MASTER's THESIS INTERNATIONAL BUSINESS LAW

»DATA PROTECTION IN (DUTCH) CORPORATIONS«

(including economic aspects and an analysis of current trends)

Author: Helena Uršič

(ANR 193549, u1256171)

Academic supervisor: Vladimir Mirkov, LL.M.

Amsterdam, May 2014

ACKNOWLEDGEMENTS

This master's thesis was written with great assistance of my collegues at EY Amsterdam (Data Privacy Services) and my EY supervisor, Ms Nora Boukadid. Thank you all for being supportive, friendly and inspiring.

I would also like to thank my academic supervisor Vladimir Mirkov from Tilburg University for being highly responsive and supportive. During the writing process his advice was priceless.

Tadej, I am fortunate to have you by my side and I sincerely appreciate the time you spent with the final corrections.

My family in Slovenia – despite living far away from home, you are always close to my heart. Thank you for being there whenever I need you!

"Managed well, the data can be used to unlock new sources of economic value,provide fresh insights into science and hold governments to account. (…). It has great potential for good—as long as consumers, companies and governments make the right choices about when to restrict the flow of data, and when to encourage it".

(The Economist, on the 27th of February, 2010)

1. Index

1. Index 2
2. Introduction 5
3. EU Data protection law in a nutshell 7
3.2. Data protection in the EU – constitutional and historical overview 7
3.3. Current European data protection legislation – main principles and rules 10
3.3.1. Institutions 10
3.3.2. Legal acts 11
3.3.3. Basic definitions 13
3.3.4. Key principles of EU data protection 15
3.3.5. Key rights and duties in the EU data protection law 17
4. New regulation as a paradigm shift 20
4.1. Short summary of the chapter 20
4.2. Reasons for the new regulation 20
4.3. Timeline 21
4.4. Commission's Proposal 21
4.4.1. New definitions 21
4.4.2. Broader jurisdiction 22
4.4.3. Explicit consent 22
4.4.4. Data minimization principle 22
4.4.5. Principle of transparency and accountability 23
4.4.6. Right to be forgotten 23
4.4.7. Right to data portability 23
4.4.8. Profiling 24
4.4.9. Higher penalties 24
4.4.10. Transfer of the data to third countries 24
4.4.11. Lead authority 25
4.4.12. Duty to employ a data privacy officer (DPO) and to carry out privacy impact assessments (PIA) 25
4.4.13. Duty to report personal data breaches 25
4.5. Parliament's amendments *26*
5. The economics of data protection 28
5.1. Short summary of the chapter 28

5.2. Privacy trade off and regulatory implications 28
5.3. Commission's proposal and economic impact assessments 30
5.3.1. European Commission research 31
5.3.2. ICO analysis 31
5.3.3. Deloitte analysis 32
5.3.4. Other views 33
6. Data protection and corporations 35
6.1. Short summary of the chapter 35
6.2. Main privacy challenges in corporations 35
6.3. Changing corporate governance in the world of stronger data protection 37
6.4. Research project: trends in corporate data protection 38
6.4.1. The aim of my research and methodology description 38
6.4.2. Online survey – findings 39
6.4.3. In-depth interviews – findings 42
7. Conclusions 44
8. Bibliography 45
9. Appendix 48

2. Introduction

On the one hand, free flow of information on the internet is life blood of the world economy, making any kind of restrictions in this regard very problematic. On the other hand, free access to data has to be balanced with respect for privacy – not only due to the regulatory requirements but also because privacy proved to be one of the (key) factors for success in business.[1]

Rapid changes in information technology forced legislators all over the world to reconsider their data protection laws. The European Union is currently debating an enormous shift in its regulatory regime by adopting a new regulation which will unify national legislations and introduce a bundle of new (some even controversial) requirements. Even the US is, step by step, moving towards more comprehensive data protection, as testified by the US Online Privacy Bill of Rights.[2]

Global businesses are following this development and trying to align their practice and governance to achieve compliance with the upcoming rules. As a result of this development their corporate governance is changing as well. Since privacy became an issue that is regularly on the agenda, a new type of officer, a chief (data) protection officer, has been included into the exclusive c-suite group in the biggest corporations. Furthermore, separate data privacy departments, not only in top IT but also in other transnational corporations, are being established. The reflection of this privacy evolution in academic contributions shows its importance for the present and, presumably even more, for the future.[3]

European Union, which contrary to the American approach considers data protection a fundamental human right, has taken initiative in the development of privacy rules. By proposing a new regulation on data protection it signals a stricter and unified policy binding for all the companies that do business in the EU. It is therefore not surprising that most of them are highly concerned about the impacts of the new regulatory framework – on their compliance, governance and finance. Privacy advisory services are becoming a new niche market in the EU, attracting law firms and consulting companies alike. Numerous economic analyses have been written and legal opinions presented to help the companies to smoothly transcend to a new regime. At a substantial (compliance) cost, though, it seems that privacy has been finally given a word it deserves in the EU.

While the literature on the legal impacts of the upcoming regulation is extensive, the economic aspects are not that well covered. Even less has been written about the consequences that increased importance

[1] Kuner, C.: European Data Privacy Law and Online Business, Oxford University Press, 2003, p. 1. See also PwC e-privacy study from 2000 showing that in many cases concern for privacy dictates and restricts what consumers are prepared to do on-line.
[2] Moerel, E. M. L. (2014). Big data protection. Tilburg: Tilburg University, p. 30.
[3] Bamberger, K. A. R and Mulligan, D. K.: New Governance, Chief Privacy Officers, and the Corporate Management of Information Privacy in the United States: An Initial Inquiry, Forthcoming in Law and Policy, Vol. 33 (2011).

of privacy has had on corporate governance. My thesis tends to fill this gap and also tens to find out more about the response of the biggest Dutch (*ergo* European) corporations to the upcoming regulation by analyzing their reactions in terms of corporate compliance, governance and financial implications.

Having defined the current state of affairs I set the following hypotheses:

1. There is an accelerated endeavor of European (Dutch) companies to reconsider their privacy strategies.
2. Awareness for privacy among the European (Dutch) companies is raising, however, it is still on low level.
3. Financial impacts are of the companies' biggest concern. Privacy costs are estimated as a part of company's financial statement.
4. Corporate governance has been changing due to the involvement of the data privacy officer. However, the communication between the privacy leader and the board is problematic.

This thesis consists of five parts. To introduce the reader to the extensive data protection law field, the first part draws an overview of privacy regulation as established in the European Union. The second part presents the regulatory reform which is currently running in the EU, summarizing the legislative procedure and proposed novelties. The third part explains basic economic theories about data privacy and lists the opinions regarding economic impacts of the proposed regulation. The fourth part presents some of the privacy challenges that companies face and their impact on corporate governance. With intention to make a sound contribution to the current academic debate, it critically assess the key findings from the online survey and in-depth interviews. The fifth part concludes.

3. EU Data protection law in a nutshell

3.1. Short summary of the chapter

This chapter describes the development of data protection law in the EU by listing the main legislative acts and giving reasons for their implementation. The evolution of European data protection law shows great concern for privacy as a fundamental human right, although this political standpoit has been occasionally confronted with theories arguing that data protection law should pay more attention to the real needs of economy and consumers. The rest of the chapter focuses on institutions, definitions and rules which compose the corpus of data protection law in the EU.

3.2. Data protection in the EU – constitutional and historical overview

Few years after *The United Nations Universal Declaration of Human Rights* had been adopted,[4] *the Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR)* was introduced as the next international document that laid down the right to protection on private and family life. Article 8 of the ECHR sets the basis for the data protection in Europe: *"Everyone has the right to respect for his private and family life, his home and his correspondence. 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 or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."* The European Court of Human Rights (ECtHR) established few years after the adoption of the ECHR, has been often requested to apply the vague definition on complex cases issuing an extensive collection of decisions on data protection. In 1960s when information technology started to penetrate everyday of Europeans, the European Council realized it was time for a new, more specific legal instrument, aligned with the IT developments. As a result of it, *The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (Convention 108) was adopted in 1981, being the first and, until today, the only international instrument in data protection field. The main aim of the convention is to protect an individual against abuses which may accompany the collection and processing of personal data, and to seek to regulate the trans boarder flow of personal data.[5] Convention 108 is open for accession to non-member states of the Council of Europe, including non-European countries. With the exception of San Marino and Turkey all the

[4] Universal Declaration of Human Rights, Article 12: *''No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.''*

[5] Handbook on European data protection law, Publications Office of the European Union, Luxembourg, 2014, p.16.

members of the Council have ratified the Convention. Outside Europe, Uruguay and Morocco were the last two countries that decided to adopt the convention.[6]

The European Union was established as an economic union of the post war Europe. Therefore it does not come as a surprise that legal instruments aimed to stronger economic integration are of its main concern. As free movement of goods, capital, services and people within the internal market required free flow of data, it soon became urgent to reach a more detailed agreement on a uniform level of data protection.[7] Although the basis protection of data in Europe had already been set by Convection 108, the *Directive 95/46/EC 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* (hereafter General Directive) adopted in 1995 importantly improved the legal environment by increasing the level of protection and giving more substance to vague Convention principle. As some member states already had their national laws on data protection by that time, one of the purposes of the Directive was also harmonization.[8] To achieve the goal defined by the European legislator, a directive by its nature does not require a complete harmonization (i.e. unification). So if the level of legal protection in a certain state is higher than the one provided in the directive, it can be maintained. Thus, differences among the EU member states originating in their various national laws still exist regardless of the Directive's clearer definitions.[9]

When Amsterdam Treaty in 1999 included judicial and police cooperation in the scope of EU law, a logic consequence was adoption of separate legal documents such as *Framework decision 2008/977/JHA* which separetly regulated protection of data in the area of freedom, security and justice. Moreover, rapid improvements in IT triggered the adoption of additional legal acts related to data protection. The two main instruments are the *Directive 202/58/EC on the processing of personal data and the protection of privacy in the electronic communications sector* (hereafter E-privacy directive) and the *Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks* (hereafter Retention Directive). The latter has been recently found invalid by the Court of Justice of the EU (CJEU) due to the fact the amount of retained data as required by the directive was excessive and hence not proportionate.[10]

---

[6] Information available at: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CM=&DF=&CL=ENG.
[7] Handbook on European data protection law, p. 18.
[8] Ibidem.
[9] Data Privacy Index, from an information law online platform Data Guidance, calculates a risk score for each country based on the severity of its data protection regime – a high risk means there is big chance of breaking the rules and being punished. Additional information available at: http://www.information-age.com/technology/security/1687058/uk-ranks-21st-in-europe-for-privacy-protection, www.dataguidance.com.
[10] Court of Justice of the EU, Press Release No 54/14, Luxembourg, available at: http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf.

Simultaneously with the adoption of Lisbon Treaty, the European Union also introduced its own human rights document, the *Charter of Fundamental Rights of the European Union* (hereafter Charter). Charter filled the gap in the EU primary law which lacked a specific provision on data protection. It can be argued, though, that European Convention, which the CJEU considered a source of the EU law and its equivalent part, was sufficient in that regard.[11] For the reason of legal certainty, however, the explicit provision in Charter is a desired improvement. With Article 8 paragraph 1 of the Charter, the right to data protection was incorporated in the primary legislation as one of the principles inherent to the Union objectives. Paragraph 2 specifies that "*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*.'' In addition Charter guarantees to "*Everyone / … / the right of access to data which has been collected concerning him or her, and the right to have it rectified*." Paragraph 3 of the same article ensures that compliance with the rules shall be subject to control by an independent body.

Charter differentiates between the right to respect for one's private and family life and the right to the protection of personal data. The right to respect one's private and family life mirrors an individualistic component: this power basically consists in preventing others from interfering with one's private and family life. Conversely, data protection sets out rules on the mechanisms to process data and empowers one to take steps – i.e., it is a dynamic kind of protection, which follows a data in all its movements. Thus, data protection as known today is actually the endpoint of a long evolutionary process in the EU leading from the right to be left alone to the right to keep control over one's information.[12]

The development described above, which came out on the top with the adoption of the Charter, shows an increased awareness of the importance of data protection in the EU. This has been recently reflected in the secondary legislation, most evidently in the proposal for a new regulation on data protection.[13] The proposed regulation will replace the current Directive on data protection and unify the legal regime across the EU.

However, as Rodota observes, it is increasingly difficult to respect the general assumption that data protection is a fundamental human right, because internal and international security requirements, market interests and the re-organisation of the public administration are heading towards the diminution of relevant safeguards, or pushing essential guarantees towards disappearance.[14] According

[11] Craig, P. and De Burca, G: EU Law: Text, Cases, and Materials, Oxford University Press, p. 362.
[12] Kuner, C,: European Data Protection Law, Corporate Compliance and Regulation, Second Edition, Oxford University Press, 2003, p. 3. See also: Kokott, J. and Sobotta, C: The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR, International Data Privacy Law, Vol. 3, No. 4 (2013).
[13] 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), Brussels, 25.1.2012, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:EN:PDF.
[14] S., Rodota in: Reinventing Data Protection?, ed. Serge Gutwirth et al., Springer, 2009, p. 77.

to Prof. Bergkamp, this is not surprising, as European data protection law exaggerated with data subject-friendly provisions and contributed to an unstimulating business environment.[15] The debate on the future of data protection in the EU Parliament and Council is expected to continue over the next year(s). During the discussions the EU legislator and market players will have to face a difficult task - finding the right balance between respect for privacy and business interests.

