJEU practice. According to the CJEU, public interest as such would not provide sufficient reasoning for disclosure. It did, however, consider reasoning based on suspicions regarding the impartiality of expert advice as adequate reasoning for the disclosure.[976] After the entry into force of the EU Institutions' Data Protection Regulation, this must also be read together with Recital 28, which confirms that the transparency of Union institutions and bodies can justify the disclosure of data. Drawing from this, it seems that the applicant is not expected to give detailed reasoning regarding the intended further processing related to his or her particular situation.

It must be noted that the General Court has in its more recent case-law argued that transparency does not justify as such transfers of personal data.[977] I see that this conclusion alone does not contradict what was just said. This conclusion was drawn in a case where the applicant had requested bank extracts from certain MEP's bank accounts. When the balancing exercise is carried out, it is relevant what type of personal data is at stake. The situation has become even more clear with the EU Institutions' Data Protection Regulation, with Recital 28 clarifying that the transparency of Union institutions and bodies can justify disclosure of data.

To conclude, if the applicant was to give general information about the intended legal basis of the further processing, the requirements elaborated in the CJEU's case-law read together with Recital 28 of the EU Institutions' Data Protection Regulation would be met.

3.3.3 THE INVIOLABLE CORE OF THE RIGHT OF PUBLIC ACCESS TO DOCUMENTS AND THE RIGHT TO DATA PROTECTION

It was earlier established that the hard core of the right has a rule-like effect; it does not allow balancing. It follows that a genuine conflict of fundamental rights exists only when the hard core, i.e. the essence of the right, collides with another

974 Case C-131/12, *Google Spain and Google Inc*, ECLI:EU:C:2014:317 and Case C-73/07, *Satakunnan Markkinapörrsi and Satamedia*, ECLI:EU:C:2008:727.

975 Case T-115/13, *Dennekamp v Parliament*, ECLI:EU:T:2015:497, para 61.

976 Case C-615/13 P, *ClientEarth and PAN Europe v EFSA*, ECLI:EU:C:2016:489, paras 47–61.

977 Case T-94/16, *Psara v. European Parliament,* ECLI:EU:T:2018:602, paras 76, 91.

right and cannot be put into effect simultaneously. It was also established that the hard core of the fundamental right might be fragmented.[978] So far this section has focused on the underlying principles of the said rights, also taking partly into account the underlying objectives and aims of the said rights and has given some first suggestions on how to reconcile the right of public access to documents with the protection of personal data by limiting the other right only to the extent of what is strictly necessary.

Next, the dimension of the hard core of the examined rights will be identified in order to conclude whether there is a genuine conflict of fundamental rights at stake, or whether is there room for proportional balancing. First, the essence of the right of public access to documents will be identified. This is followed by a similar, though lengthier, analysis of the essence of the right to the protection of personal data. It was earlier established that the right to protection of personal data is a multidimensional concept and the upcoming analysis reflects this feature of data protection.

3.3.3.1 The essence of the right of public access to documents

The underlying principles of public access to documents, the right to receive information, were discussed earlier. This principle can be further elaborated in two different sets of circumstances related to access to personal data. The first circumstances would cover all types of personal data, and the second circumstances would cover situations where the data relates to persons who are in a position to influence public decision-making. The first set of circumstances will be discussed next. Thereafter, the second set of circumstances will be covered.

3.3.3.1.1 The right to receive information

The colliding rules on the surface level of law are the requirements to establish the necessity for data transfers based on the EU Institutions' Data Protection Regulation and the right to receive information without stating reasons based on the Transparency Regulation. These colliding rules were discussed in detail in Chapter VI, section 2.

