universität wien

MASTER THESIS

Titel der Master Thesis / Title of the Master‘s Thesis

„Network and Information Security in the Corporate Environment;

An Analysis of the Data Protection Legal Framework for Businesses in Europe“

verfasst von / submitted by

Panagiota Salasidou

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of

Master of Laws (LL.M.)

Wien, 2017 / Vienna 2017

Studienkennzahl lt. Studienblatt / Postgraduate programme code as it appears on the student record sheet:	A 992 548
Universitätslehrgang lt. Studienblatt / Postgraduate programme as it appears on the student record sheet:	Europäisches und Internationales Wirtschaftsrecht / European and International Business Law
Betreut von / Supervisor:	Prof. Dr. Dr. hc Peter Fischer

TABLE OF CONTENTS

List of Abbreviations

BCRs	Binding Corporate Rules
CJEU	Court of Justice of EU
DPA	Data Protection Authority
DPD	Data Protection Directive (Directive 95/46/EC)
DPO	Data Protection Officer
ECHR	European Convention of Human Rights
ECJ	European Court of Justice
EDPS	European Data Protection Supervisor
EU	European Union
EU/EEA	European Union/European Economic Area
GDPR	General Data Protection Regulation (Regulation (EU) 2016/679)
IT	Information Technology
NIST	The National Institute of Standards and Technology is the US Federal Agency that develops and promotes measurement, standards and technology.
OECD	Organisation for Economic Co-operation and Development
PETs	Privacy Enhancing Technologies
TFEU	Treaty of the Functioning of the European Union
WP 29	Working Party for the Protection of Individuals with Regard to the Processing of their Personal Data

Introduction

Early on from the formation of Europe as we know it today, the right to privacy was a principle upheld and underlined for its necessity, incorporated in the Convention for the Protection of Human Rights and Fundamental Freedoms as an axiom that lays the "foundation of justice and peace in the world"[1] in order for a democratic society to function effectively. The ECHR, which has been signed by all Member States of the EU stipulates in its art.8[2] that '*everyone has the right to respect for his private and family life, his home and his correspondence*' subject to certain restrictions.

This right was widely interpreted and confirmed by the European Court of Human Rights in cases like L.H. v. Latvia [3] where the Court found a violation of art. 8 of the ECHR based on the fact that the Latvian law did not limit the scope of collection of private data resulting in a retention of medical data spanning over 7 years. In other cases the Court found that where the domestic law allows the collection of personal data, these data should be safeguarded appropriately by efficient means that inhibit their misuse and abuse .[4]

In the 1980s the Organization for Economic Co-operation and Development, recognizing the ever growing importance and power of computer data processing and the consequences that such pervasive technologies would have in privacy matters for millions of people, issued the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data[5]. These Guidelines, even though non-binding and adopted only as a Recommendation of the OECD Council, have set the tone for the collection and management of personal information through automated means.

The basic principles of the OECD Guidelines as updated in 2013 and are still in place

---

[1] Convention for the Protection of Human Rights and Fundamental Freedoms (European convention on Human rights, as amended) (ECHR) [1950] , preamble
[2]ECHR [1950], art 8
[3] L.H. v. Latvia Ap no. 52019/07 (ECtHR , 29 April 2014)
[4] S.and Marper v. The United Kingdom no.30562/04 and 30566/04 (ECtHR, 4 December 2008)
[5] Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data[1980 as amended in 2013] OECD Council <http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm> accessed 8 March 2017

are the collection limitation principle[6], the data quality principle[7], the purpose specification principle[8], the use limitation principle[9], the security safeguards principle[10], the openness principle[11], the individual participation principle[12] and the accountability principle[13].

These principles have been in their majority introduced in other legislations issued by the European Commission and the rest of the members of the OECD (such as Canada and the U.S.) , once again underlining the fact that the development of automatic data processing has made it crucial for privacy protection laws in relation to personal data to tighten.

In 2007 the Treaty of the Functioning of the European Union came into effect, followed by the Charter of Fundamental Rights of the European Union. In art. 16 [14] of the TFEU and in art. 8 of the EU Charter of Fundamental Rights[15] , the right to data protection was formally turned into a separate fundamental right , distinct from the right to privacy. This development resulted in the necessary adoption of all Member States of the European Union which are also members of the TFEU and the Charter of Fundamental rights, of rules that constitutionally uphold the right of protection of personal data.