3.3. Current European data protection legislation – main principles and rules

3.3.1. Institutions

European data protection law is an extensive legal field which consists of a variety of legal acts, informal documents and case law produced by numerous European and national institutions. Due to the limited scope of the thesis only key characteristics indispensable for understanding of the thesis subject will be presented.

European Commission, taking responsibility over the majority of legislative initiatives in the EU, is often described as the engine of legislative changes. Its predominant role can be explained by the fact that it is the only European institution that has sufficient financial resources and competent employees to actively work on legislative proposals. Not surprisingly, also the proposal for the EU data protection regulation was written by the Commission's Justice department and, after months of public discussions and shared opinions, was passed to the Parliament.[16]

Contrary to the Commission, **the European Council** is purely political and not an executive organ. Council may be involved in legal issues relating to data protection in two ways; first, in the course of debate about EU legislative initiatives by providing a forum through which member states can make decisions and exercise their political influence and second, through Article 33 Committee, which is a consultative body on data protection questions for member states set in the General directive on data protection.[17]

European parliament is the institution that is gaining more and more power in the EU. From the consultative body it evolved into one of the key players in the European legislative process. When dealing with privacy issues, the following committees play a role: Committee on Internal Market and Consumer Protection, Committee on Legal Affairs and Committee on Civil Liberties, Justice and Home

[15] Bergkamp, L: The privacy fallacy: adverse effects of Europe's data protection policy in an information-driven economy, Computer Law & Security Report, Vol. 18, no. 1, 2002, p. 37.
[16] See more on p. 21.
[17] Kuner, C.: European Data Protection Law, Corporate Compliance and Regulation, Second Edition, Oxford University Press, 2007, p. 6.

Affairs (LIBE).[18] The great importance of Parliament and its equal position towards Council is evident from the process of adoption of the new regulation, in which the Parliament's vote was decisive to pass the proposal to the next level in the legislative procedure.

The European Court of Justice is assigned the task of interpreting EU law. There are two ways in which the Court reviews the legislation. Firstly, it is possible that national courts request for preliminary ruling, i.e. an elaborated interpretation of the rules in the EU legislation. Secondly, a small group of specifically defined bodies may demand from the Court to check whether a certain legal act is invalid.[19]

European data protection supervisor's main responsibility is to monitor the processing of personal data by European institutions and bodies and to control compliance with data protection rules. However, its role expands over purely supervisory tasks – it also has a substantial influence on policy making and may intervene before the CJEU in cases involving data protection.[20]

Finally, the **Article 29 Working Party** is an independent, advisory body that was established by the General Directive. It meets several times in a year to discuss the relevant privacy issues and consists of the representatives of members states' data protection authorities. Working Party's decisions often fill the gaps that appear due to unclear legislative provisions. Thus, they are the ones that (besides Court's decisions) most strongly influence the development of data protection law in the EU.[21]

3.3.2. Legal acts

As mentioned above, the European data protection law slowly evolved throughout years as a necessary consequence of the establishment of the EU internal market and human rights concerns. Starting in the 1980s, the EU adopted a range of secondary instruments aimed to regulate processing of data, although its primary law still kept silent about privacy at that time. EU Charter and Lisbon Treaty, both adopted in 2009, filled this gap by proclaiming privacy and data protection a fundamental right.[22]

Previous subchapter analyzed primary law that set up a basis for data protection, thus, the following will only focus on secondary legislation.

General directive and E-privacy Directive are two instruments that give most substance to EU data protection law. General Directive, seen as the basic legal act or *lex generalis*, has two main purposes: to

[18] See more on p. 21.
[19] Kuner, C.: European Data Protection Law, Corporate Compliance and Regulation, Second Edition, Oxford University Press, 2007, p. 7.
[20] Ibidem.
[21] Idem, p. 9.
[22] Bergkamp, L: The privacy fallacy: adverse effects of Europe's data protection policy in an information-driven economy, Computer Law & Security Report, Vol. 18, No. 1 (2002), p. 32.

allow for the free flow of data within Europe, in order to prevent Member States from blocking inter-EU data flows on data protection grounds and to achieve a minimum level of data protection throughout all Member States. Its content is often expressed in six underlying principles: legitimacy, purpose limitation, transparency, proportionality, security and control. The Directive contains a fundamental prohibition from transferring data to third countries with inadequate level of data protection which is of great relevance for multinational companies.[23]

Contrary to General Directive, the scope of E-Privacy Directive is much more limited as it only regulates privacy of telecommunications, emails, internet and other similar devices. The directive, which was adopted in 2002, distinguishes three categories of data: a) data that constitutes the content of the messages, b) data necessary for establishing and maintaining the communication such as information about communication partners, time and duration of the communication (traffic data), c) data related to the location of the communication device (location data). [24]

Traffic data can be used by the service provider only for billing and technically providing the service. With the consent of the data subject, however, these data may be disclosed also to other controllers offering added value services (e.g. giving information about the closest metro station or on weather forecast). Any other access to data is prohibited, unless it fulfills the requirements for justified interference with the right to data protection.[25]

The amendments of the directive in 2009 prohibited sending emails for direct marketing purposes without obtaining a prior consent. Since then, member states have been required to provide judicial remedies against violations of the ban on unsolicited communications. Also, setting of cookies (a small file or part of a file stored on a World Wide Web user's computer, created and subsequently read by a Web site server, and containing personal information - as a user identification code, customized preferences, or a record of pages visited)[26] is regulated more strictly.[27]

Before March 2014, Data Retention Directive was a constituent part of EU data protection law. According to this directive, service providers were obliged to keep traffic data available for a period between 6 and 24 months. The rationale behind the directive was to help fighting serious crime by giving the authorities

[23] Kuner, C.: European Data Protection Law, Corporate Compliance and Regulation, Second Edition, Oxford University Press, 2007, p. 20.
[24] Idem, p. 24.
[25] Ibidem.
[26] Merriem-Webster Online Dictionary, available at: http://www.merriam-webster.com/dictionary/cookie.
[27] Handbook on European data protection law, Publications Office of the European Union, Luxembourg, 2014, p.16.

access to stored private data. However, the CJEU has recently declared the directive invalid since its extensive retention period requirement violated the principle of proportionality.[28]

Ultimately, an important aspect of EU data protection law represent CJEU case law and Article 26 Working Party's opinions, however, due to a word limit they will not be examined in detail.

3.3.3. Basic definitions

3.3.3.1. Personal data

When writing about EU data protection it is critical to define the object of protection, namely, personal data. According to Article 2 of the General Directive the definition of 'personal data' includes any information relating to an identified or identifiable natural person (which is called 'data subject'). An identifiable person is 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. European Court of Human Rights has not yet (directly) answered the question whether data attached to a specific legal entity may also be considered personal. In the EU Member states are free to tackle the question in their own national legislations.[29] A special regard should be paid to sensitive data, e.g. data that relates to a person's racial or ethnic origin, his political or religious opinion and his health and sexual life. The General Directive makes clear that any processing of such data shall be prohibited unless one of the few exceptions listed in Article 8 applies.

In last few years anonymization and pseudonymisation of data are two new concepts that have been used often when dealing with big amount of personal data. If personal data are anonymized, they are considered disconnected from the source and can therefore be freely processed; if they are only pseudonymised (I.e. by using numbers instead of names), however, they may still enable identification of the initial source and their processing should be restricted.

3.3.3.2. Users of personal data

In principle, a user of personal data can be a legal person including its affiliates, while departments or other organizational sections of a company are excluded from the definition. Most generally, users are split in two groups – controllers and processors. 'Controller' is the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and

[28] Recently found invalid. Judgment in Joined Cases C-293/12 joined with Seitlinger & Others, Case C-594/12, judgement from the 8th of April 2014.
[29] Kuner, C.: European Data Protection Law, Corporate Compliance and Regulation, Second Edition, Oxford University Press, 2007, p. 91.

means of the processing of personal data. 'Processor' is a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.[30]

Due to developments in information technology the line between controller and processor is disappearing. Nowadays most of the companies are active in both roles – e.g. they store data of their clients as a controller of data and use them for marketing purposes as a processor.[31]

3.3.3.3. Processing of data

Data may be processed manually or automatically. Processing includes all forms of using data – collection, recording, organization, storage, adaptation, retrieval, consultation, use, disclosure, blocking, erasure, destruction, combination or alignment etc. Any of the forms requires a legal basis that allows for processing of data. For instance, to store its employees' data a company has to possess a valid employment contract. However, if the department, responsible for the issue passes the employees' data to tax authorities, the processing exceeds the purpose limitation from the contract and a new, explicit legal basis is required.[32]

3.3.3.4. Consent

The legal basis for processing the data is a consent, which has to be free, informed, specific and unambiguously given. A consent is free when all the civil law assumptions are fulfilled: following the German theory these assumptions are legal capacity, appropriate form, defined and possible object, no fraud and a *causa*. The data subject needs to be fully informed about the consequences of his consent and may change or withdraw it anytime. This means, *vice versa,* that before any additional processing of the subject's data, a new consent must be obtained.[33] The amendment of the E-Privacy Directive in 2009 set stricter conditions for consent in cases of storing information or gaining access to information stored in the terminal equipment of a subscriber or user. Article 29 Working Party realized the lack of guidance on how this exception should be treated and published an opinion which clarified that proper compliance may be achieved by granting internet users option to opt-out cookies every time they access an unknown website.[34]

---

[30] Handbook on European data protection law, Publications Office of the European Union, Luxembourg, 2014, p.51-52.
[31] Kuner, C.: European Data Protection Law, Corporate Compliance and Regulation, Second Edition, Oxford University Press, 2007, p. 72.
[32] Handbook on European data protection law, Publications Office of the European Union, Luxembourg, 2014, p.47-48.
[33] Idem, pp. 56-61.
[34] Kosta, E.: Consent in European Data Protection Law, Martinus Nijhoff, 2013, p. 307.

3.3.3.5. Purpose limitation

Article 6 (1)(b) of the General Directive provides that personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with this purposes. In practice this means that companies should always keep in mind what the purpose of processing is when collecting or processing personal data and should communicate such purpose to their customers and employees. This make good business sense but it is also necessary to ensure that the legal grounds for the particular data processing are later not found to be invalid.[35]

3.3.3.6. Data transfer

There is no definition of data transfer in the EU legislation, however, the CJEU suggested in *Lindquist* decision that a data transfer should be an active act which involves sending of data, and not just making it passively accessible (this also applies for sharing the data on the internet).[36] Nowadays data transfers outside Europe are of special attention, however, they are only allowed as long as the third country guarantees sufficient level of protection.[37]

3.3.4. *Key principles of EU data protection*

Despite not being explicitly mentioned in the secondary legislation, it is clear that right to data protection is not absolute and needs to be balanced with other legal principles. Article 52 (1) of the Charter defines the **proportionality** test which is used in cases of collision.

The tension between the right to data protection and freedom of expression is the one that attracts most attention. In article 9 of the General Directive the legislator provided an exception for the cases of collision between freedom of journalistic, artistic or literary expression and data privacy. CJEU thoroughly explained the scope of journalistic expression in *Satamedia* where it held that journalism has to be interpreted in a broad sense.[38] Another striking collision can occur between data privacy and property rights. In *Promusicae v. Telefonica de Espana* the company tried to get access to people who were using their program and exploiting copyrights. At this point its right to property collided with privacy of internet user guaranteed by the telephone provider.[39]

---

[35] Kuner, C.: European Data Protection Law, Corporate Compliance and Regulation, Second Edition, Oxford University Press, 2007, p. 100.
[36] Case C-101/01 Lindqvist [2003] ECR I-12971.
[37] Kuner, C.: European Data Protection Law, Corporate Compliance and Regulation, Second Edition, Oxford University Press, 2007, p. 79.
[38] Case C-73/07 Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy [2008] ECR I-9831.
[39] C-275/06, Promusicae [2008] ECR I-271.

Apart from proportionality, the rest of principles relevant for data protection law is listed in Article 6 of the General Directive. Among them, the most fundamental one is the **principle of lawful processing**. Its main purpose is to make sure that any interference with the right to respect private life is properly balanced. As article 6(a) does not elaborate it any further, additional guidance may be seek in the Article 52 of the EU Charter. Two conditions derived from the principle of proportionality signal that interference complies with the requirement of lawful processing. Firstly, processing must be provided for by law and must respect the essence of rights and freedoms. Secondly, processing is only allowed if it is necessary and if it meets the objectives of general interest recognized by the Union or the need to protect the rights and freedoms of others (the so-called proportionality test).[40]

The second key principle is the **principle of purpose specification and limitation**. Article 6 (b) reads: *"… personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards."* In 2013, Article 29 Working Party issued an opinion in which it held that the purpose must be specified and made manifest by the controller *before* the processing of data starts.[41]

Principle of data quality relates to relevancy, accuracy and retention period of data processed. To comply with the relevancy requirement it is necessary to omit processing of the irrelevant data. This can be done by using pseudonymization techniques (discussed above) which partly conceal data. Data accuracy means that data has to reflect the true condition and be, if necessary, updated. According to article 6 of the Directive every reasonable step must be taken to ensure that data which are inaccurate or incomplete are erased or rectified. Finally, data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.[42]

Two additional principles can be derived from the European Directive and other international agreements. First, the **fair processing principle** tends to ensure transparency of data processing, enabling data subjects to stay aware of the procedures and establishing trust. Second, **accountability,** which is also emphasized in the OECD 2013 Guidelines, is aimed to achieve active compliance of the controller.[43]

---

[40] Handbook on European data protection law, Publications Office of the European Union, Luxembourg, 2014, p.65-69.
[41] Article 29 Working Part Opinion 03/2013 on purpose limitation, 2013. Available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.
[42] Handbook on European data protection law, Publications Office of the European Union, Luxembourg, 2014, pp. 72-75.
[43] Idem, pp. 76-78.