Being fully aware of the harsh criticism this may cause among my dear, distinguished Finnish colleagues, I dare to argue that the applicant's right to file an application without stating reasons does not fall within the hard core of the right of access to documents. But this is only within certain parameters. First, to be more

978 See Chapter I section 2.2.1.

accurate, a lighter version of stating reasons for the application. I would call this *informing the controller of the legal basis on which the personal data is intended to be processed*. This would signify that the applicant would inform the civil servant who decides on the disclosure of personal data, of the legal basis on which the intended further processing of personal data will be based. This would not require further or more detailed reasoning from the applicant and would not include the necessity to establish the intended processing purposes. Thus, simple information about the intended legal basis for the processing would suffice for exercising the right of public access to documents which contain personal data. This would require that an applicant who requests access to personal data is at least aware of the data protection requirements and carries out some light planning on how to process the data. In other words, the applicant should understand that there are certain limitations to how personal data may be further processed. It would also set a light supervisory responsibility on the public sector actor who discloses the information. The ultimate responsibility to ensure that the data has been appropriately processed would stay with the competent data protection authority, with this being the national supervisory authority in most cases. When personal data is disclosed to an applicant in the Member States, this would set the national supervisory authority as the final guardian of the secondary processing of personal data. The GDPR sets out similar powers and duties for the supervisory authorities in all Member States, hence this should guarantee the appropriate supervision of the data processing in all Member States. The European Data Protection Supervisor would hardly take the role as the final guardian of the processing in these situations, because the competence of the EDPS covers the EU institutions. Unless data transfers between institutions were based on the same structure, the role of the EDPS would continue to be supervising whether the institutions have met their obligations when disclosing the personal data.[979]

It was established earlier that the Transparency Regulation itself recognizes the possibility of the public authority engaging in a dialogue with the applicant in order to better meet the needs of the applicant. This possibility is also recognized in the national legislation, for example, in Finland. It follows that if stating the legal basis for the intended data processing in order to apply the rights given in the Transparency Regulation is accepted as starting point, the institutions should assist the applicant with this task when the applicant is unaware of this requirement. And when the legal basis for the secondary processing purposes is apparent, the institution should take this into account on its own initiative, even if the applicant hadn't understood the need to formulate this reasoning in their application. This duty would follow from the requirements of good governance and can be derived from the practice related

979 Data transfers to third countries based on access to documents legislation are excluded from the scope of this assessment.

to public access to documents, i.e. the institutions' obligation to assess whether there is an overriding public interest.[980] The threshold for submitting the intended legal basis for data processing, when data is sought based on the Transparency Regulation, should not be set too high. Requiring very detailed reasoning about the processing purposes approaches the limits of the essence of the Transparency Regulation and the right of access, and would simultaneously set an obstacle to anonymously requesting public access to documents. This would invade the hard core of the right of access.

Actual access to information lies within the hard core of the fundamental right of public access. This can be realized by handing out the personal data to the applicant when the information about the intended legal basis is given to the controller, i.e. EU institution. Submitting the intended legal basis would not set obstacles for the aims and objectives of the Transparency Regulation either. It would not render the two transparency tools of democratic decision-making void; quite the opposite. Further, simply notifying the intended legal basis would not prevent the actualization of the other aims and objectives identified earlier in this thesis – good governance and reducing corruption – either. Thus, a light informational obligation about the legal basis would not infringe the hard core of one's fundamental right of access to documents, provided that this obligation remains light. It is of utmost importance that the threshold for providing such information remains on such a level that the identity of the applicant can remain anonymous.

The judgment by the General Court in the Bavarian Lager case balanced data protection with public access to documents by excluding the data protection legislation entirely from the assessment. The approach suggested in this thesis would take the core elements of the data protection legislation into account. These elements are privacy and the requirement to have an appropriate legal basis for the processing of personal data. Furthermore, other rights provided by the Charter of Fundamental Rights, i.e. the data subject's right of access to his or her personal data or the right to rectify the data concerning him or her, would not be hampered either. The data subject could exercise these rights in relation to the original controller and in cases where the secondary data processing takes the form of full-scale data processing, the data subject can exercise these rights towards the secondary data controller. This also reflects the current situation when it comes to the processing of personal data. The judgment and consequences of the Google case give a perfect example of that.[981]

Furthermore, the suggested approach would be also in line with the requirements set by the CJEU's judgment stating that in principle both data protection and transparency legislation should be fully applied. The suggested solution is drawn

980 See Chapter III, section 5.2.

981 Case C-131/12, *Google Spain and Google Inc*, ECLI:EU:C:2014:317.

from giving a narrow interpretation for the requirement "*to state reasons for the application*". One of the underlying principles of the Transparency Regulation is the narrow interpretation of the exceptions to public access to documents. When data protection legislation is applied to public access to documents requests based on Article 4(1)(b) of the Transparency Regulation, the contradictory requirements set in the data protection legislation, i.e. the obligation to state reasons, should be interpreted narrowly. This is how the contradictory goal set by the Bavarian Lager case can be achieved; applying the rules of the data protection legislation in light of the principles drawn from the Transparency Regulation. This is possible by interpreting the current provisions accordingly, or the situation could alternatively be clarified by new formulation of certain provisions of the Data Protection Regulation.