In view of all the aforementioned rules, it is evident that the protection of personal data is an issue much debated by all the European institutions that are fighting for the efficient realization of this protection.

Data protection, according to scholarly and legislative analysis of the definition, is an "informational self determination right"[16]. Specifically, data protection is considered

---

[6] ibid, art 7
[7] ibid, art 8
[8] ibid, art 9
[9] ibid, art 10
[10] ibid, art 11
[11] ibid, art 12
[12] ibid, art 13
[13] ibid, art 14
[14] Consolidated version of the Treaty on the Functioning of the European Union (TFEU) [2012] C326/47, art 16
[15] TFEU [2012] C326/47 , art 8
[16] Christopher Kuner, *European data protection law : corporate compliance and regulation* (2 edn, Oxford, Oxford Univ. Press, 2007) 3

to be a set of proceedings that have as their main purpose the safeguarding of the personal data of persons from unlawful or excessive processing (either computerized or manual).

These measures that are to be in place to prevent such damaging processing of information may be legal or non- legal (e.g. program security checks) and should embody the restrictions and admittances regarding the processing of personal data. The definition of processing of such data is under data protection laws so broad that it virtually includes any operations that can be performed on these data.

Businesses in Europe and worldwide have been struggling for years to comply with the data protection laws, given their complexity and the fact that they have to apply legislations of different jurisdictions that hold either a higher or a lower standard in safeguarding one's personal data. For European corporations or businesses that are operating in Europe , this confusion will vanquish to a certain degree, since the data protection reform promises companies to comply only with one pan-european data protection framework. In this sense, the necessary compliance of one business to the laws of multiple jurisdictions will be replaced by the compliance to only one legal act, thus reducing the administrative costs for many companies that are trying to access new markets. Moreover, a more solid data protection framework will generate more profits for corporations, given that consumers will have a clearer understanding of their rights concerning their personal data and how these are dealt with. In this way, consumers will be encouraged to use new products and services without having to think that they face a personal data risk in doing so.

Bearing in mind that the necessity for competitiveness is ever present in the corporate environment and given that the protection of personal data is a right that businesses ought to uphold in their commercial cycle, the new reform of EU legislation and the legal acts that are in place for transborder flows of personal data to third countries will allow the increase in profit and the entrance of new players into the globalized market.

In the chapters that follow, I will analyze the existing legal framework in data protection for EU corporations and for businesses that even if they are not located in the EU, they are dealing with data from European citizens and thus are bound by the

legislations that are voted by the Commission for the protection of the aforementioned individuals. In the course of the thesis, the options for risk management according to the established European legislative mechanisms will also be explored and how these options can render a business plan viable, resulting in the flourishing of the corporations and managing to keep it up-to-date with the advancements of technologies and the threats that arrive with these innovations. Lastly, the role of the Data Protection Officer will be presented and explained, a role that is perhaps the key enabler for the compliance to the new reformed legal framework.

1. Terminology in the data protection environment

As we have seen in the introduction, matters of privacy have troubled the European legislators who have done the outmost to protect this important principle of one's life by issuing legislations that guarantee the safeguarding of personal data for individuals and corporations. For this reason, definitions that were vital to the data protection landscape were developed and explained through statutes, court decisions and legal opinions by professionals in the field.

1.1. Information Security

One of the most important concepts concerning the matter of data protection and has been introduced in the legal world the past twenty years is that of information security. The concept of information security deals primarily with the preservation of three pillar principles: Confidentiality- Integrity- Availability. Such principles are to be upheld in the processing of data so as to ensure that information that has value to an organization or an individual can be protected from outside threats like stealing or tampering with one's personal data.[17] Especially for businesses, information security allows them to protect stored data which in turn enables these enterprises to ensure business continuity, maximize the return of investments – as the data will not be compromised and will be dealt exclusively by specific carriers- , engross business opportunities and minimize any business risk – amongst others, concerning the loss of trust by consumer's and clients. [18]

The term of information security embodies in itself the fortification of the corporate information systems and the protection of information -data- that a business is dealing with. In this sense, the corporate systems to be protected include amongst others computers, communication networks, storage media, software, firmware, services, and related resources that are used to acquire, store, process, manage, communicate and transmit data or information. On the other hand, the information to be protected includes a wide variety of data, for example personally identifiable information about