3.3.5. Key rights and duties in the EU data protection law

The following chapter embraces the main rules of the EU data protection law as currently enforced. Due to the limited scope of my thesis, it only focuses on the General Directive as *lex generalis* in the field of data protection law.

As mentioned above, the EU data protection law distinguishes two types of data – **sensitive and non-sensitive data**. The latter cannot be processed unless an exception, such an explicit consent, vital interest of data subject, a legitimate interest of others or a public interest, applies. In opposite, non-sensitive data can be processed freely whenever there is a valid consent (which is not necessarily explicit) or a contractual relationship.[44]

Every processing has to be **secure and confidential**. In this purpose the controllers and processors need to implement appropriate technical and organizational measures (installing appropriate hardware and software as well as informing the employees, carefully storing documentation, organizing trainings, employing a DPO). In case of a breach, they are obliged to notify it to victims and authorities. Similarly to the processing also the relationship between the processor and controller requires a sufficient level of confidentiality.[45]

The most fundamental **right** of a data subject is **to access the information** as to whether or not the data are being processed. This information must be given in an intelligible form and needs to include: purposes of processing, the categories of data concerned, the data undergoing processing, the recipients or categories of recipients to whom the data are disclosed, any available information about the source and logic involved in any automatic processing of data.[46] Not only is the data subject entitled to receive information about possible processing of his data, he is also entitled to request the rectification, erasure or blocking of data in case that such processing violates the General Directive's objectives. If a data subject requests rectification, the controller may demand a proof of the alleged inaccuracy. In such a case, the burden of proof placed on the data subject should not be so high as to preclude him/her from having the data rectified. Of course a data subject is not always entitled to get access to data or to claim its erasure. If another overriding legal interests exist, his request may be declined. Overriding public interests may involve public interests such as national security, public security and prosecuting of criminal offence as well as private interests if they are more compelling than data protection interests. As a part of the right to obtain information or to demand erasure, the controller has the duty to notify the third parties, to which the data was transferred, about the data subject's request, unless it would

[44] Idem, pp. 84-93.
[45] Idem, pp. 94-98.
[46] Idem, p.112.

involve disproportionate effort.[47] In addition, data subject has the right to object processing of his data whenever they could be used in direct marketing purposes, be subject to automated decision (such as credit scoring) or when they compel with some specific interests of the data subject.[48]

The General Directive requires an **independent authority** to be established in every member state with the task to actively supervise and protect data subjects' rights. In order to ensure proper independence, member states have to provide an appropriate organizational structure in which the authorities do not face any kind of the State's oversight.[49] There are substantial differences among the European member states as regards their institutional structure in data protection law. Some of the states assigned the supervisory tasks to institutions that have strong powers including enforcement of the decisions, while in other countries only an ombudsman, an institution with no concrete powers, is designated as data protection authority.[50]

Considering IT developments and public demands, the directive provides for some **remedies and sanctions**. Firstly, if a data subject addresses a controller with a request related to his data protection infringement(s), he is entitled to receive a response without excessive delay. In addition, the data subject must be able to exercise his right without excessive expense. Secondly, in case that controller does not respond to the requests or does not respond adequately, the data subject has the right to lodge a claim with supervisory authority. If the data subject considers the decision issued by the authority incorrect, the final step is to lodge a claim with court. As a part of the judicial proceedings the national court may also request a preliminary ruling on interpretation of European law.[51]

An important aspect in the EU data protection law is the question of **applicable law and jurisdiction**. General Directive defines two (main) legal bases for the application of EU data protection law in EU member states.[52] Firstly, as Article 4(1)a foresees, EU law applies whenever data controller is established in the EU and process the data in the context of the activities of establishment. Secondly, it also applies when a non-EU data controller uses its equipment in a Member State (without being established on the European territory). Apparently, the second rule tries to prevent the evasion of data controllers of their legal responsibilities through relocation of their establishments outside the EU, while still using technical means located in the EU to processes data in a way inadequate for the European standards. Due to a

[47] Idem, pp. 114-116.
[48] Idem, pp. 117-118.
[49] Case C-518/07, Commission and EDPS v Germany, judgment form the 28th March 2010.
[50] Kuner, C.: European Data Protection Law, Corporate Compliance and Regulation, Second Edition, Oxford University Press, 2007, p. 14.
[51] Handbook on European data protection law, Publications Office of the European Union, Luxembourg, 2014, p.124-132.
[52] ??

possibility of a very broad interpretation of certain expressions, the provision has created a lot of controversy (especially among companies involved in electronic commerce).[53]

Finally, one of the most striking dilemmas in data protection law, especially for the international companies, is the issue of **international transfers**. In the era of globalization, data is being daily transferred all over the world. It is, however, clear that not all the countries provide an adequate level of data protection. Article 25(1) of the General Directive allows for the transfer of personal data which are undergoing processing or are intended for processing only if the third country in question ensures an adequate level of protection. It is up to the Commission and Member States' decision which countries they consider adequate. So far, the Commission has issued 13 adequacy decisions confirming adequate status of the following countries: Andorra, Argentina, Australia, Canada, Switzerland, Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, US (under safe harbor)[54], New Zealand ad Uruguay.[55]

In addition to adequacy decisions, Article 26 provides two other legal bases for international transfers. The first one are standard contractual clauses that may be found in two different forms – as standardized set of clauses approved by the Commission or as *ad hoc* contracts that are individually approved by a national DPA. The second base is a collection of exceptions such as consent of data subject or public interest which occasionally legitimate data transfers.[56]

Despite not being explicitly mentioned in the text of the directive, binding corporate rules are one of the most widely used ways how to achieve compliance with data protection laws. BCRs are set of legally-binding data processing rules adopted by a company which grant rights to data subjects. As they resemble contractual clauses they could be listed within the second group of legal bases for international transfers mentioned above. BCRs are an innovative toolkit for protecting the privacy of data subjects while facilitating international global transfers of personal data to corporate groups in countries without sufficient data protection legislation.[57]

---

[53] Kuner, C.: European Data Protection Law, Corporate Compliance and Regulation, Second Edition, Oxford University Press, 2007, p. 112.

[54] The US Safe Harbor is an agreement between the European Commission and the United States Department of Commerce that enables organizations to join a Safe Harbor List to demonstrate their compliance with the European Union Data Protection Directive. This allows the transfer of personal data to the US in circumstances where the transfer would otherwise not meet the European adequacy test for privacy protection. More information available at: http://www.galexia.com/public/research/assets/safe_harbor_fact_or_fiction_2008/safe_harbor_fact_or_fiction-Introduc.html.

[55] Information available at the European Commission's official website: http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm.

[56] Kuner, C.: European Data Protection Law, Corporate Compliance and Regulation, Second Edition, Oxford University Press, 2007, p. 192.

[57] Idem, p. 219.

4. New regulation as a paradigm shift

4.1. Short summary of the chapter

The following chapter introduces the new regulation as proposed by the European Commission and Parliament. Also, it shortly discusses reasons that led to the proposal and describes the stages in the legislative procedure. The major part of the chapter focuses on the novelties in the draft regulation which are attracting most public attention and are expected to have the greatest impact on economy.

4.2. Reasons for the new regulation

As mentioned above, The Lisbon Treaty, signed on 13 December 2007, brought fresh air not only to the future of the European Union in general, but also to the relevance of the right to the protection of personal data. Firstly, the amended Treaty on the Functioning of the EU now includes a provision on the protection of personal data. Secondly, in the Article 8 of the Charter of fundamental rights of the EU, the EU compilation of human rights, the right for data protection is recognized as one of the fundamental principles in the EU.[58]

In the digital age, the collection and storage of personal information are essential. Data is used by all businesses – from insurance firms and banks to social media providers and search engines. In a globalized world, the transfer of data to third countries has become an important factor of everyday life. As there are no borders in the online world, data may be easily sent from Berlin to be processed in Boston and stored in Bangalore.[59]

Both, emphasizing the right to have your data protected with the Lisbon Treaty and rapid development of IT, signaled the necessity to strengthen the European data protection law.[60]

Another important (though a much more pragmatic) reason for a reform is the fact that vague language of the Directive resulted in excessive fragmentation and legal uncertainty across the European Union. To avoid different standards, the adoption of a new legal document that would unify the European national legislations seemed to be the way to go.[61]

---

[58] Cuipers, C, Purtova, N, Kotsa, E.: Data Protection Reform and the Internet: the draft Data Protection Regulation, Tilburg Law School Legal Studies Research Paper Series No. 03/2014, p. 4.
[59] Commission's Press Release on the Data Protection Day 2014: Vice-President Reding calls for a new data protection compact for Europe, Brussels, 28. 1. 2014.
[60] Ibidem.
[61] Kuner, C.: The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law , Bloomberg BNA Privacy and Security Law Report, 6 February 2012, p.4.

4.3. Timeline

On the 4th of November 2010, the Commission set out a strategy to strengthen EU data protection rules. The goals were to protect individuals' data in all policy areas, including law enforcement, while reducing excessive regulation for businesses and guaranteeing the free circulation of data within the EU. The Commission invited reactions to its ideas and carried out a separate public consultation to revise the General Directive.[62]

On the 25th of January 2012 the Commission published its proposal of the EU Regulation on Data Protection and sent it to the European Parliament and Council in further legislative procedure. In January 2013 the Parliament's Internal Market Committee, Industry Committee and Employment Committee voted on the opinion about the Commission's proposal. Legal Affairs Committee voted as the last one in March 2013. The amendments of all the four committees' were handed over to the Civil Liberties' Committee (LIBE Committee) which was in charge of preparing the final version of the proposal for the voting in the European Parliament. On the 12th of March the LIBE's version of proposal was adopted by 621 MPs votes. This positive reaction is a significant achievement because it enables the newly elected EP to continue the work without repeating the whole procedure. It is expected that the negotiations between the Parliament and the Council, which are the next step in the European ordinary legislative procedure, will be held in the second part of 2014 and that the final agreement will be reached before the end of 2014.[63]

4.4. Commission's Proposal

Prof. Kuner considers the proposed Regulation a *''Kopernican movement''* in EU law and predicts that it will have a massive impact on European companies.[64] Some of the features from the Commission's proposal which will, if adopted, significantly transform the European Union data protection regulatory framework, are described below.

4.4.1. New definitions

The Commission's proposal gives new meaning or amends some of the key definitions from the General Directive. For example, in Article 9(1) it expands the definition of sensitive data to include genetic data and data concerning *"criminal convictions or related security measures".* The change is crucial, since processing of such data will be possible only under strict conditions. Online identifiers (e.g. IP address)

[62] IP/10/1462, Brussels, 4 November 2010.
[63] Hunton&Williams, EU Data Protection Regulation Tracker, available at: http://www.huntonregulationtracker.com/legislativescrutiny/.
[64] Kuner, C.: The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law , Bloomberg BNA Privacy and Security Law Report (2012), p.4.

are also considered sensitive data as long as they may relate to an identified or identifiable person. The proposal includes a number of new(ly defined) terms e.g. personal data breach, biometric data, data concerning health, main establishment, representative, enterprise, child, binding corporate rules, supervisory authority and group of undertakings.[65]

4.4.2. Broader jurisdiction

The Commission's proposal widens the scope of jurisdiction over companies based out of Europe if the data subject related to the data processed *"offers goods or services in the EU''* or *''monitors such data subjects''.* The academics have already raised the question what exactly ''offering goods or services'' means. According to Kuner it is regrettable that the Commission does not have the power to issue delegated acts to explain the scope of this provision. However, he claims, the consequences of the change are not too difficult to predict – the new provision will definitely bring more non EU-based companies offering services over the Internet within the reach of EU law.[66] According to the Commission's proposal the Regulation applies also *"when non-EU-based controllers process data of data subjects residing in the Union, when such processing relates to the offering of goods or services to such data subjects or to the monitoring of their behavior"*. As stressed in the recitals 19 and 20 this provision is intended to prevent depriving data subjects of the Regulations protection merely because a controller is not established in the Union.[67]

4.4.3. Explicit consent

The draft regulation suggests a tighter definition, namely an explicit consent which will presumably leave less space for circumventions of the rules and will put more burden on controllers. Article 4(8) presupposes that such consent will be obtained either by a statement or by a clear affirmative action of a data subject. If there is, however, imbalance between the position of data subject and controller, a consent cannot be a legitimate basis for the processing of data. The recital 37 clarifies that this applies specifically for the relation between employee and his employer.[68]

4.4.4. Data minimization principle

Data minimization principle demands from companies to limit data they store to the lowest amount possible. Article 5(c) of the Commission's proposal provides a more explicit expression of the "data

[65] Idem, p. 8.
[66] Idem, p.6.
[67] Idem, p. 9.
[68] Idem, p. 10.

minimization" principle than is currently contained in the General Directive and requires companies to limit the data they collect more strictly.[69]

4.4.5. Principle of transparency and accountability

By introducing the principles of transparency and accountability the European Commission confirms its efforts to raise the European standards of data protection for individuals. Article 22 (3) stipulates that compliance measures should be independently verified, though the use of *"independent internal or external auditors"*, however, this is only required when *"proportionate"*. The concept of accountability seems to include the measures listed in Article 22(2) such as keeping documentation of data processing, implementing data security requirements, performing data protection impact assessments and designating a DPO.[70]