Notification of the intended legal basis would not set an obstacle for the institutions to apply some of the exceptions laid down in the Transparency Regulation. If there was a danger that was reasonably foreseeable and not purely hypothetical, the privacy exception could apply, or some other exception for that matter, such as the exception at 4(3), which protects the institutions' decision-making process. This would guarantee that the other element in the hard core of data protection, namely privacy, would enjoy appropriate protection.

Lastly, if stating reasons for the application was considered a violation of the essence of the Transparency Regulation, even when such a requirement would consist only of a light informational obligation which does not reveal the identity of the applicant, a genuine conflict of fundamental rights would exist. If personal data was disclosed regardless of the existence of the legal basis for the secondary data processing, it appears that the data subject's rights would not be safeguarded. This characteristic feature of the data protection legislation would be dimmed, and the weight would be on the privacy rights.

3.3.3.1.2 Right to receive information related to public decision-making

This section has focused on the right to receive information. Earlier in this thesis, it was argued that the right to receive personal data which relates to persons who are in a position to influence public decision-making is within the hard core of the right of public access. There have been some attempts to express this element in the previous case-law, both on the EU level and on the national level.[982] To draw the previous discussions together, when contextual, moment-to-moment interpretation is exercised, the aims and objectives of the Transparency Regulation – that is, strengthening the democratic structures of society – must be taken duly

982 Case C-28/08P, *Bavarian Lager*, ECLI:EU:C:2010:378; KHO 2014:83.

into account and the nature of the personal data dictates how its disclosure is to be assessed.[983] There is no right to anonymous decision-making.

Furthermore, I argue that there is always a legal basis for processing the personal data of such persons who are in a position to influence public decision-making. This legal basis can be drawn either from Article 6(1)(f) of the GDPR which concerns the legitimate interest of the controller or Article 6(1)(e) of the GDPR which relates to public interest of the controller. Alternatively, the national flexibility provided by the GDPR could be exercised to provide a more clearly-framed legal basis for the said data processing.

Thus, a presumption of an existing legal basis for data processing should be deemed to exist when personal data relates to persons who are in a position to influence public decision-making. If the disclosure of the personal data would infringe the privacy rights or some other interests of the said data subject, some of the exceptions of the Transparency Regulation could then be applied. Thus, the information should be withheld if there are any grounds to conclude that some of the interests protected by the exceptions laid down in the Transparency Regulation would be jeopardized by the disclosure.

3.3.3.2 The essence of the right to protection of personal data

This section will elaborate the elements which can be placed within the hard core of the right to the protection of personal data.[984] It was earlier established that the hard core of a fundamental right does not necessarily constitute only one element, but may contain several different elements. In other words, there might be several elements in the hard core of a right and, as such, the right could have a rule-like effect.[985] In order to establish these elements, the circumstances of the case must be appropriately assessed when identifying the essence of the right.[986] Next, I will argue that two elements will form the essence of the right to the protection of personal data. The first element is privacy or the right to self-determination. The second element is the requirement to have an appropriate legal basis for the processing of

983 See for example the 1 preamble of the *Explanatory Report – CETS 205 – Access to Official Documents*, which states that transparency of public authorities is a key feature of good governance and an indicator of whether or not society is genuinely democratic and pluralist, opposed to all forms of corruption, capable of criticizing those who govern it, and open to enlightened participation of citizens in matters of public interest.

984 For example Clifford and Ausloos have also elaborated the question of the hard core of the data protection and in particular the role of fairness in this context. See D. Clifford and J.Ausloos, "Data Protection and the Role of Fairness" in *Yearbook of European Law* 37 (2018).

985 See T. Ojanen, "Making the essence of fundamental rights real: the Court of Justice of the European Union clarifies the structure of fundamental rights under the Charter" in *European Constitutional Law Review* 2 (2016), 321–323.