---

[17] Lukas Feiler, *Information security law in the EU and the U.S. : a risk-based assessment of regulatory policies* (Wien,Springer, 2011), 1

[18] Thomas J.Smedinghoff, *Information security law : the emerging standard for corporate compliance* (Ely, IT Governance Pub, 2008), 13

clients, employees , customers, business plans , e-mails and a wide variety of other data that are connected to the business activities and are linked to the reputation of the business and its capacity to generate profit . This kind of information can take all sorts of forms, from scriptum to digital e.g. videos, contracts, employee payrolls, business accounts etc.

The means used to ensure protection from threats concerning data are referred to as security controls. These controls can take many forms, from physical (eg. limited access to certain areas in the building where data is stored , like server rooms) to digital, for example antivirus systems, firewalls , encryption mechanisms , access authentication etc.[18]

Even though the above means are implemented to deter, detect and respond to threats, such security should not be interpreted as an absolute. In today's society with the technological knowledge of many individuals and organizations that might want to maliciously or benevolently collect data about oneself it is highly improbable that the information of a person can be absolutely sealed from third unauthorized parties. For this reason, it is material to note that it is not a matter of secured or unsecured data but rather a matter of degree that is best expressed in terms of risk.[19] In environments like these, where technology is galloping daily, the probability of a malicious third party to exploit vulnerabilities in the corporate systems and circumvent potential safeguards is ever present. Nevertheless, corporations have a general duty to provide security through any means available to them, that is going to be "reasonable" and "appropriate" to fight any external threat agent or technical failures that cannot be foreseen. This general duty burdens primarily the senior managers and the board of directors who have a legal obligation to implement all the above measures and train their employees in this endeavor. [20]

This general duty of corporations to uphold certain standards of security in dealing with personal data is an obligation mentioned in the DPD and generally applies to all companies in all industry sectors that possess personal information.

---

[18] Data Protection Commissioner, 'Data Security Guidance' <https://www.dataprotection.ie/docs/Data-security-guidance/1091.htm> accessed 6-7-2017
[19] Feiler (n 17) 2
[20] Smedinghoff (n 18) 39

In art. 17 [21]it is stated that the controller of data should implement practices and processes in order to ensure that that the data that are being dealt with are not being used or accessed by unauthorized individuals. [22] This requirement can be achieved through the creation of a security plan that will secure the preservation of the three pillar principles of Confidentiality, Availability and Integrity.

1.2. The Principles of Confidentiality, Integrity and Availability

1.2.1. Confidentiality

Confidentiality is the necessity for the protection of personal data from "unauthorized disclosure or access"[23] meaning the responsibility of the controller of data to implement authentication mechanisms that certificate the persons and devices that seek access to the information and access control to systems , networks and information. In doing so, the integrity and availability of the systems and the information that they store will be guaranteed.[24] While transforming the DPD into national law, certain countries in order to ensure a full protection from "unauthorized disclosure or access" have enriched their legislation with the obligatory implementation of Privacy Enhancing Technologies (PETs). Such countries like Germany and the Netherlands have included an article referring to PETs in their domestic laws regarding data protection. The concept of PETs aims at creating an environment where any unlawful use of personal data would be technically impossible to be achieved. Practically, this could be implemented through organizational and technical solutions eg. by using technologies that accomplish the largest possible use of truly anonymous data. Such enrichments to domestic legislation are greeted with pleasure, but the Commission considered it to be an excessive

---

[21] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive) [1995] *L 281 /31*, art 17

[22] Vijay Basani , '9 Important Elements to Corporate Data Security Policies that Protect Data Privacy' (*Security magazine*, 10 May 2016) <http://www.securitymagazine.com/articles/87113-important-elements-to-corporate-data-security-policies-that-protect-data-privacy> accessed on 6-5-2017

[23] Data Protection Directive [1995] *L 281 /31* , art 16

[24] Smedinghoff (n 18) 23

administrative burden for the controller of data who in any case bears the primary responsibility for the protection of the information he holds, and for this reason such a clause was not added to the Data Protection Directive.