4.4.6. Right to be forgotten

When it comes to the right to be forgotten, its reversed side, the duty of the controller to inform third parties about the data subject's request to erase data, is of a special importance. This duty, which is stipulated in Article 17 of the draft regulation, is limited to what is possible and does not involve a disproportionate effort.[71] As Dr. Van Hoboken observes, the added value of the updated provision for data subjects that want to see their data deleted is relatively minor, though it is the improvement that has received the greatest attention in academia as well as from general public.[72]

4.4.7. Right to data portability

The right to data portability has two elements. Firstly, under Article 18(1) of the draft Regulation, individuals whose personal data are processed electronically and in a *"structured and commonly used format"* are given the right to obtain a copy of that data for further use. Secondly, Article 18(2) provides for the right for individuals to transmit their personal data from one provider to another. Given that the majority of personal data are processed electronically, Article 18 seems to have widespread applicability and the potential to offer significant benefits to individuals.[73] Kuner sees the main advantage of this new

---

[69] Idem, p. 9.
[70] Idem, p. 13.
[71] Idem, p. 11.
[72] Van Hoboken, J.: The Proposed Right to be Forgotten Seen from the Perspective of Our Right to Remember Freedom of Expression Safeguards in a Converging Information Environment, Prepared for the European Commission, Amsterdam, May 2013.
[73] Bapat, A: The new right to data portability , Privacy, Data Protection Journals, Volume 3, Issue 3, available at: http://www.hunton.com/files/Publication/c924a1bc-b27e-420f-ada4-6635d6c9ab4a/Presentation/PublicationAttachment/d4ce9cda-8229-4778-bdf3-73eb9a9c3f70/The_new_right_to_data_portability_Bapat.pdf.

right in enabling the individuals to change online services more easily by granting them the right to obtain a copy of their data from their (former) service provider.[74]

4.4.8. Profiling

Article 20 of the proposal defines profiling as *"a measure that produces legal effects concerning a person based on automatic processing intended to evaluate certain personal aspects"*. As such, profiling covers many routine data processing operations that may also benefit the individuals concerned, such as, for example, routine operations to evaluate the performance of employees. Kuner cautions that severe restrictions on the way that such profiling may be conducted will cause many companies to reevaluate their data processing practices, particularly in the online sphere.[75]

4.4.9. Higher penalties

Under the General Directive the amount of administrative sanctions was left to implementation by the member states and as result of it the numbers varied widely. The proposed regulation plans to transform the old system which enables to set the fines on a (too) low level by substantially increasing the sanctions over what was previously possible and unifying their rates across the EU. These sanctions are imposed mandatorily for any intentional or negligent violation of certain provisions of the Proposed Regulation, and are divided into three categories, amounting up to 2% of a company's annual worldwide turnover.[76] As Kuner ascertains, it is the first time in the history of data protection law that the fines are high enough to be able to draw attention of CEOs and general counsels in European companies.[77]

4.4.10. Transfer of the data to third countries

Article 40 abandons the presumption under the General Directive that personal data may not be transferred absent an *"adequate level of protection"* in the recipient country, and instead provides three different systems of safeguards that a company may use to legitimize a transfer. The first system enables transferring on the basis of Commission's adequacy decision, the second on the basis of appropriate safeguards (such as European Data Protection Seal, standard data protection clauses and contractual clauses) and the third on the basis of binding corporate rules. It is the first time in history that BCRs have been explicitly mentioned in a legal text, which undeniably shows their importance for the EU. Another

[74] Kuner, C.: The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law , Bloomberg BNA Privacy and Security Law Report, 2012, p.11.
[75] Idem, p. 11.
[76] Idem, p. 21
[77] Ibidem.

important development is that DPAs will no longer require authorization of transfers using the EU standard contractual clauses which will be, as Kuner notices, a great advantage to data controllers.[78]

4.4.11. Lead authority

Article 51 provides that a company (acting as a controller or processor) established in more than one Member State, is required to approach the authority in the state of its main establishment, the so-called leading authority. Thus, instead of dealing with 28 different data protection authorities, the company has only one respondent which importantly simplifies its privacy procedures. If there is a lawsuit brought against a company, this should be done in the state of the lead authority.

4.4.12. Duty to employ a data privacy officer (DPO) and to carry out privacy impact assessments (PIA)

With the last version of the Commission's proposal the duty to employ a DPO applies to the companies with more than 250 employees. To comply with this rule it suffices to have an officer in the company's headquarter and grant him rights to cover subsidies as well.[79] Furthermore, the proposal introduces the obligation of controllers and processors to carry out data protection impact assessments. This duty, however, only applies in certain circumstances, some of which are clear (e.g. when processing biometric data), but others of which are vague (e.g. when data processing operations *"are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes*"). The European Commission estimates the cost of an impact assessment between 14.000 and 149.000 EUR. This significant amount would be a large financial burden for small and medium-sized enterprises, although it could be argued that Recital 71, stating that only newly established and large scale filing systems require a PIA, indicates the Commission's purpose to exclude them from the requirement.[80]

4.4.13. Duty to report personal data breaches

The Commission's proposal sets the deadline to report a breach within 24 hours from the event. This strict requirement is softened by addition of the words *"where feasible"* and by a provision implying that notice within 24 hours does not need to be given when the data controller provides a *"reasoned justification to the DPA as to why this time period could not be upheld".* Kuner warns of excessive

[78] Idem, p. 17.
[79] Idem, p.15.
[80] Idem, p. 14.

notifications of data security breaches due to this tight 24-hours requirement and draws attention to the US experience where a similar rule created strong incentives to over- notify.[81]

4.5. Parliament's amendments

During the discussion in the European Parliament the MPs suggested more than 4000 amendments to the Commission's proposal.[82] The consolidated version of the text, handed over by the LIBE Committee in March 2013, importantly reduced the number of the proposed changes. Nevertheless, a few new requirements that it introduced are far reaching and tend to set the standards of data protection even higher.[83]

First of all, the Parliament's version of the regulation clarifies its territorial scope. It explicitly states that the Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, "*whether the processing takes place in the Union or not.*"[84]

In Article 6(1), which lists the situations in which processing of data is legitimated (and needs to be carefully balanced), the EU parliament introduced the "reasonable expectations test" to determine whether a third party should be allowed to process data. In doing so, it gave more weight to the data subject's position in a balancing exercise. Researchers from Tilburg University state that the same test was implemented in the American practice, however, they point out that it has received a lot of criticism.[85]

The Parliament omitted the Commission's proposal to prohibit the use of consent in cases of a significant power imbalance (for instance in relation between an employee and his employer).[86] Thus, the amended version adopts a moderate approach by advising to take certain precautions in order to avoid giving an unwanted consent.

Parliament paid more attention to the fact that there are often minimal differences between controller and processor, while the deviations in legal consequences could be far reaching. Since even the controllers and processors themselves have difficulties with defining their proper status, it is naive to

---

[81] Idem, p. 14.
[82] EU draft Data Protection Regulation: the LIBE Committee amendments , A Hogan Lovells Briefing Paper, 2013, p. 1. Available at: http://www.hldataprotection.com/files/2013/11/EU-Draft-Data-Protection-Regulation-LIBE-Committee-Amendments.pdf.
[83] Information available at: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2F%2FEP%2F%2FTEXT%2BREPORT%2BA7-2013-0402%2B0%2BDOC%2BXML%2BV0%2F%2FEN&language=EN#title1.
[84] Cuipers, C., Purtova, N., Kotsa, E.: Data Protection Reform and the Internet: the draft Data Protection Regulation, Tilburg Law School Legal Studies Research Paper Series No. 03/2014, p. 3.
[85] Idem, p.4.
[86] Idem, p. 6.

expect that a data subject could do it with less effort. The Parliament's text addresses this problem by requiring that arrangements between controllers and processors *''duly reflect the joint controllers respective effective roles and relationships vis-à-vis data subjects''*. Importantly, in case of unclear responsibility, the controllers shall be jointly and severally liable.[87]

The Parliament's text articulates the principle of accountability more explicitly. Article 22 has been fundamentally reviewed to reflect a comprehensive vision of the content and rationale of the accountability: the controller has an obligation to *adopt* technical and organizational measures to ensure and *demonstrate* – in a transparent manner - that the data processing is consistent with the Regulation.[88]

Apart from renaming it to the right to be erased, the Parliament's version kept all strict characteristics of the Commission's initial proposal of the right to be forgotten. Having been extensively studied by numerous academics and practitioners, the scope of the right is nevertheless difficult to estimate. On the one hand it could be argued that it is just a right to access in a disguised form,[89] but on the other, it could have far reaching consequences.[90]

Commission's Proposal of the right to data portability received substantial criticism for being formulated too restrictively. Therefore, the Parliament's version deleted the whole provision and joined the right to data portability with the right to access, granting the data subjects broader rights as they had in the Commission's proposal.[91]

With regard to regular privacy impact assessments, the European Parliament version included a requirement to assess the necessity and proportionality of the processing operations in relation to the purposes, an indication for the time limits for erasure and duty to assess the context of data processing. European Parliament deleted the provision that excused public authorities from the obligation to carry out the data processing operation.[92]

The Commission's proposal included a few vague provisions which were supposed to be clarified in later stages by the Commission's delegated and implementing acts. Due to uncertainties and possible

[87] Idem, 7.
[88] Idem, 10.
[89] Ibidem.
[90] Similarly as the recent judgment in Google case spreads the scope of the right to access from the General Directive. Case C-131/12 Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, judgement form the 5th of May 2014.
[91] Cuipers, C, Purtova, N, Kotsa, E.: Data Protection Reform and the Internet: the draft Data Protection Regulation, Tilburg Law School Legal Studies Research Paper Series No. 03/2014, p. 12.
[92] Idem, 14.

arbitrariness typical for this type of legal acts, the Parliament reduced the scope of Commission's power and limited the number of provision it can elaborate further.[93]

5. The economics of data protection

5.1. Short summary of the chapter

The following chapter explains economic implications of privacy laws by balancing their costs and benefits. It critically assesses the economic efficiency of the current regulatory framework. Finally, it presents recent research on economic impact of the draft EU data protection regulation.

5.2. Privacy trade off and regulatory implications

In line with their free market ideology the Chicago school scholars, with Posner in the leading role, claim that data protection is inefficient. The reason for such view is the fact that only when all the information is revealed (including the private ones) information asymmetry is avoided and the market price drops to the lowest level possible.[94] However, Hirschleifer and Taylor share the opposite view. According to their theories data protection prevents that the consumers bear the burden of negative externalities induced by the companies that use their personal data without any limits. Another way to explain why consumers are likely to lose when their privacy is not protected is through the prism of behavioral economics.[95] Following the behavioral theories, incomplete information, bounded cognitive ability to process the available information and a host of systematic deviations from theoretically rational decision-making, result in irrational decisions of a consumer. As the market equilibrium will tend *not* to afford privacy protection to individuals when they are not fully rational or in fact myopic, privacy regulation may be needed to improve consumer and aggregate welfare.[96]

Due to the fact that subjective gains of privacy protection are very difficult to estimate while the corporate profits gained by intruding someone's privacy can be calculated much more easily, it seems that benefits of disclosing the data are much higher.[97] However, if all the aspects, also private ones, would be taken into account, the final result might be notably different. It should be born in mind that the final equilibrium of balancing between cost and benefits of data protection depends on circumstances in global economy as well as on subjective preferences. Usually, economic analyses operate with the same costs and benefits of data (un)disclosure, however, the ponders the researchers assign to a certain cost or benefit vary greatly and result in different outcomes.

---

[93] Idem, p. 17.
[94] Acquisti, A.: Joint WPISP-WPIE Roundtable, The Economics of Personal Data and Privacy: 30 Years after the OECD Privacy Guidelines, 1.12. 20010, Background Paper 33, "The Economics of Personal Data and the Economics of Privacy", p. 4.
[95] Idem, 4 and 5.
[96] Idem, 6.
[97] Idem, 12.

Starting with the benefits of a more disclosed data, i.e. fewer data protection rules, Aquisti lists a bunch of positive consequences for data processors. If data is revealed, business subjects have more information about the consumers which is considered a strong capital by most of the companies. The data collected can be used in the future either in marketing purpose (to get access to consumers) or to enable (re)assessment of the clients (for example when estimating their creditworthiness). Data can be also sold to another company or processed in order to identify the trends on the market.

Disclosed data benefit consumer as well. As flexible privacy rules enable businesses to target the clients more precisely, this finally results in less spam mail and more precise information.[98] In certain cases the consumers' gain may be estimated in exact numbers – this occurs when they receive financial compensation for their data shared, for example in form of paid survey participation. Not only less privacy improves company's performance in relation to their customers, it also increases the efficiency of their employees.[99] For example, training a healthy worker is a better investment for an employer; however, it can only be achieved if health privacy rules do not stop this matching and they enable the employer to inspect medical records.