986 For circumstances of the case, see R. Alexy, *A Theory of Constitutional Rights*, (Oxford, 2010) 54, 100–107.

personal data. Thereafter, an assessment of some other central elements of data protection will follow. These elements might be placed close to the inviolable core, but not at the centre of the said right.

3.3.3.2.1 Right to privacy and self-determination in contextual interpretation

I argue that the hard core of the right to the protection of personal data must be assessed differently when data processing takes place in the public sector and when it takes place in the private sector. As Ojanen notes, "*the identification of the essence is a matter of contextual, moment-to-moment interpretation*".[987] In Alexy's terms, the circumstances of the case are the elements for measuring the dimensions of principles.[988] As earlier argued, when the processing of personal data takes place in a commercial environment, such as Facebook or supermarkets' loyalty programmes, the data subjects often voluntarily provide personal information to the controller. In such scenarios, the more traditional approach where the weight is on the endangerment of the data subject's privacy in a case of disclosure does not seem to provide a sufficient answer as to what falls within the hard core of the said right. Instead the weight should be laid on self-determination. When the data subject him or herself is the source of the information, the need to protect the right to control one's own personal data seems to gain more importance.

Thus, one should place self-determination at the centre when data is processed for private sector purposes. This also reflects the developments deriving from the GDPR. As argued earlier, self-determination is gaining increasing importance in the new data protection regime. It was also argued earlier that the right to self-determination does not have a similar effect when the processing of personal data takes place in the public sector, because of the different requirements for public sector data processing. A particular emphasis was set on the public sector legal basis when it comes to data processing. Generally, the legal basis for public sector data processing is more precise and derives from the national or Union legislation.

To elaborate this further, when processing takes place in the public sector, the data subject is hardly providing the controller with a vast amount of information on their own initiative. The data subject is often in a position where they have no control over the collection of their personal data. The same applies for the controller. The processing of personal data carried out by public authorities is generally based on a legal obligation or the public interest. When these legal bases are applied, there is

987 T. Ojanen, "Making the essence of fundamental rights real: the Court of Justice of the European Union clarifies the structure of fundamental rights under the Charter" in *European Constitutional Law Review* 2 (2016), 326. See also M. Brkan, "The Unstoppable Expansion of the EU Fundamental Right to Data Protection: Little Shop of Horrors?" in *Maastricht Journal of European and Comparative Law*, 23 (2016), 827.

988 R. Alexy, *A Theory of Constitutional Rights*, (Oxford, 2010) 54, 100–107.

detailed legislation covering the processing of personal data.[989] The controller seldom has a choice regarding the processing purposes, or the amount of data collected etc. When detailed provisions regulate the said processing, there is less room for data subject's self-determination. Thus, there is little space to place the right to self-determination within the hard core of the data protection, when processing is carried out by the public sector. The public sector should limit its data collection to what is necessary in any case, and this premise should be taken duly into account in the law drafting process. By contrast, weight should be set on the protection of data subjects' interests in these situations. It follows that public authorities should ensure that the privacy of data subjects will not be infringed.

It was earlier established that similar circumstances would lead to similar outcomes.[990] The context in which the said rights are balanced create different circumstances. Identifying these different circumstances enables the formulation of precise conditions leading to similar outcomes in similar cases. Thus, even if the inviolable essence must be assessed differently on a case-by-case basis, this does not lead to arbitrary outcomes.[991] When balancing takes place in the social media type of environment, the data subject's right to self-determination forms a part of the inviolable core; the data subject has deliberately shared information about him or herself on social media. However, when balancing takes place in the context of public sector processing, it is the right to privacy which forms a part of the inviolable core of the right. This characterization of different circumstances creates a rational formulation for the balancing in each case.

Now, even though I separate self-determination from privacy, it ought to be noted that self-determination is an underlying value of privacy and as such cannot be entirely separated from privacy. Thus, the core of self-determination returns to privacy rights.[992] It follows that even in the contextual case-to-case analysis where the data processing environment sets a different angle for the assessment, the core of these rights stems from the same source.[993]

The right to object also reflects the underlying principle of self-determination. The right to object was earlier identified as one of the conflicting rules.[994] However,

989 See for example case C-398/15, *Manni*, ECLI:EU:C:2017:197, where the CJEU balanced interests related to protection of personal data and public access to such data. The CJEU decided the case in favour of transparency, setting an onus on the national court to examine whether there might be particular reasons to restrict public access to the personal data and give instead more limited access only to such requesters who have a specific interest in access.