1.2.2. Integrity

To define the principle of Integrity we have to make a distinction between system integrity and data integrity. When talking about system integrity, we are referring to the protection of systems from any external or internal threat agents that would compromise the accuracy, completeness and reliability of the stored data.[25] Thus in order for this principle to be upheld, mechanisms that protect the stored data from any alteration, must be implemented. On the other hand, data integrity means that the data that are stored in the corporate system are true and accurate concerning the data subject and have not been altered in any shape or form.

1.2.3. Availability

Lastly, when it comes to the third pillar, Availability, it is important to note that this principle encompasses the protection of data from "accidental or unlawful destruction or loss"[26]. The controller should give the possibility to the data subject to access and use all the information regarding him or her, in a way that is user-friendly and secure from any kind of tampering.

1.3. What Constitutes Personal Data?

The concept of "personal data" in the data protection landscape finds itself in the epicenter of all the legislative texts that have been issued on the matter. Its significance can be attributed to the fact that any concern for individual privacy stems from the definition of what constitutes personal data, the boundaries of the definition and how they can be safeguarded. The definition for personal data in the Data Protection Directive [27] and the GDPR [28] reads as follows:

---

[25] Smedinghoff (n 18) 23
[26] Data Protection Directive [1995] *L 281 /31* ,art 17
[27] Data Protection Directive [1995] *L 281 /31*, art 2 par. a
[28] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119/1, art 4 par.a

" 'personal data' shall mean any information relating to an identified or identifiable natural person ('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;"

This definition of personal data came into its final form after a proposal by the European Parliament to the Commission which opted for a very broad definition of personal data in order to cover all information which may be linked to an individual.[29] The necessity for an as wide coverage as possible derives as well from art.1 of the DPD that calls for the protection of fundamental rights of persons in relation to privacy and especially their personal data. Bearing this in mind, it is easier to implement the provisions of the legislative texts, especially in complicated situations where the data of individuals are not directly at risk, but could potentially be. Despite the broad definition of personal data, the legislators did not wish for an overreach of this protective umbrella to other legal domains. For this reason, many exemptions to the data protection laws have been set in place in order to restrict the spectrum of the application of data protection laws.[30]

1.4. Processing of Personal Data

A second definition that comes hand in hand with the term of personal data and completes the reasons why data protection laws come into place is that of "processing". The terminology for 'processing', as is the case with 'personal data', is purposely kept very wide to basically signify any kind of dealing with information that is acquired by the controller- corporation. Due to this fact, even in the process of e- commerce, the mere storage of personal data constitutes data processing.[31]

---

[29] Opinion 4/2007of the Working Party 29 on the concept of personal data [20 June 2007] 01248/07/EN , WP 136

[30] Such exemptions can be located in Data Protection Diretive and cover amongst others personal data that deal with operations that fall strictly into the domestic law regulations (public policy, defence etc.) (Data Protection Directive [1995] *L 281 /31*, art 3)

[31] Kuner (n 16) 74

The definition for processing of personal data can be located in the Data Protection Directive and the new GDPR [32,33] that will come into force in 2018 and reads as follows:

"'processing of personal data' ('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;"

Since the processing of personal data covers like an umbrella all the individual situations where handling of information occurs, it is often up to the national courts to decide not only if a specific action constitutes processing but if it is also in correlation to personal data. For this reason in cases like Tietosuojavaltuutettu v Satakunnan Markkinaporssi Oy and Satamedia Oy (Satamedia) the Court of Justice found that even the dealing with data from documents that were considered to be in the public domain constituted processing and therefore it was up to the national judge to determine whether or not these data were acquired lawfully and appropriately in respect to the individual's personal rights.[34] Furthermore, this ruling from the Court of Justice underlines the fact that data protection law is applicable only in cases when 'personal data' are processed. Thus when it comes to public information, data protection laws and their special provisions for the handling of personal data do not apply .[35]

Last but not least, it is important to point out that the processing of personal data should take place in a lawful and fair manner. These two rules translate to the fact that the processing should take place in a way that does not have unjustified adverse effects on the individuals concerned and that it should be according to the national and European legal barriers. The new Regulation (GDPR) adds to the mix that the data should be also processed in a transparent manner, meaning the controller should disclose to the data subject how he or she intends to use the data and give individuals