If privacy regulation is stringent, the companies more often face administrative sanctions, monetary fines and even criminal liability. For business, the fines that directly reduce the profit are the most apparent cost of privacy rules. However, there is another important cost of stringent privacy rules – uncertainty due to the too extensive or incoherent legislation which may cause, at worst, over-investments in compliance strategies. Also, as protection of data makes collection of personal information more difficult and costly, the companies become less competitive on market. By restricting the availability of customer data in the market new entrants and small companies are put in a competitive disadvantage by privacy regulation.[100] Strict privacy rules may be disadvantageous for consumers as well – Acquisti gives the example of a Facebook user who decided to choose the most strict privacy settings for his user account. This decision prevented him from having access to certain websites which would have been otherwise of his special interest, since they were only reachable through via Facebook Connect authentication.[101]

On the other hand, there is an extensive list of cost triggered by insufficient privacy regulation. Apparently, accessibility to private information enables companies to charge more for their services. For instance, Acquisti describes the Amazon's discriminatory practices when it overcharged higher the consumers who previously purchased a similar product expecting them to be more likely to pay more for the second one. Without stringent rules, data subjects may experience more data abuses and breaches

[98] Idem, p. 8 and 9.
[99] Idem, p.
[100] Bamberger, K. A. R and Mulligan, D. K.: New Governance, Chief Privacy Officers, and the Corporate Management of Information Privacy in the United States: An Initial Inquiry, Forthcoming in Law and Policy, Vol. 33 (2011), p. 39.
[101] Acquisti, A.: Joint WPISP-WPIE Roundtable, The Economics of Personal Data and Privacy: 30 Years after the OECD Privacy Guidelines, 1.12. 20010, Background Paper 33, "The Economics of Personal Data and the Economics of Privacy", p. 11.

which may result in substantial amount of spam mail, general discomfort and even worse consequences such as poor work evaluation or criminal charges. In this way, low data protection is resulting in a transfer of negative externalities of data exploitation onto consumers. Although less stringent rules seem beneficial for companies, this is not necessarily the case. Namely, if more data is disclosed, chances for abuses of these data are, logically, higher. Data breaches negatively affect company reputation, reduce the amount of purchases and may even affect its value. In the US, it has been calculated that the stock prices return fell down on average by 0,6% after a breach was released (it is also true, however, that in the majority of cases it soon returned to normal levels).[102]

In his paper, Ian Brown lists three types of market failures that emerge in cases of insufficient privacy protection: negative externalities (receiving tones of spam email), information asymmetry (lack of knowledge about the real value of his private information) and anti-competitive practice.[103]

To resolve these shortcomings he suggests three privacy regulation models. The first model requires that consumers remain anonymous, the second one requires that consumers are offered opt-out for data processing, while the third one only allows processing of data when there is an explicit consent of data subject. Bouckaert and Degryse found that opt-out was the most efficient model. Opt out is also a good way to prevent hindering of innovation due to stronger privacy protection. On the contrary, Tang, Hu, and Smith argue that opt-out is only optimal when few people are sensitive to privacy harms or when losses are low.[104] For intermediate levels of sensitivity and losses, privacy seals are socially optimal. When many people care strongly about privacy and face high losses, however, baseline protections are socially optimal.[105]

5.3. Commission's proposal and economic impact assessments

Recently, a number of research papers estimating the financial impact of the proposed EU data protection regulation have been published. While the majority considers the proposed regulation a great financial burden for the businesses, European Commission does not share the same view and sees the regulation as a positive improvement for the European economy. Brief summaries of the reports are presented below.

[102] Idem, p. 12.
[103] Brown, I.: The economics of privacy, data protection and surveillance, Oxford University, p. 5.
[104] Idem, 11.
[105] Ibidem.

5.3.1. European Commission research[106]

According to the Commission's findings the reform will bring substantial benefits for the European companies and will boost economic growth. One of its major benefits, unification of national legal systems, will admittedly decrease the cost up to 2,3 billion per year. In addition, one-stop-shop provision which enables the companies to deal with one single supervisory authority and not 28, as it is currently the case, will simplify the procedures and reduce the cost of doing business in the EU.

The European Commission emphasized that the reform will have no negative consequences for small and medium enterprises (SMEs). Namely, the Commission has proposed to exempt SMEs from several provisions of the Data Protection Regulation – from the obligation to appoint a data protection officer insofar as data processing is not their core business activity, from the notifications to supervisory authorities, from impact assessments unless there is a specific risk and from providing an access to data if requests are excessive or repetitive. In addition, Commission argues that the new regulation which enables the companies to deal with only one authority instead of 28 the EU's data protection reform will help SMEs break into new markets.

5.3.2. ICO analysis[107]

On behalf of the British Information Commissioner's Office (ICO) the group of London economists conducted a research on the economic impacts of the proposed regulation. Firstly, they divided the legal improvements of the new regulation into two groups – the ones that cause direct and the ones that cause indirect costs. In the first group they listed free subject access request, breach notification duty within 24 hours, data protection impact assessment, employment of a data protection officer and new (high) fines. In the group of the indirect cost they included the costs arising from the newly defined right to be forgotten, data portability provision, higher standard for the consent, data minimization requirement and the general uncertainty that the proposal brings in the EU.

The research results were striking: according to the received answers approximately 40% of the companies have incorrect understanding of the regulation's provisions. Interestingly, the gaps in understanding and uncertainties are less frequent if there is a data protection officer in a company who is able to follow up the regulatory updates and has an overview over the complex practice. In terms of economic impact the researchers estimated a negative net present value of the regulation, resulting in 2,1 billion pounds overall losses.

---

[106] Progress on EU data protection reform now irreversible following European Parliament vote, European Commission - MEMO/14/186 12/03/2014, available at: http://europa.eu/rapid/press-release_MEMO-14-186_nl.htm.

[107] Implications of the European Commission's proposal for a general data protection regulation for business, Final report to the Information Commissioner's Office, prepared by London Economics, 2013.

Proposed regulation introduces a few new terms or gives a new meaning to already implemented ones. An example is the definition of personal data which now also includes online IDs such as IP addresses and cookies. The fact that this definition is at the moment still unclear may result in substantial unwanted costs for the companies e.g. payments for (legal) advice or cost of implementing an incorrect compliance strategy.

New obligations imposed on processors and controllers of the information are also likely to result in additional costs. Firstly, data protection impact assessments will have to be conducted prior to certain risks, though it is not clear what exactly *"risks for data protection"* means. It is possible to assume that such risk assessments have to be conducted in case of processing sensitive data such as biometric or children's data or in case of profiling. In addition to privacy assessments, the draft regulation requires all the controllers to clearly demonstrate their compliance with privacy laws. Therefore, companies will have to provide an official proof of privacy impact assessment, update internal documents and, in many cases, employ a data privacy officer.

An important novelty is withdrawal of charges for accessing data. The old legislation allowed charging a person that wanted to view into his or her data. The new regulation, however, prevents companies from taking any monetary remuneration in this regard, putting additional burden on the SEMs and opening door for an excessive number of access requests. Besides offering free access to data, controllers will also be obliged to provide more comprehensive information.

Certain sectors of industry will experience even more devastating impacts. Direct marketing, for example, will have to entirely change its way of operating. Advertising companies that are processing with personal data will lose some of the investors since, especially the business angels, prefer not to be limited by strict opting-in.

According to the researchers from London Economics the European legislator was overambitious in the ideas it incorporated in the draft regulation and put too great burden on the businesses.

5.3.3. Deloitte analysis[108]

The research conducted by Deloitte focused on four sectors that make use of personal data in their daily operation: direct marketing, online behavior advertising, web analytics and credit information.

First, direct marketing uses a variety of marketing channels such as traditional mail, email and telephone to match consumers with product and service offerings that are customized to the interests of a target

[108] Economic impact assessment of the proposed European General Data Protection Regulation, Deloitte, December 2013.

group. Given its specific nature there are numerous problems that could arise from the new regulation. Explicit consent could strongly defer the scope of direct marketing as well as stricter purpose limitation principle. Namely, it is highly unlikely that the costumers would consent to have their data used for online marketing. Additional burden for the industry means duty to notify breaches, especially due to its short and stringent deadline. Deloitte's research estimates that the total impact on European GDP would be approximately 85 billion euros with 1,3 million job losses.

Online behavioral advertisement is a form of advertising that matches the online behavior of users and online advertising. The regulation would have a great impact on this industry due to the broader concept of personal data that also includes location data and on-line identifiers. In case that such data is processed, a consent requirement and additional limitations apply, which causes obstacles to more effective advertising. As Deloitte states, it is not to accept that the users would widely give consent to process their data for the purpose of online advertising, therefore the profits will most likely fall – according to Deloitte's estimations – by approximately 4,2 billion euros with 66.000 jobs less.

Web analytics analyze browsing activities. By using personal data they are able to offer a user experience tailored to a costumer's needs. However, if explicit consent is required and the purpose for which the data can be used is strictly limited, the efficiency of the industry substantially decreases. Deloitte claims that the final result could be 880 million euros lower profits and 14.000 jobs lost in the EU.

Lastly, credit information is another industry that benefits from less stringent privacy regulation. The major obstacle here would be right to be forgotten which would enable the costumers to have all their credit history deleted. Following Deloitte's estimations, 83 billion euros would be lost in this way and 1,4 million jobs would become unnecessary.

5.3.4. Other views

In her paper Elina Pyykkö observes that proposal dictates how data is to be used regardless of the operational context. She expresses concern that stronger data protection in the EU will be achieved at the cost of economic growth. For example, forcing the credit and financial services industry to obey the same rules as social networks creates a risk that credit providers adjust their portfolios to allow for the greater credit risks they have to bear because of the lower level of information available. This might result in lower consumer credit volumes and in lower technological innovations in the industry.[109]

Similarly, Prof. Moerel argues that the proposal for the new regulation should be fundamentally changed. In criticizing European privacy laws she does not go as far as Bergkamp, who blames the EU for

[109] Pyykkö, E.: Data protection at the cost of economic growth?, ECRI Commentary No. 11, 2012.

adopting economically inefficient law.[110] Contrary to Bergkamp she argues that treating privacy as human right is inherent to European culture and well founded. However, she uses examples from US practice to show in which way the EU law can be improved.[111]

For example, in the EU there is a requirement that data has to be adequately secured. In the US, there is no similar rule, however, there is a strict notification breach duty. This requirement has proven a strong driver for US companies to improve data security and data compliance in general (such as data minimization, use of encryption and increase of security) to prevent data security breaches (and subsequent reputational exposure) rather than address these after the fact. She claims that reputational exposure of multinationals for data protection and security breaches has had a stronger impact on data security than the EU fundamental data protection laws have ever had.[112] In line with her argument she supports the proposal for the duty to notify breaches, however, this is one of the rare parts where the draft regulation does not need alternations.

Other novelties such as stricter accountability principle, explicit consent, data minimization and purpose limitation principle, should be fundamentally transformed or omitted. In Moerel's opinion extensive documentation requirements, Data Protection Impact Assessment (DPIA) requirements, ex-ante requirements to consult and even obtain authorization of the Data Protection Authority in respect of certain more sensitive data, processing operations and accountability requirement should be a part of company's compliance program but not specified in the proposed regulation. Namely, the requirements are too specific and have as an inherent danger working as a "tick box" list for compliance measures regardless of their actual impact. It should be left to companies how to best achieve compliance in their organization, for which they should be accountable.[113]

[110] Bergkamp, L: The privacy fallacy: adverse effects of Europe's data protection policy in an information-driven economy, Computer Law & Security Report, Vol. 18, no. 1, 2002.
[111] Moerel, E. M. L. (2014). Big data protection. Tilburg: Tilburg University, p. 31.
[112] Idem, p. 33-34.
[113] Idem, p. 55-56.

6. Data protection and corporations

6.1. Short summary of the chapter

The following chapter describes some of the challenges that companies have to address due to privacy regulation. Furthermore, it explains in what way legal development has affected corporate governance and corporations' compliance strategies. Second part of the chapter, based on in-depth interviews and online survey, analyzes state of affairs in Dutch corporations and lists some trends resulting from the strengthened concern for privacy and upcoming regulation.

6.2. Main privacy challenges in corporations

Concern for privacy is a necessary consequence of developments in information technology. As protection of data has to run in parallel with the rapid innovations in computer science, its scope and importance has been crucially extended in recent years. (New) legal rules have encouraged companies to implement (stringent) privacy strategies. However, as economic analysis of privacy law makes it clear, legal compliance is not the only reason for privacy concerns. Benefits gained from the strengthened privacy framework, such as better reputation, more loyal clients etc., are often an even stronger incentive for companies to comply with privacy rules.

A **data protection strategy** in a company normally consists of four steps. First step is taking an inventory of data processing practices. Such an inventory can often be the most expensive and long-lasting part of a compliance project. The questions that need to be answered during such an audit are for instance: What personal data does the company process? What are the purposes for which they are processed? Which entities in the company process data as data controllers? Does the company process any sensitive data? The second step is identifying compliance gaps and developing a plan to deal with them. In order to find the gaps it is necessary to cooperate with several departments, at least with legal, IT and HR office. The plan (road map) written on the basis of this research has to be feasible and realistic as it will be later implemented. The third step is drafting and implementing policies and procedures in the company e.g. revising contractual language with suppliers, reviewing online privacy policies, completing notifications to local data protection authorities and obtaining necessary consents. In the last step it is necessary to develop and implement procedures to embed the plan in the company. The plan should also include the appointment of data protection officer and trainings for some other employees.[114]

[114] Kuner, C: Kuner, C.: European Data Protection Law, Corporate Compliance and Regulation, Second Edition, Oxford University Press, 2007, pp. 238-241.