990 R. Alexy, *A Theory of Constitutional Rights*, (Oxford, 2010) 54, 100–107.

991 See Chapter I, section 2.2.1.

992 See Chapter IV, section 1.

993 See also H. Nissenbaum, *Privacy in context – Technology, Policy, and Integrity of Social Life*, (Stanford University Press, 2010) 73. Nissenbaum suggest that privacy is control or restricted access to information about us.

994 See Chapter VI, section 2.

as has been underlined previously, this does not yet imply that a conflict of principles and fundamental rights exists.

Even if the right to self-determination and privacy can be placed within the hard core of the right to the protection of personal data, the rule of the right to object does not fall within the hard core of the right to protection of one's personal data. First, this element is not separately mentioned in the Charter of Fundamental Rights, unlike, for example, the data subject's right of access and right to rectification. Second, the GDPR provides an explicit possibility for the controller, and also for the Union or national legislator, to exempt from the right to object. Third, the right to object applies only in such situations where the processing of personal data is based on certain legal bases.

Furthermore, the GDPR sets a threshold for applying the right to object. When a data subject exercises his or her right to object, the objection must relate to a particular situation. The exact content of particular situation has not yet been elaborated in the case-law as the GDPR became applicable in May 2018. Furthermore, the controller is allowed to continue the processing when it demonstrates compelling legitimate grounds for it. These compelling legitimate grounds must also override the interests of the data subject. Thus, even if the Union or national legislator has not exercised the leeway provided by the GDPR and set an exemption from the right to object, the controller can deny the data subject's right to object if there are legitimate grounds for it. Hence, the controller has some margin of appreciation regarding the data subject's right to object. Eventually it will be for the Court to decide whether this margin has been appropriately used.

Hence, it is established that the right to object is not within the hard core of the right to data protection. The next step is to assess whether the limitations to right to object would be suitable to gain the objectives it is aimed at. To conduct a proper assessment on this issue, one should first establish the how right to object would be limited.

3.3.3.2.2 Legal basis for the processing of personal data

When formulating the hard core of the right to the protection of personal data, there is one element that should be placed at the very centre of the hard core of data protection regardless of the context in which the processing takes place. This is the legal basis for the processing of personal data.

The Charter of Fundamental Rights very clearly stipulates that personal data must be processed on the basis of the consent of the data subject or some other legitimate basis laid down by law. The GDPR sets the legal basis for data processing in Article 6. Unlike the purpose limitation principle, the GDPR does not allow exemptions from this requirement in national or Union law. Apart from the requirement of legal basis, the GDPR allows exemptions from all of the elements

stipulated by the Charter of Fundamental Rights. These are the purpose limitation principle, the right of access to one's own personal data and the right to rectify it. The restrictions to these rights must be laid down in national or Union law, but the requirement to have a legal basis for data processing may not be exempted even by national or Union law.[995]

Furthermore, the weight given to an appropriate legal basis is apparent when personal data is collected from publicly available information, as was the case in Google v Spain.[996] It was clarified in the Google case that even if the data is already in the public sphere, that fact itself does not provide sufficient preconditions for meeting the data protection requirements, and the secondary data processing must also be in line with the data protection legislation. And the first requirement to meet the data protection legislation is to have an appropriate legal basis for the data processing.

Lastly, the requirement for a legal basis also separates data protection clearly from privacy rights. This is noteworthy as it demonstrates data protection's emergence onto the field of fundamental rights as an independent player. Even if the protection of personal data is still strongly connected with privacy rights, and the protection of one's privacy together with self-determination forms an essence of the right to the protection of personal data, the requirement for a legal basis is the decisive feature which separates data protection from its roots.

3.4 OTHER ELEMENTS NEAR THE HARD CORE OF THE RIGHT TO DATA PROTECTION

The previous subsection studied the elements constructing the hard core of the right to data protection. This subsection will discuss other essential elements of the said right. As was argued earlier in this thesis, the elements covered in this section do not however fall within the hard core of the said right. First, a concluding glance at the purpose limitation principle will be given and this is followed by some remarks about special categories of personal data.