---

[32] Data Protection Directive [1995] *OJ L 281 /31*, art 2 par.b
[33] General Data Protection Regulation, [2016] *OJ L 119/1*, art 4 par.2
[34] Rebecca Wong , 'The Data Protection Directive 95/46/EC: Idealisms and realisms'[2002] Vol. 26(2-3) International Review of Law, Computers & Technology, Routledge, 229-244
[35] Kuner (n 16) 98

appropriate, timely and accurate privacy notices when collecting their personal data.[36]

1.5 Actors in the Data Protection Environment

The complexity of the environment under which data processing takes place and the constant organizational shifts caused by technological developments increase the need for a broader definition of the actors that participate in the data protection scenery. Definitions for these participants need not only be accurate but also broad enough, the reason being that in this way it will be possible to determine who is required to be in compliance under the legal frameworks concerning data protection, who benefits from such compliance and against whom should data be protected. The partakers in this environment stretch from communication services providers[37] to software manufacturers and from businesses in their capacity as personal information controllers to the customers/governments that make use of services of businesses.[38] The DPD and the GDPR give block definitions for the actors in data protection so as to ensure a coverage as wide as possible for the protection of the data subjects from malicious actors during the process of their data by the aforementioned enmeshed.

1.5.1. Data Controllers

Data controllers are related to activities which reflect the life cycle of information from its collection to its destruction. They are the ones who dictate the purposes of the data processing and give instructions on why, how and under which conditions data should be processed. The DPD[39] definition for data controllers, which is repeated in the GDPR[40] , reads that:

"...'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are

---

[36] General Data Protection Regulation, [2016] *OJ L 119/1* art. 5 par. 1a
[37] Communication services providers are the internet access providers, the internet backbone providers and providers that operate the public switched telephone network. The list is non-exhaustive.
[38] Feiler (n.17) 19
[39] Data Protection Directive [1995] *OJ L 281 /31*, art 2 par.d
[40] General Data Protection Regulation, [2016] *OJ L 119/1* , art 4 par. 7

determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;…"

Controllers have protection obligations and carry liability against any destruction or loss of data that might occur while under their supervision.[41] Security obligations are directly applicable to the controller who is responsible to notify the data subjects and authorities in cases of security breaches.

1.5.2. Data Processors

Data processors are separate legal entities with respect to the controller, processing personal data on his behalf and for his interest.[42] In the definition given under the DPD data processors are described as:

''…a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;…''[43]

Under the DPD data processors have a severely reduced role in comparison to that of data controllers since they do not carry liability for data protection to the extent that a data controller does.[44] However, this will change after the implementation of the GDPR as the Commission has chosen to strengthen the controlling instances for processors by holding them responsible to the same standard as controllers concerning the protection in handling information.[45]

This step to the direction of assumption of liability by processors comes in a time where the advancements in technology have blurred the lines between the controllers and processors and translates to a necessity for the modern technological era. So far, controllers had the sole responsibility for the handling of data, but with relationships

---

[41] Elizabeth Kennedy; Millard Christopher 'Data security and multi-factor authentication: Analysis of requirements under EU law and in selected EU Member States' [2016] Vol.32 (1) Computer Law & Security Review: The International Journal of Technology Law and Practice, 91-110 (Multi-factor authentication)
[42] Opinion 1/2010 of the Working Party 29 on the concepts of "controllers'' and "processors" personal data [16 February 2010] 00264/10/EN ,WP 169
[43] Data Protection Directive [1995]*OJ* L 281 /31 ,art 2 par.e
[44] Kuner (n 16) 69
[45] Paul de Hert; Vagelis Papakonstantinou, 'The new General Data Protection Regulation: Still a sound system for the protection of individuals?' [2016] Vol.32 (2) Computer Law & Security Review: The International Journal of Technology Law and Practice, 179-194 (GDPR: A Sound System)

between them and processors becoming increasingly intertwined, a clause for the responsibility of processors in regards to the processing of personal data is welcomed.

An example of such an occurrence would be an Internet Service Provider (ISP) which provides for hosting services is considered to be a processor for data which are published online by its customers. This processing however comes often hand in hand with storing of the data disclosed. Such data can later on be re-used by the ISP in other operations, thus turning him into controller. With acknowledging the same standard of liability for controllers and processors, the new legal framework ensures for a more stable and secure environment in the data protection landscape, which will translate in higher customers' trust.