In addition, every company needs to take into account the duty to **notify data privacy authorities.** Due to the flexibility in the diction of the General Directive the national laws vary considerably. However, a minimum level of information that needs to be notified to the authority and a minimum amount of events which trigger such a notification are clearly defined. Since failure to notify may have serious consequences for a company (including criminal charges for officials responsible), notification is one of the most important compliance actions. As regards the dilemma which role in a company should be in charge of preparing a notification, Kuner suggests assigning this duty to someone from legal department.[115]

An important challenge for the companies is the **processing of employee data**. Before starting with any kind of processing there has to be a valid legal basis. For most types of processing of employee data, this is either the employment contract or "legitimate interest" test. Consent, on the other hand, is a dangerous basis for processing and some data protection officials do not even recognize it as a valid one.[116] Another important issue related to employee data is the usage of company computers. Namely, with the increased use of the internet and e-mails in the workplace, companies have a need to monitor how the employees use the systems. This is necessary not only to measure performance, but also to ensure that employees are not using the system for illegal purposes. When monitoring the computer usage, it is of the utmost importance that the legitimate interests of a company and privacy of an employee are balanced in a proper way.[117] As Article 29 Working Party stated in its opinion: "*Workers do not abandon their right to privacy and data protection every morning at the doors of the workplace. They do have a legitimate expectation of a certain degree of privacy in the workplace as they develop a significant part of their relationships with other human beings within the workplace. However, this right must be balanced with other legitimate rights and interests of the employer, in particular the employer's right to run his business efficiently to a certain extent, and above all, the right to protect himself from the liability or the harm that workers' actions may create.''*[118]

Living in a digital world, it is indispensable for a company to use internet for the communication with its consumers and business partners. The fact that a company owns a website is of vital importance for its marketing strategy and tactics. Whenever this is the case, the company's duty is to ensure proper standard of data protection for all website visitors by issuing a clear privacy policy.[119]

---

[115] Idem, p. 248.
[116] Idem, p. 260.
[117] Idem, p. 262.
[118] Article 29 Working Party, Working document on the surveillance of electronic communications in the workplace, (WP 55, 29 May 2002), p.4.
[119] Kuner, C: European Data Protection Law, Corporate Compliance and Regulation, Second Edition, Oxford University Press, 2007, p. 282.

Data protection should be observed also in cases of a corporate restructuring e.g. mergers or acquisitions. In a due diligence procedure, the steps that need to be taken are, as Kuner lists, evaluating data to be processed, finding a legal basis for processing, providing notice, ensuring security measures and providing a legal basis for international transfers. Having completed a due diligence, the purchaser of a company obviously wants and requires access to the data held by the acquired company. However, if an acquisition is structured as an asset deal the acquisition of personal data will be considered a data transfer to third party under data protection law and has to be processed accordingly.

6.3. Changing corporate governance in the world of stronger data protection

Previous chapter lists a few evident situations in which data protection plays a crucial role in a corporation. Apparently, data protection in corporations has evolved from a matter of a pure compliance into a c-level issue and has significantly influenced corporate governance.

American researchers Baberger and Mulligan claim that descriptions of privacy law *"on the books"* fail to capture even very basic attributes of the manner in which privacy regulation actually works. Specifically, they notice that no explanation has been offered for the fact that, even without any changes in formal statutes, corporate privacy management in the United States has undergone a profound transformation. American corporations now commit relatively massive amounts of resources to privacy, as evidenced by the appointments of chief privacy officers and other privacy professionals, privacy certification and training, new privacy practices in major law and audit firms, and the development of privacy seal and certification programs.[120]

To find out more about privacy law *''on the ground''*, Bamberger and Mulligan conducted numerous interviews with leading privacy officials in American corporations. The analysis of the discussions brought them to some interesting conclusions. Firstly, they realize that privacy has been deeply integrated into general corporate decision making. In the leading corporations it is most often considered a part of risk management. Secondly, not only do companies rely on the national data protection legislation, they are also adopting their own internal rules in order to offer consumers better protection.[121] The latter is highly appreciated since it may establish a better connection with the clients and may also strengthen public trust in a company, which is, especially for the US companies, of the utmost importance. Finally, they conclude, as the role of privacy officer has been given importance equal to the rest of the board members, privacy has finally reached the c-level.

[120] Bamberger, A.K. and Mulligan, D.K.: Privacy in Europe: Initial Data on Governance Choices and Corporate Practices, The George Washington Law Review, Vol. 81, No. 5 (2013), p. 1659.
[121] Idem, p. 1537.

During 2010 and 2012 Bamberger and Mulligan repeated their research in the EU. The results showed that European countries pay more attention to legality of data processing and face more legal influence in privacy matters. Another characteristic is emphasized importance of workers' rights in the EU, especially in Germany. As one of the interviewees explained: *"The issue of data protection is also very much influenced by work councils and by unions."* Contrary to the responses from US officials, the researchers found that term "trust" arose infrequently in conversations about privacy.[122]

In the EU, DPO roles are mostly taken by lawyers and they hold very high positions within a company. A DPO is envisioned as an extension of the regulator, placed within the company with access to data and decision makers, but with overriding obligations to regulators and the law.[123]

Similarly to the US firms, European companies integrate privacy into existing risk management functions, aligning it with other core company's goals and thereby benefiting from a broader set of resources and structures. Whereas in the United States they found a uniform decision to distribute expertise and accountability throughout corporate decision making, relying on embedded personnel with specialized privacy training and business leads ultimately accountable for privacy, in Germany many firms adopt a similar model but with greater centralized control over policymaking. The greater centralization of control is attributable to the independence requirement placed on DPOs by law. [124]

6.4. Research project: trends in corporate data protection

6.4.1. The aim of my research and methodology description

The fact that Baberger and Mulligan's research project only focused on Spain, France and Germany, encouraged me to conduct a similar research in the Netherlands. However, there are some substantial differences between our research strategies. Firstly, Baberger and Mulligan primarily focused on corporate governance, while my research also tackles the issue of the upcoming data protection reform and its financial impacts. Secondly, the scope of Baberger and Mulligan's project was much broader as they had more than two years to finalize their research results while my timeframe was extremely tight (two months from setting the hypotheses until delivering the outcomes). Finally, Baberger and Mulligan interviewed privacy leaders regardless of the nature of their firm including independent lawyers and

[122] Idem, p. 1573.
[123] Idem, p. 1579.
[124] Idem, p. 1588.

governmental representatives, while my research focused exclusively on employees of big multinational firms headquartered in the Netherlands that are placed on the latest Forbes 2000 list.[125]

For my research project I used two methodologies; firstly, I prepared a questionnaire with 38 multiple choice, scaled and ranking questions serving as a basis for the online survey which was launched on the 5th of May, 2014. 20 potential respondents from risk, legal and IT departments of leading multinational companies were invited to take part in the survey. Even though I had to exclude few responses due to their unsuitability, the final response rate was 28%. Secondly, I conducted three in-depth interviews with corporate privacy leaders, which were also chosen from the two lists mentioned above. The questions used during the discussion were focused on the same topics as the online questionnaire and mostly open-ended, thus leaving room for additional comments.

To analyze the responses I used qualitative analysis based on constant comparative strategy. This type of strategy involves taking one piece of data (one interview, one statement, one theme) and comparing it with all others that may be similar or different in order to develop conceptualization of the possible relations between various pieces of data.[126]

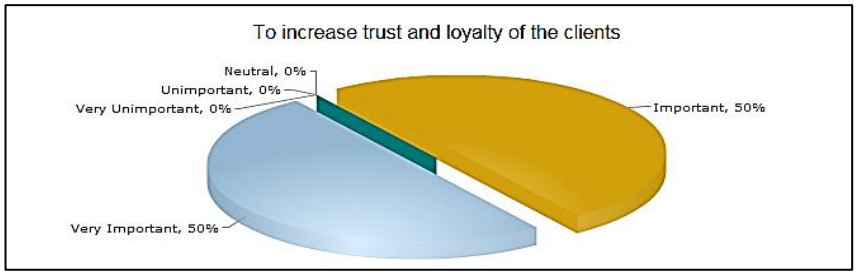
When interpreting the results I arranged the relevant answers into three groups: first, reasons that are of legitimate concern for data protection in companies, second, interaction between data protection and corporate governance and third, economic impact of the upcoming regulation. The crucial findings are presented below.

6.4.2. Online survey – findings

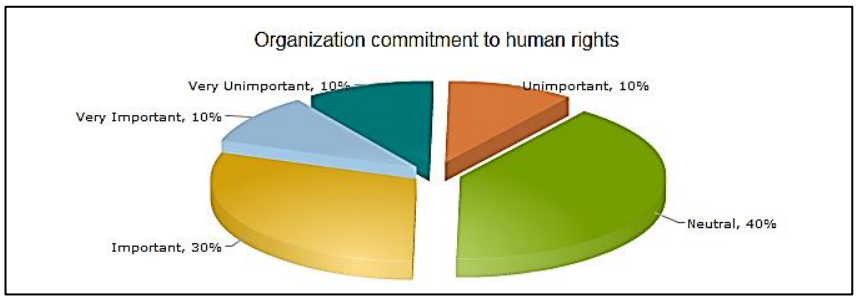
6.4.2.1. Reasons to implement privacy controls

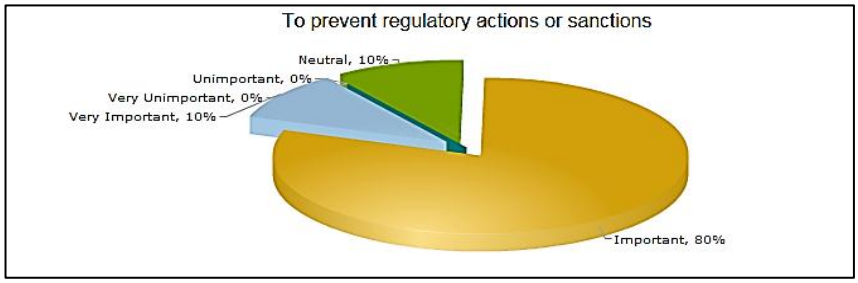
Contrary to the findings of the two American researchers, the results of my research show great concern of European (Dutch) companies for trust and loyalty of their clients. This is, according to the majority of respondents, the main reason for (stricter) data protection in their companies. Threat of regulatory sanctions is put on the second place. Concern for human rights, though being the very foundation of the EU data protection law, is seen as less important.

[125] The list is available through: http://www.forbes.com/global2000/.
[126] Thorne, S.: Evid Based Nurs, Data analysis in qualitative research, 3, 2000., p.68.



What are the main reasons for implementing data protection strategy in your company?

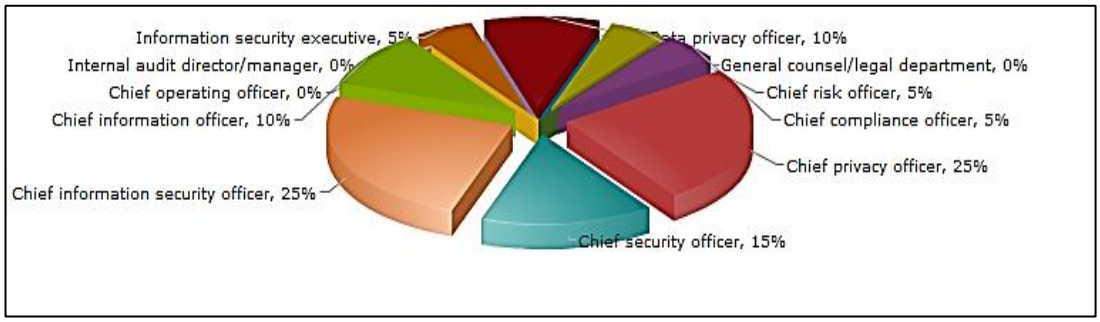


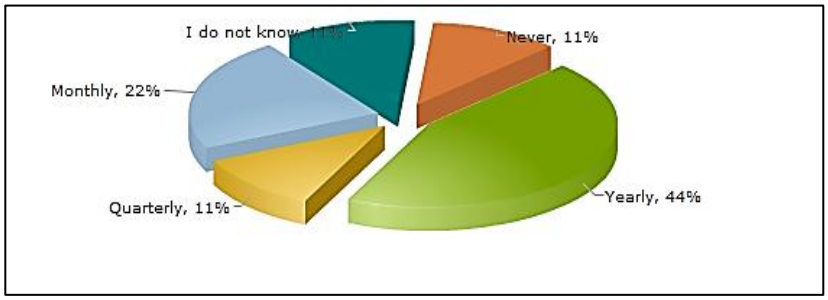


6.4.2.2. Privacy and corporate governance

As seen from the survey results, chief privacy officer and chief information security officer are the roles that are most often in charge of privacy. This confirms Baberger and Mulligan's finding that European companies have been introducing a new type of c-suite officer. However, it seems that privacy is still quite low on corporate agenda – the boards discuss it rarely, in most companies only once a year.

Which role in your company is responsible over privacy?



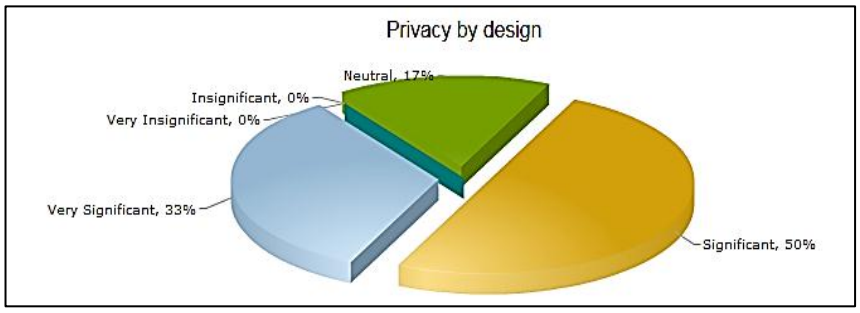


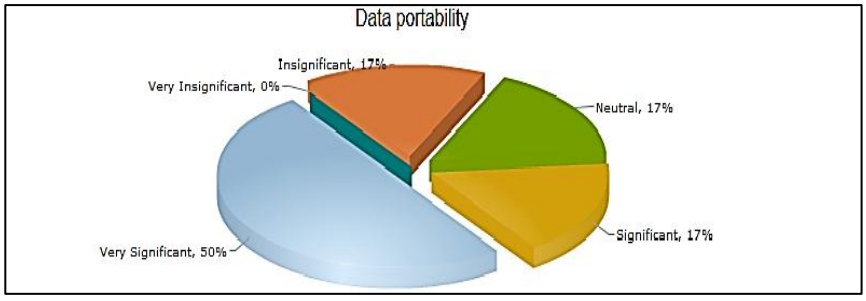
How often is privacy discussed in your board?