Purpose limitation is one of the fundamental principles and corner-stones of the European data protection regime. The purpose limitation principle is safeguarded by the Charter of Fundamental Rights, and on more practical level it has played a significant role, for example, in the Privacy Shield negotiations between the EU and the United States. Nevertheless, the purpose limitation principle is not absolute in the sense that it wouldn't allow any restrictions without a collision of principles

995 The GDPR does provide flexibility regarding the legal basis what it comes to reconciling protection of personal data with the freedom of information.

996 Case C-131/12, *Google Spain and Google Inc*, ECLI:EU:C:2014:317.

and thereby a collision of rights. Further processing of personal data for scientific and statistical purposes, for example, is not to be considered incompatible with the initial processing purposes and as such, it is not in contradiction with the purpose limitation principle. The GDPR also gives leeway to the Member States to derogate from the purpose limitation principle, and the CJEU's analysis of Safe Harbour violating the essence of the right to a private life did not culminate in the breach of the purpose limitation principle – instead the core element was too wide and general access by public authorities to the content of electronic communication.[997]

Thus, the purpose limitation principle does not belong within the hard core of the right to the protection of personal data even if it must be placed very close to the hard core. The purpose limitation principle does not therefore carry a rule-like effect as the elements in the hard core of the right do; it is not absolute. It follows that the purpose limitation principle can be restricted and when this restriction is proportional, in other words realized only to the extent necessary to realize public access to documents, it does not lead to a collision between the protection of personal data and public access rights.

Another element which must be place close to the hard core of data protection is sensitive personal data. It was earlier argued that access to personal data related to the public decision-making process falls very close to the hard core of the right of access. Sensitive data in turn falls very near the hard core of the right to data protection. This illustrates the importance of contextual interpretation and the significance of the circumstances of the case. Sensitive personal data has been given a special status in European data protection legislation. This issue was discussed earlier in this thesis and now it suffices to note that sensitive data must be placed close to the hard core, but it does not form the essence of the said right.

4. TENTATIVE INTERPRETATION TOOL RECONCILING THE RIGHT TO PUBLIC ACCESS WITH THE PROTECTION OF PERSONAL DATA

To draw together the discussions from the previous chapters and sections, an interpretation tool together with a tentative drafting proposal will be provided in this section. This will reflect the current case-law and newly adopted EU Institutions' Data Protection Regulation accordingly. There was an excellent opportunity to provide further clarification on the relationship between the examined Regulations in the course of the recently concluded reform of the Data Protection Regulation.

997 Article 23 of the GDPR; Case C-362/14, *Schrems,* ECLI:EU:C:2015:650, paras 90–94.

This opportunity was not wasted, and the new Regulation clarifies certain elements, which have caused tension between the Transparency and the Data Protection Regulation.

However, some issues remain unsolved and an interpretation tool providing the means to apply both Regulations simultaneously will be elaborated next.

4.1 CURRENT SITUATION

Consent has been one of the main components when it comes to the disclosure of personal data from public documents. The data subject's consent is one legal basis for data processing. It is the legal basis which most clearly reflects the right to self-determination. The Charter of Fundamental Rights does not set a preference on consent as a legal basis, but it does distinctly mention it. The Charter states that personal data must be processed on the basis of the consent of the person concerned or some other legitimate basis laid down by law.

Article 6 of the GDPR sets out five other legal bases for data processing. Similarly, the EU Institutions' Data Protection Regulation sets out alternative legal bases for data processing. When an assessment of the data processing takes place in relation to public access to documents, there is public sector data processing at hand. This means that the data should not be processed based on the controller's legitimate interest; the GDPR excludes this possibility from the public sector. Most public sector processing is based on legislation and on the subsections (c) and (e) of Article 6(1) of the GDPR. These legal bases relate to legal obligations to which the controller is subject and the public interest. It follows that the legal basis for data processing should in most cases be drawn from these subsections. However, other legal bases, i.e. consent, contract and the vital interest of data subject, are available for public sector actors too.[998] Even if the public sector is not entirely deprived of the use of consent as a legal basis, it should be used sparingly, given the imbalance between the controller and processor.[999]

Asking for the consent of the data subject for further transmission of their personal data in such cases where a third person has filed an application based on the Transparency Regulation provides an easy way out – when the data subject does indeed consent. However, I see that the central means to disclose and further process personal data should not be the data subject's consent. This sets the balancing of

998 Similarly EU Institutions' Data Protection Regulation Article 5 allows processing of personal data based on the said legal basis.