1.5.3. Data Subjects

Data subjects are considered to be the customers, governments, other corporate entities etc., whose personal data are being handled by the aforementioned data actors. Data protection laws are established to secure that data subjects' rights are being upheld and that they are protected against any unlawful or negligent disclosure. Under the GDPR, data subject's rights are being enforced due to the fact that the reformed framework takes into consideration the online environment and genetic/biometric data and since the identification that is required by law need not only be by the data controller but also by whichever other entity has access to the personal data of the data subject.

1.5.4. Threats in Data Protection Environment

During the processing of data, there are a number of threats that can hinder the unobstructed outcome of the process. These threats are either external or internal. External threats can be the ones that derive from malicious actors like hacking, cyber attacks to the corporate database, breach of security and disclosure of personal data etc. Internal threats can be caused not only maliciously but due to neglect in the corporate security systems, lack of training which can result in the improper handling of data by the employees etc.

Threats, either internal or external have one thing in common: the destruction, tampering or loss of one of the company's most essential asset, information. For this

reason, it is of paramount importance for corporations to take any kind of security and operational measure to counterattack them and safeguard the data according to applicable legislation.

2. Overview of the Legal Framework Concerning Data Protection In Europe

The decision making instruments of the EU, keeping in mind the necessity for the protection of personal data of its citizens and the uniform application of law, have made a political decision on the reform of the data protection rules, which would create a simple framework of protection for individuals and return of profits for businesses that operate within the borders of EU. This reform which is set to come into force in May 2018 [46] is highly anticipated given the fact that it will enable citizens to gain back control of their personal data and create numerous benefits and opportunities for enterprises, estimating that the new rules to be set will create benefits of 2.3 billion a year [47].

The replacement of the entirety of data edifice is crucial given the galloping developments of technology in recent years which translates into vast amounts of personal data transfers. The new rules that have been proposed by the European Commission and already been voted are the GDPR [48] and the new Directive for the processing of personal data by competent authorities[49]. While both legislations are salient for the completion of the data protection landscape, the reach of the Directive is beyond the scope of this thesis, given that it predominantly deals with the *"...process of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security..."* as stated in art. 1 par. 1 .

---

[46] European Commission, 'Protection of Personal Data' <http://ec.europa.eu/justice/data-protection/> accessed on 23 April 2017

[47] European Commission , 'What benefits for businesses in Europe' (Data Protection Reform Factsheets, 16 January 2017) <http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=52404> accessed on 23 April 2017

[48] General Data Protection Regulation, [2016] *OJ L 119/1*

[49] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] *OJ L 119/89*

Due to the fact that it does not apply directly to the process of personal data by enterprises in the process of their business activity, it is considered to be – despite its importance to the data protection scenery- irrelevant to the scope of this paper. The same holds for the E-privacy Directive which safeguards the privacy of individuals in the electronic communications sector and the free movement of such data[50] – texts, e-mails, calls etc. Given that the E –privacy Directive has a very limited scope of protection, the rules that it sets forward would be a subject of a thesis that focuses primarily on the communications sector and is considered to be beyond the scope of this paper.

2.1. The General Data Protection Regulation [51]

One of the most important legal acts that the European Commission has voted upon following the much needed reform of the data protection legislation is the GDPR that shall apply across all Member States of the European Union from 25th of May 2018. This legislative text creates high expectations for the millions of individuals and undertakings across Europe, being viewed as the key enabler of the Digital Single Market. Since this legal act is voted as a Regulation, it translates to the fact that it will be directly binding for all Member States and directly applicable for them, without the need for a national law that would transpose it into its domestic legal jurisdiction. In this way, the 28 different domestic legislations that are in place will be replaced by one uniform law.