6.4.2.3. Economic impact of new legal requirements

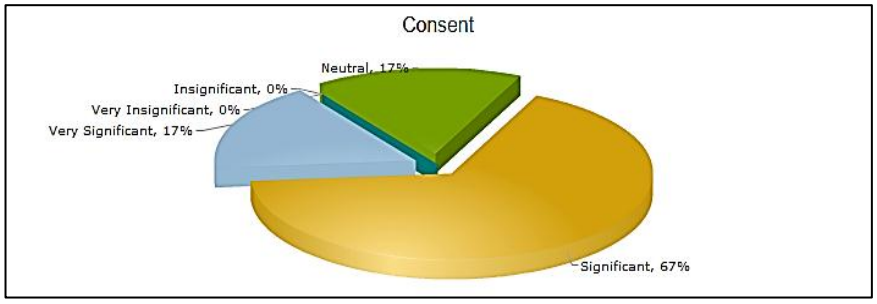
Contrary to the European Commission's study[127], the respondents are neutral to the one stop shop rule which the EU advocates as the greatest achievement of data protection reform and a cost-saving measure. According to the respondents, more significant financial impact is related to administrative fines, privacy by design, portability requirement and explicit consent. Also, the respondents estimate that adoption of the new regulation will result in higher compliance cost in the next year.

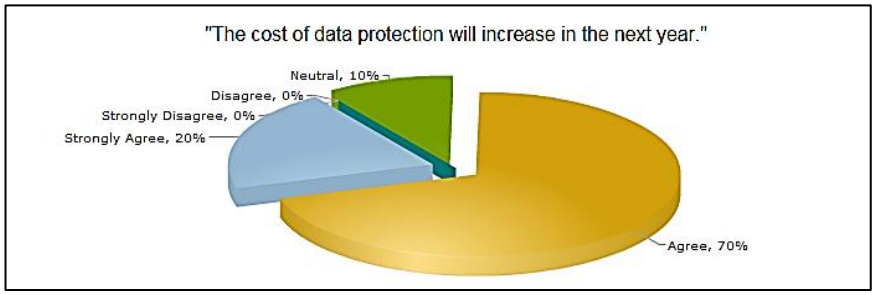
What is the financial impact of the proposed rules for your company (or will be)?





[127] See page 37.





Do you agree that the cost of data protection will increase in the next year?

6.4.3. In-depth interviews – findings

6.4.3.1. Reasons to implement data protection

In the same way as the online survey the interviews disprove the hypothesis that the European companies care less about trust and loyalty of their clients than their US competitors. It seems that the question of trust relates more to the industry in which a company is active (for example, retail and consumer products sectors seem to be more influenced by privacy considerations) and to its general reputation in global economy than to the place of its establishment. Thus, in majority of cases, legal compliance is the secondary reason for the implementation of privacy controls.

It may sound contradictory, however, as one of the interviewees observes, the mere fact that data protection is implemented is sometimes more important than efficiency of that protection. This can be seen in a case of a data breach: "*You can have a really bad incident, but if you manage a crisis well, a breach is not considered fatal. It is important how the breach happened and how the company acts. If it tries to hide it from the public than people have negative emotions.*"[128]

6.4.3.2. Privacy and corporate governance

Strengthened data protection in the EU considerably influences corporate governance. The interviewees report that their companies are undergoing corporate structure reforms in order to meet new legal

[128] Interview no.1, see page 51

requirements.[129] *Inter alia* these transformations should result in more clearly defined responsibilities of chief privacy officer. However, one of the respondents reports that his company has decided not to appoint a DPO or a c-level person that sits on the board, but rather assign privacy duties to a manager type of an employee with global responsibilities. *''We follow this approach: privacy must be a part of the process owners thinking. It should not be a c-level person that takes all the burden. We are more striving for a manager that is making sure that everything in the process is working. Maybe it is a small difference but it should be visible to the organization.''*[130]

As regards the cooperation of the board, interviewees mostly describe it as insufficient: ''*I think that board is not aware enough. You need some guts to take it up. But here they do not understand the importance of privacy. Another problem is also that privacy is vague and more complex compared to, let's say, competition.''* [131]

What the ideal background and abilities of a privacy leader are, is still an open question. One of the respondents claims: *''The role is not technology focused. It is not a legal role either. A combination of a legal and a business person with interest in technology, but not a technology person.''* On the other hand, some people see a DPO as a person within legal group with legal expertise. *''Privacy is a legal topic, interpretation of law – as a DPO you daily work on privacy impact assessments, but sometimes you face nasty legal issues that need to be answered by a lawyer. IT background is important as well as business, but this is a common point for everybody that works in a corporation.''*[132]

6.4.3.3. Economic impacts

Undoubtedly, economic impacts are at the moment the major concern in terms of EU data protection. The interviewees' responses signal that the most burdensome provisions are the following: right to be forgotten, data portability, privacy by design and breach notification. As the latter gives no chance to stop the breach and to find a cause before a public notification, it is considered harmful to companies as well as to the public. Right to be forgotten is another problematic novelty. *"It requires to go through all the supply chain and print out everything you have about the client. To comply with this rule, it would be necessary to replace the whole system. But you need years to do it! This is really a concern because we may end up in a non-compliant situation and we cannot avoid it.''* Data portability requirement was obviously written with the intention to limit the new, rapidly growing IT firms and is not enforceable for many of the traditional businesses. Privacy by design is another vague and problematic provision. One of

[129] Intervju No. 2 and 3, see pp.55 and 53.
[130] Interview no. 1, see p. 51.
[131] Interview, No 1, p. 53.
[132] Intervju No. 1 and No. 2, see 51 and 53.

the interviewees reports that his company is currently coping with tones of problems arising from inappropriate handling of data protection in the past. This legacy is the biggest burden when implementing privacy by design as all the systems have to be reviewed and many of the contracts re-negotiated.[133]

For all the respondents, higher fines are the most problematic provision. However, even more burdensome than the high percentage is the fact that a fine can be triggered by any type of a breach in a company, without exception. *''If a person in Romania illegally sells some data twice, you can be fined with 5% of your annual turnover! As it is proposed in the draft regulation, it is possible that the Romanian authority itself define whether such a behavior is considered inappropriate and charges the whole group with a 5% fine,''* warns one of the interviewees.[134]

7. Conclusions

As my survey has proved, there is an accelerated endeavor of European (Dutch) companies to reconsider their privacy strategies. This developments were mostly triggered by the adoption of the proposal for a new data protection regulation which will fundamentally change the current privacy regime in the EU. The companies are striving for better legal compliance, however, they are also considering some other reasons for implementing data privacy strategy. As the survey have illustrated, one of the most important incentives is to maintain trust and loyalty of the clients.

The research outcomes confirmed increasing awareness for privacy among the European (Dutch) companies. Nevertheless, there is still a lot to do – to achieve proper compliance, the companies have to transform their privacy strategies, educate their employees about the last developments in the field of data protection and adopt binding corporate rules.

Doubtlessly, financial impacts of the upcoming data protection are of the companies' biggest concern. Privacy by design, right to be forgotten, data portability, breach notification and administrative fines are the novelties which will impose the highest financial burden on companies. Interestingly, all these measures were criticized already at the time when the draft regulation came to public for the very first time, but no fundamental changes have been made since then.

To sum up, the hypothesis that corporate governance has been changing due to more stringent privacy rules has been confirmed as well. European corporations are appointing new data privacy officers and

[133] Ibidem.
[134] Ibidem.

chief privacy officers. By doing so, the privacy is finally becoming a c-level issue and is climbing up the business agenda.

8. Bibliography

Monographies

- Kuner, Cristofer: European Data Privacy Law and Online Business, Oxford University Press, 2009.
- Handbook on European data protection law, European Union Agency for Fundamental Rights and Council of Europe, December 2013.
- Kuner, Cristofer: European Data Privacy Law and Corporate Compliance, Oxford University Press, 2003.
- Craig, P. and De Burca, G: EU Law: Text, Cases, and Materials, Oxford University Press.
- Kosta, E.: Consent in European Data Protection Law, Martinus Nijhoff, 2013.
- Cuipers, C, Purtova, N, Kotsa, E.: Data Protection Reform and the Internet: the draft Data Protection Regulation, Tilburg Law School Legal Studies Research Paper Series No. 03/2014.

Articles

- Rodota, S. in: Reinventing Data Protection?, ed. Serge Gutwirth et al., Springer, 2009.
- Kokott, , J. and Sobotta, C: The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR, International Data Privacy Law, Vol. 3, No. 4, 2013.
- Bergkamp, L: The privacy fallacy: adverse effects of Europe's data protection policy in an information-driven economy, Computer Law & Security Report, Vol. 18, No. 1, 2002.
- Bano Fos, J. M.: An Individual's Quest to Always Be Remembered: A Critical Approach to the Right to Be Forgotten in the European Data Protection Directive (February 13, 2014).
- Birnhack, M.: The EU Data Protection Directive: An Engine of a Global Regime (September 16, 2008), Computer Law and Security Report, Vol. 24, No. 6, 2008.
- Kuner, C.: The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law (February 6, 2012), Bloomberg BNA Privacy and Security Law Report (2012).
- Wong, R.: The Data Protection Directive 95/46/EC: Idealisms and Realisms (January 14, 2012), International Review for Computers and Law, 2012.

- Implications of the European Commission's proposal for a general data protection regulation for business, Final report to the Information Commissioner's Office, prepared by London Economics, 2013.
- Moerel, E. M. L. (2014). Big data protection. Tilburg: Tilburg University.
- Bamberger, K. A. R and Mulligan, Deirdre K.: New Governance, Chief Privacy Officers, and the Corporate Management of Information Privacy in the United States: An Initial Inquiry, Forthcoming in Law and Policy, Vol. 33 (2011).
- Economic impact assessment of the proposed European General Data Protection Regulation, Deloitte, December 2013.
- Pyykkö, E.: Data protection at the cost of economic growth?, ECRI Commentary No. 11, November 2012.
- Acquisti, A.: Joint WPISP-WPIE Roundtable, The Economics of Personal Data and Privacy: 30 Years after the OECD Privacy Guidelines, 1.12. 20010, Background Paper 33, "The Economics of Personal Data and the Economics of Privacy".
- Van Hoboken, J.: The Proposed Right to be Forgotten Seen from the Perspective of Our Right to Remember Freedom of Expression Safeguards in a Converging Information Environment, Prepared for the European Commission, Amsterdam, May 2013.
- Bapat, A: The new right to data portability, Privacy, Data Protection Journals, Volume 3, Issue 3.
- EU draft Data Protection Regulation: the LIBE Committee amendments , A Hogan Lovells Briefing Paper, 2013.
- Brown, I.: The economics of privacy, data protection and surveillance, Oxford University.
- Lynch, L.: EU Data Protection's Paradigm Shift , From Directive to Regulation, EY publication.
- Katko, P., Naftalski, F.: Data privacy and global mobility, 2012 Human Capital Conference, EY publication.

Internet sources

- Gardner, S.: European Parliament Votes Overwhelmingly In Favor of Data Protection Reform Proposal (March 17, 2014), available at: http://www.bna.com/european-parliament-votes-n17179885695/.
- Smolaks, M.: European European Parliament Votes Overwhelmingly In Favor of Data Protection Reform Proposal Parliament Approves EU Data Protection Regulation Draft (March 12, 2014), available at: http://www.techweekeurope.co.uk/news/new-eu-data-protection-regulation-draft-approved-141369.

- "EU Data Protection Regulation: one step forward", available at: https://www.twobirds.com/en/news/articles/2013/global/libe-committee-of-the-euro-parliament-votes-on-compromise-amendments-to-the-draft.
- Merriem-Webster Online Dictionary, available at: http://www.merriam-webster.com/dictionary/cookie.
- http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CM=&DF=&CL=ENG.
- http://www.information-age.com/technology/security/1687058/uk-ranks-21st-in-europe-for-privacy-protection.
- www.dataguidance.com.
- http://www.galexia.com/public/research/assets/safe_harbor_fact_or_fiction_2008/safe_harbor_fact_or_fiction-Introduc.html.
- Information available at the European Commission's official website: http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm.
- Hunton&Williams, EU Data Protection Regulation Tracker, available at: http://www.huntonregulationtracker.com/legislativescrutiny/

Case law

- Case C-101/01 Lindqvist [2003] ECR I-12971.
- Case C-73/07 *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy* [2008] ECR I-9831.
- C-275/06, *Promusicae* [2008] ECR I-271.
- Case C-518/07, Commission and EDPS v Germany, judgement form 28.3.10.
- Case C-131/12 *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González,* judgement from 13. 5. 2014.
- Case C-293/12 joined with Seitlinger & Others, Case C-594/12, judgement from 8. 4. 2014.

9. Appendix

INTERVIEW, 27. 5. 2014	
Corporate form of the company	Public – traded on SE
Scope of operation	Global
Total number of employees	139.000
Annual revenue	More than 10 bilion
Industry	Consumer product and retail

1. **What is your role in the company? Could you explain how big part of your daily responsibilities relates to data privacy?**

In last months, privacy is 30 percent of my work (average of 10%). Currently I am the leader of the working group working for data privacy transformation.