999 See Recital 43 of of the Regulation (EU) No 679/2016 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) (OJ L 119, 4.5.2016, p. 1–88).

the rights on the data subject. Naturally the data subject assesses the situation purely from his or her personal angle. This does not seem to provide a well-adjusted approach to disclose personal data. I see that it should be the controller, which in these cases is the institution or body, that should conduct the balancing test.

To elaborate further where I am coming from, I see that that the data subject should not be put in a position where they can stipulate how another person's fundamental rights are to be fulfilled, or in other words to decide how someone can exercise the right of access and receive information from public documents. This is in particular the case when the nature of the personal data falls in the hard core of the right of access and relates to public decision-making. Furthermore, in such cases where the right to object applies to data processing and access is requested to information which relates to public decision-making, a particular weight in the assessment should be set on the shared objective of good governance, an aim shared by both of the examined Regulations. When assessing how to interpret whether compelling legitimate grounds exist, a heavy weight should be given to this aim.

Furthermore, one last observation about current practice will be made, namely Council practice to disclose *erga omnes* all documents. It was earlier argued that public access to documents does not equal online internet access to documents. The potential invasion of privacy is on different level in these two situations. Recent judgments by the European Court of Human Rights support this argument. The European Court of Human Rights concluded in its Satamedia decision that "*the fact that the data in question were accessible to the public under the domestic law did not necessarily mean that they could be published to an unlimited extent*".[1000] Furthermore, all of the requirements of the data protection legislation must be taken duly into account in such situations. Hence, despite of the good aim of enhancing transparency, *erga omnes* disclosure would actually restrict the access to public documents which contain personal data. Disclosure of such information should be carried out on a case-by-case basis.

4.2 INTERPRETATION TOOL AND DRAFTING PROPOSAL

It was earlier established that personal data may not be further processed for purposes which are incompatible with the initial processing purposes. It was also established that all processing of personal data must have a legal basis. When further processing of personal data is addressed conjointly with the Transparency Regulation, it should be assessed in a two-step process. First the applicant would provide information about the intended legal basis for the controller. This first phase

1000 See ECtHR 77 June 2017, *Satakunnan Markkinapörssi Oy and Satamedia Oy v Finland* (ECLI:EC:ECHR: 2017:0627JUD000093113), para 190.

would be quite informational in its nature. The controller would carry out a prima facie type assessment of the legal basis provided by the applicant. This first phase would be based on the EU Institutions' Data Protection Regulation, in particular its Recital 28 as read together with the underlying principles of the Transparency Regulation. In cases where the applicant is not able to provide the controller with information about the intended legal basis, the controller would not disclose the said information.

The second phase would fall entirely under the Transparency Regulation. When the first phase has been fulfilled, the institution would still need to assess whether some of the exceptions laid down in the Transparency Regulation would become applicable. While the distinctive feature of the data protection legislation was reconciled with the right of access during the first step, the second phase would ensure that the privacy of the data subject is protected. Further, the second phase would also ensure that the other interests protected by the said exceptions are not compromised. When another reason to withhold the information exists, for example the protection of international relations, the said exception would apply. Thus, the personal data should be disclosed when an appropriate legal basis exists unless there are reasons to withhold the information based on the exceptions laid down in the Transparency Regulation.

When there is no reason to withhold the personal data based on the exceptions provided in the Transparency Regulation, the applicant would receive the personal data. As was established earlier, personal data that is in the public sphere must also be processed in accordance with the data protection legislation. Thus, the applicant should ensure that the requirements set by European data protection legislation are met when the data is further processed. It was earlier noted that the institution would have a light responsibility to control the further processing of personal data in such cases. This duty would have been fulfilled by verifying that the applicant has the right to process personal data based on the GDPR or EU Institutions' Data Protection Regulation. The actual supervisory duty would remain with the competent supervisory authority.