2.2. The Data Protection Directive [52]

Until the GDPR comes into force, the primary tool concerning data protection is the DPD that applies across Europe for the past 20 years. The amendment process for the DPD started in 2009 and resulted in the 2012 comprehensive Commission Proposal for the reform of the data protection rules in the EU. [53]

---

[50] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] *OJ L201/37*, art 1 par.1
[51] General Data Protection Regulation, [2016] *OJ L 119/1*
[52] Data Protection Directive [1995] *OJ L281 /31*
[53] European Commission, ' Protection of Personal Data' <http://ec.europa.eu/justice/data-protection/ > accessed on 10 June 2017

The significance of this Directive can be derived from the fact that by now it has become the international data protection metric against which data protection adequacy is measured. The preamble reads that the necessity for this legal act stems from the ever increasing exchange of personal data between undertakings in different Member States and in this way the removal of obstacles of flows of such data will be easier to be achieved, safeguarding at the same time an appropriate level of protection of rights and freedoms.[54]

Until May 2003 , when the first official report by the Commission on the progress of the implementation of the Data Protection Directive came out, many countries where still reluctant on the adoption of rules that would comply with the Directive. [55] However the increasing need to strengthen the regulatory environment on data protection quickly dispersed these doubts and slowly the entirety of the European Member States adopted national rules in accordance with the Commission's text.

2.3. Legal Frameworks for Data Transfers to Third Countries Outside the EU/EEA Area

The instruments of the European Union have done the outmost to protect data transfers that take place within the borders of the EU, from Member State to Member State. At the same time however they have provided for the adoption of legal frameworks that allows the regulated flow of such data to third parties outside the EU. Such legal acts are the ones to follow.

2.3.1. The Privacy Shield Program [56]

The EU-U.S. Privacy Shield and Swiss –U.S. Privacy Shield Framework, which has been designed by the U.S. Department of Commerce, the European Commission and the Swiss Administration has been deemed adequate on July 1st ,2016 by the European Commission and on January 12th, 2017 by the Swiss Government to enable data

[54] Data Protection Directive [1995] *OJ L 281 /31* , preamble 5-8

[55] Stephen Saxby, 'Data protection directive gets its first progress report', [2003] Vol 19 (4), Computer Law & Security Report,271 ,< http://www-sciencedirect-com.uaccess.univie.ac.at/science/article/pii/S0267364903004011?via%3Dihub> accessed 15 May 2017

[56] European Commission, 'The EU-U.S. Privacy Shield', <http://ec.europa.eu/justice/data-protection/international-transfers/eu-us-privacy-shield/index_en.htm> accessed on 5 March 2017

transfers under EU law and Swiss Law.[57]

The framework provides a mechanism for companies on both sides of the Atlantic to which they can adhere to in their effort to achieve maximum data protection requirements when transferring personal data from EU or Switzerland to the U.S. This framework allows all the involved parties that partake in such data transfers to clarify the legal requirements in transatlantic data flows. As the Commissioner for Justice, Consumers and Gender Equality Vera Jourova eloquently said, the Privacy Shield Framework *"...brings stronger protection standards that are better enforced, safeguards on government access and easier redress for individuals in case of complaints…"*.[58]

2.3.2. Adequacy Decisions [59]

For data transfers to third countries outside of the EU where no particular framework has been set in place, the Data Protection Directive provides in its art.25 [60] a solution by giving the power to the Commission to issue 'adequacy decisions' for data transfers to third countries. These adequacy decisions contain an insurance that the third country to which personal data from EU are to be transferred, cater for an adequate level of protection by reason to its domestic law or of the international commitments it has entered into. Some of the countries that have been so far recognized to provide for an adequate level of protection are Andorra, Argentina, Canada (commercial organizations), Faeroe Islands, Guernsey, Israel , Isle of Man, Jersey, New Zealand, Switzerland and Uruguay. [61] In 2017 , talks between Haruhi Kumazawa, Commissioner of the Personal Information Protection Commission of Japan and Vera Jourova EU Commissioner for Justice, Consumers and Gender Equality of the European Commission have advanced in an effort of the Commission to reach an 'adequacy

---

[57] International Trade Administration U.S. Department of Commerce, 'Privacy Shield Overview', <https://www.privacyshield.gov/Program-Overview> accessed on 6 May 2017

[58] European Commission, 'European Commission launches EU-U.S. Privacy Shield: stronger protection for transatlantic data flows' [12 July 2016] IP/16/2461 (Press Release) < http://europa.eu/rapid/press-release_IP-16-2461_en.htm > accessed on 6 May 2017

[59] European Commission 'Commission decisions on the adequacy of the protection of personal data in third countries' < http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm > accessed on 6 May 2017