2. **Is your company controller or processor of data?**

I could not say we are only controller or only processor. We have both roles.

3. **What is the primary reason for implementing data privacy controls?**

Main reason to pay more attention: our company is seen to be a good company. Co-workers and costumers should trust us and that's the number one reason for me. There are other people in our company that have other objectives – the main is legal compliance. Well, surely it is a driver, a motivation ... But my personal driver is to put a promise in life. We have a privacy statement and this should be seen. My second driver is avoiding breach cases. I do not mean legal consequences, but all the bad things that come when a client loses trust. I don't necessarily mean authorities actions.

Website visitors data is not considered PIA information – there is only statistics that we use. As regards privacy of third party companies – I know that there are some companies that treat third parties equally to their employees, but we are not that much concerned about it.

4. **What is your estimation of the total number of data privacy breaches faced by your company over the past year?**

We had data breaches in our company, not alarming, just every second year or something similar.

5. **Which role(s) within your company is(are) responsible for data privacy? Ideally, who should be responsible for data protection in a company?**

The work group which I lead suggests new future privacy organization. There will also be something like a DPO, but we don't call it like that. It will be more manager type with global responsibilities … Not a c-level person that sits in the board. Primarily we follow this approach: privacy must be a part of the process owners' thinking. It should not be a c-level person that takes all the burden. We are more striving for a manager that is making sure that everything in the process is working. Maybe it is a small difference but it should be visible to the organization.

The role is not technology focused. It's not even a legal role. A combination of a legal and business person, with interest in technology, but not a technology person. We have identified only one or two roles where company IT should take care of technology in terms of privacy protection, to know whether technology is effective or non-effective.

6. **As a result of the emphasized importance of privacy - could you say that corporate governance in your corporation is changing?**

I would not say that a new profession is emerging, in Germany a DPO known already for a long time. Maybe this is more relevant for another countries than in the Western Europe.

7. **How often are data protection issues presented to your board? Do you think your board pays enough attention to data protection? If not, why so?**

Board does not have enough understanding for data privacy. Especially not for the new things. They are just not there. Data privacy has been for a long time a legal requirement, but never such a hot thing. But now it can happen that a CEO has to leave due to a privacy breach ... In past also not disussed in board because technology was not that important for the companies as today (only for example Amazon). But privacy will become much more discussed in the future!

Ebay breach caused no panic in our company, it just reminded us that when we process costumer data like payment information – which is sensitive data – it should be much more secure.

You can have a really bad incident, but if you manage a crisis well, you can even be more successful afterwards Snowden showed people what's the reality so they don't have illusions anymore. A breach is not considered too bad for a company. In Ebay they also have a more complicated (two factor) system but people forget about the breach because they like comfort. It is important how the breach happened and how the company acts. If it tries to discuss it down in the media than people have negative emotions.

8. **Can you roughly estimate the total spend of your company on the privacy? Do you agree with the statement: *"The cost of data privacy will increase in the next year."*?**

Would that also include PCR – payment cards (data security)? If not, a huge difference. Then total cost is not significant, low….

Next year the costs will deinitely increase, 100% - it's the new regulation but also compensation effect from past. In the past the companies tried to incorporate BCR but this was very difficult task. Then things paused for some years. When regulation is enforced, many investments needed to fix the issues

9. **If your company has already considered the proposed rules, which are the burning issues in your opinion?**

a) Right to be forgotten

You need a very comprehensive IT approach to rule out traces. Before, they only deleted record. This is not enough with the new regulation. It requires you to go through all the supply chain and print out everything you have about the client. It would be necessary to replace the system. But you need years to do it! Perhaps for some time just impossible, it doesn't matter how much money you have. That is really a concern because we may end out in non-compliant situation and we cannot avoid it. In a company you also have other objectives, you need to grow …

We had some opportunities to work with the Working Party and we explained our concerns.

b) Data portability

Client says: Before you delete me, I want to have everything on a stick so that I can transfer to a vendor I like. Without proper interface description I don't see any meaningful thing for a costumer. But its enforceable, it's your right! I only see the point in FB/Google+ case, if you want to transfer… I think the latter was the intention of the Commission.

c) Fines

When we saw the proposal we were quite concerned. In the first version it stated AT LEAST 5% - NO THRESHOLD! Even a small breach may trigger a fine, unfair. In the new version no minimum limit, which is very good. But on the other hand the Parliament voted for a higher percentage. If a person in Romania two times in a role sells some data, you can pay 5% of your annual turnover! As it is written now the Romanian authority can define "this is bad and now I want 5%".

10. How do you estimate the following novelties in the proposed regulation?

- **Data minimisation**

We need to be minimalistic already. But talking in the EU context, we have different approaches. But we have never collected data excessively.

- **Breach notification**

No. Four on my list. It has been discussed and changed (24 to 72 hours). It is important that you don't go out to public before you really understand the breach. A legal requirement to inform public hurts the company (and even the public). It's better to have a chance to stop the breach and to find a cause.

I have respect to Commission and for the work that they have done. I believe they had professionals but the final version is always a compromise of different views. They are trying to make the things better.

Now the balance is a little bit to consumers.

Our company is a good company, but we want to be better. This requires a lot of investments. And trust! We are trust based company, we trust our co-workers a lot. We don't want to check them, but on the other hand we are forced to do it due to the legislation.

11. How would you estimate the proposed regulation overall (subjectively)?

Unification in the EU is a very good one! It makes the system better for everyone. Not just for an individual, also for companies. The trust increases! I believe that this can boost economy. Subjectively – I like it very much (with certain exceptions mentioned before…).

INTERVIEW, 28. 5. 2014	
Corporate form of the company	Public – traded on SE
Scope of operation	Global
Total number of employees	49.560
Annual revenue	More than 10 bilion
Industry	Products and retail

1. What is your role in the company? Could you explain how big part of your daily responsibilities relate to data privacy?

I am the only one in the firm that has expertise for privacy and I have been in this role since April last year, *de facto* I am chief privacy officer. Currently we are still deciding who will be the corporate privacy officer – ideally c-level in the company. There is still no decision taken who is going to be this. This has to do with the departure of several persons in HR department. It used to be based in HR department. But now it is my advice to have it within legal group with legal expertise. It is a legal topic, interpretation of law – as a DPO you daily work on privacy impact assessments, but sometimes there are nasty legal issues that need to be answered by a lawyer. IT background important, business also, of course, but this is important part of a company in any case.

2. As a result of the emphasized importance of privacy could you say that the corporate governance in your corporation is changing?

Yes, I can see introducing a chief privacy office and more data privacy officers. Not *per se* legal counsels, better to have HR managers at a level high enough to fulfill this role, same with marketing department (executives appointed). This is all based on our BCR – we are about to launch them, we just got the approval from the European Data Protection Authority and I'm now waiting for the final ESCO approval (20. 6.). Executive committee needs to decide then on final dates (just formality). Everyone needs to understand the rules, mandatory for everyone in the company, they describe the company structure – a chief privacy officer, assistant privacy officers where there need to be and a privacy counsel, who is able to take decisions where needed. To be as efficient as possible the compliance counsel should also act as privacy counsel.
This development can be compared to competition law – only after high fines were introduced, the companies started to pay attention. Now it is a top issue in the companies, everyone wants to work on it. It sounds strange but it helps the company if there are huge fines upcoming. 5% upcoming makes all alarm bells ringing. The discussion within the company "should we have a privacy officer?" now cannot be answered otherwise then YES. It is evident we don't want to be fined, we want to follow the rules.

3. How often are data protection issues presented to your board? Do you think your board pays enough attention to data protection? If not, why so?

I think the fact that we still don't have a CPO is a big message. I think that board is not aware enough. You need some guts to take it up. But here they don't understand the importance of privacy. The other problem is also that privacy is more vague, more complex, compared to competition.

4. What is the main reason for implementing data controls?

The main reason to implement data privacy control is compliance. Then comes reputation. We also want to respect human rights and privacy is one of them. Not sure that everyone in the company would give the same answer, but this is at least my driving force.

5. What is your estimation of the total number of data privacy breaches faced by your company over the past year?

They have already experienced breaches, but not many. There are most probably some breaches that I don't even know about.

6. **Can you roughly estimate the total spend of your company on the privacy? Do you agree with the statement: *''The cost of data privacy will increase in the next year."*?**

At this moment insignificant. But it will change greatly! We need A LOT of resources, but I don't know if I get enough budget for it. So it's also a choice for a company. First years are a big investment – implementations, manuals, guidelines, trainings, … Privacy by design takes more time – It is necessary to negotiate IT contracts, especially during the course of contract. At this point in time not many investments, in fact just me who is working on privacy and I am not even allowed to do it full time (but I still do it as I am working more than required).

7. **Has your company already considered privacy reform? Opinion?**

We are not concerned about the regulation because our corporate binding rules are anticipating what is going to happen in the EU. That's also why we are doing them now.

I expected it to be enforced in 2015, but it will not be before 2017. The fact that there were European Parliament elections it was almost impossible to get the regulation further in process. There has to be some regulation, I'm convinced that there will be one.

From my company's perspective, I cannot agree the regulation is a good one, because there can be an extreme financial or administrative burden due to certain rules. Difficult to predict now…

8. **If your company has already considered the proposed rules, which are the burning issues in your opinion?**

The fines are on the top! 5% of global turnover is a huge money and it can be triggered in a company where there is no privacy law. So we need a global policy … I am absolutely convinced that only CBR may be a solution. De Brauw working group is working for us on BCR. More and more international companies are going on this path. More and more centralization of functions.

9. **How do you estimate the follwonig novelties in the proposed regulation?**

a) Data minimization

They start to grasp, but not there yet. We are sitting on way too much data. Practical example: HR are moving from one data base to another (personal performance). There is a law that this data should be deleted after 2 years. But if you have an employee that requires this data for 10 past years you need to give it to him. So in such a case it would be better to comply with law beforehand, so that you are not required to give the employee all the data. What would happen if all the employees in the firm ask for data? Retention guideline make sure that the HR is not sitting on data. Slowly the awareness is coming. You need a global policy (BSR).

b) Breach notification

72 hrs is almost impossible. Very difficult to get prompt information on breaches – and if not, you cannot inform authorities. If data processor is sitting on data breach and doesn't tell you, you are responsible but you don't even know.

c) Data portability

I never had had this issue. I cannot come up with an example.

d) Data by privacy

An enormous legacy but we have to do it – PIA formulars are now available for everyone, every system has to do it, to review. Every new system needs to be review in such way.
I discovered that many contracts are not compliant so constant repair actions.
You have thousands of systems and many of them do not include personal data but some of them do. And then a PIA should be triggered. This is responsibility of a data privacy officer. If tomorrow there is data protection authority knocking on our door and willing to do a dawn raid because they want to see how we are organize, the first thing they want to see is data privacy assessment. You need to have it in place!

Only in this way you can say for example – ok, this is a US company, processor, accessible from different servers (20 different non adequate countries) and it also has a sub/processor … And then you can make a business decision if we are taking this processor or another one. Microsoft and Oracle use standard contracts with the US interpretation of privacy laws. Almost in 100% this is not compliant with the EU laws! This means you have to negotiate fiercely. If you are in an initial phase you can go to another party, but if you have a stable relationship this is very difficult. So you need to do this triage, where the risk and the most data is and then start form there. And then make sure that all systems are OK. Task for privacy officers.

10. **How do you estimate the new regulation – personal opinion?**

It is good to have one consistent approach to privacy. Definitely there are issues that are developed behind a desk and not practically. But generally good… For the company high cost, but there's no other alternative.

If business is not costumer based (in chemicals for example privacy is not core business) it is much more difficult to raise awareness. In Vodafone for example different, everyone wants to be a data privacy officer there.

INTERVIEW, 4.6. 2014	
C orporate form of the company	Private
Scope of operation	Local
Total number of employees	4000
Annual revenue	50-500 mio
Industry	Healthcare

My function in the company is being the head of the department medical archives, since 1st April 2014 I am also privacy officer (but not yet official). I am still studying for it.

Im working on privacy only half of my working time. 50% of time I am archiving 3,5 milion of medical records (Aalkmar, Rotterdam, Limburh, Alphen al den Rijn) for minimum 15 years. BGBO is the law for privacy protection of medical records. This law says you have to keep it for so long. Not that much for children...

I spend 20 hours per week handling the requests for inspection in the medical records. 2 persons full time repsonsible for asnswering the questions of patients, giving copies of medical records, corrections or records ... When diffcult, they come to me. 800 requests per year. I also store the employees'data that come to me after they leave the company.

The mostly precessed data are personal data and employees data. They are both – processor and controller.

There are two laws BGBO (lex specialis – health data) and BGP. All the database needs to be sent to ministry of health. This is their duty. Reputation is important but not more important than law. Patients need to have trust in privacy.

In last year we didnt have breaches, a long time ago we had a breach.

Personnel is not a problem – everybody is aware. We have courses, workshops ... The problem is that a client does not only communicate with their hospital but also with other persons for example with his GP, lawyer ...

Privacy in last years also in ICT department (data protection) - tasks divided, cooperation necessary.

Costs compared to other departments are not that high, but will increase in next years.

I have been aware of the new regulation for 2 months. I spoke about the new regulation with the board. »Changes need to be done until January 2016.« He is now studying the rules. He knows about the DPO duty.

In general, he thinks the regulation is very good. People are not staying in Holland only. They are moving around the EU. Good that privacy rules are the same.