When I was drafting the concluding chapter, negotiations on the EU Institutions' Data Protection Regulation were still ongoing. At that time, I suggested adding a new provision in the former Data Protection Regulation in order to clarify that the purpose limitation principle does not apply when personal data is requested based on the Transparency Regulation. The suggested formulation for the new provision would have been: *Personal data may be disclosed based on a request filed under Regulation 1049/2001 when the applicant informs the controller of the intended legal basis [his/her right to process the personal data based on the GDPR].*

Thus, the entire Article would read as follows:

Article 6

Change of purpose

Without prejudice to articles 4, 5 and 10:

1. Personal data shall only be processed for purposes other than those for which they have been collected if the change of purpose is expressly permitted by the internal rules of the Community institution or body.
2. Personal data collected exclusively for ensuring the security or the control of the processing systems or operations shall not be used for any other purpose, with the exception of the prevention, investigation, detection and prosecution of serious criminal offences.
3. *Personal data may be disclosed based on a request filed under Regulation 1049/2001 when the applicant informs the controller of the intended legal basis of the processing*.

However, the new EU Institutions' Data Protection Regulation does not contain a similar provision on change of purpose as the previous Data Protection Regulation had. The initial idea of the drafting proposal was that it contains the two-step process for the assessment discussed earlier in this thesis. It was suggested that personal data may disclosed *based on a request under Regulation 1049/2001*, which is the Transparency Regulation. This formulation suggests that the Transparency Regulation applies to such information. In other words, once the applicant has fulfilled the light informational obligation, the exceptions laid down in the Transparency Regulation become applicable.

Another solution was adopted in the EU Institutions' Data Protection Regulation. This was the clarification in Recital 28 on the legitimate grounds for further processing. This also clarifies that personal data may be further processed based on transparency legislation. Furthermore, Article 9(3) states that Union institutions and bodies shall reconcile the right to the protection of personal data with the right of access to documents in accordance with Union law. This thesis provides a suggestion for interpreting the Union legislation and the contradictory requirements stemming from the legal framework in order to meet the requirement set by the CJEU to fully apply both Regulations, without violating the essence of either of the examined rights.

The new EU Institutions' Data Protection Regulation will incorporate some elements elaborated in this research, such as the controller's responsibility to assess whether the personal data should be disclosed or not. It will also clarify that personal data may be transferred for the purposes of the institutions' transparency. These are welcome steps forward on this particular issue. However, some work still remains to be done. This thesis provides tools for interpreting the new Regulation together with the existing case-law, in particular how to assess when the criteria for the reasoning of the application have been met.

5. CONCLUDING REMARKS

To draw together the previous sections, the apparent tension between the colliding rules of data protection and public access to documents legislation on the surface level of law does not reflect a collision of the underlying principles. The principles which reflect these rights can be reconciled while maintaining the essence of both rights. Thus, there is no genuine conflict of fundamental rights, even if the tension between the examined rules is apparent.

When appropriate balance has been sought from the deeper levels of law, the hard core of both rights should be maintained. Neither fundamental right should be restricted more than is strictly necessary for the realization of the other right. The core elements for reconciling public access to documents with the protection of personal data are restricting the purpose limitation principle and giving effect to the requirement to have an appropriate legal basis for the data processing. To balance this with the right of access, the requirement to state reasons must be narrowly interpreted. In other words, only a simple notification of the applied legal basis suffices to meet the said criteria.

Furthermore, the privacy of the data subjects will be protected by the provisions laid down in the Transparency Regulation. Situations where processing takes place in the private sector, and where the emphasis should be on self-determination, do not fall within the scope of this thesis.

Balancing requires trying the limits of each right – but only to the extent strictly necessary to realize the other. Being perfectly aware of the grinding of teeth this suggestion will cause among my data protection-loving European colleagues and, at the same time, the freezing cold welcome it will receive from my dear Finnish colleagues, I dare to say that it provides a balanced solution to reconciling the protection of personal data with public access to documents. Four years of GDPR negotiations taught me that the best compromise solutions are those with which no-one is entirely content. That is when the true balance is found. Limits are heavily tested, but no redlines crossed; the essence is preserved.