[60] Data Protection Directive [1995] *OJ L 281 /31* , art 25 par.6

[61] Commission ' Adequacy Decisions' (n 59)

decision' with Japan in a view to promote the same standards of data protection as a fundamental right.[62]

2.3.3. Binding Corporate Rules[63] & Model Contractual Clauses [64]

Many multinational and domestic corporations have chosen in order to enforce their data protection internal framework to adopt additional rules of conduct. Such rules are the 'Binding Corporate Rules' and the 'Model Contracts for the Transfer of Personal Data to third countries'. BCRs are used by multinational companies and are internal rules of procedure – much like a Code of Conduct- that adduce appropriate and sufficient safeguards for the transfer of data to the member of a group of the multinational company. [65] On the other hand, Model Contracts are standard contractual clauses that can be decided if they are sufficient to safeguard the transfers of personal data from corporation to corporation that have signed the (sic) contract that entails provision for data protection. The Commission decides on the sufficiency of such contracts and has issued so far two sets of standard contractual clauses for transfers from data controllers to data controllers and one set for the transfers to processors established outside the EU/EEA.[66] This procedure is based upon Art. 26 par. 2 of the Data Protection Directive [67] , enables the adoption of such model clauses but does not prohibit the addition of more clauses concerning data protection as long as they do not contradict the initial standard clauses that are issued by the Commission.

The importance of data protection and the complexity for it to be achieved is

---

[62] European Commission 'Joint statement by Commissioner Věra Jourová and Haruhi Kumazawa, Commissioner of the Personal Information Protection Commission of Japan on the state of play of the dialogue on data protection' [4 July 2017] STATEMENT/17/1880 (Statement) <http://europa.eu/rapid/press-release_STATEMENT-17-1880_en.htm> accessed on 10 July 2017

[63] European Commission 'Overview on Binding Corporate Rules' < http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/index_en.htm > accessed on 6 May 2017

[64] European Commission, ' Model Contracts for the transfer of personal data to third countries' <http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm> accessed on 15 July 2017

[65] Commission, 'Binding Corporate Rules' (n 63)

[66] Commission, 'Model Contracts' (n 64)

[67] Data Protection Directive [1995] *OJ L 281 /31,* art 26 par. 2

showcased by the fact that all the above legal frameworks are trying to cover the new developments that arise in the process of transfer of personal data and create a secure environment for these activities to flourish. For transfers between Member States the central pillars for the granting of this protection is the DPD and the GDPR, while for transfers to third countries other legal frameworks like the BCRs , Model Contractual Clauses, Adequacy Decisions and the Privacy Shield , are used to a great extent in order to create the necessary adequacy standard based upon which data can be securely transferred.

3. Comparative Analysis of the Data Protection Directive and the General Data Protection Regulation

The Data Protection Directive has been the key instrument for data protection in the EU and an example to the protection of flows of personal data globally for the past 20 years. With the galloping evolution of new technologies, the European legislators sensed the need for a change and strengthening of the data protection rules, thus on the 24th of July 2014 the trilogues between the Council , the Commission and the Parliament initiated in order to achieve an agreement on the new legal act for the protection of personal data, the GDPR.[68] Under the new legal framework, the businesses will have clearer responsibilities and will be able to comply with the new rules and avoid penalties in doing so. This satisfactory development comes as a relief to many multinational corporations that under the Data Protection Directive had to comply with the national jurisdictions of many Member States, which transposed the legal act into domestic legislation, often deciding on its implementation with rules stricter than the ones set out in the Data Protection Directive.

The two texts (the DPD and the GDPR) have many things in common, with many parts of their body being identical and many definitions remaining the same. Nevertheless, the new GDPR[69] adds a handful of new rights and responsibilities for the data actors, along with some new innovations that the previous legal act did not incorporate. In the paragraphs that follow, the two texts will be examined side by side and the changes to the data protection landscape under the GDPR will be emphasized.

In both the DPD and the GDPR , the scope of protection remains the same with that being that the GDPR in succeeding the DPD has as its objective the protection of the right to privacy with respect to the processing of personal data.[70] Concerning which law applies in each member state however, there is a differentiation given the legislative way in which these frameworks have been voted. In the DPD , the law that applies in

---

[68] Kennedy; Millard 'Multi-factor authentication' (n 41)
[69] General Data Protection Regulation, [2016] *OJ L 119/1*
[70] See Data Protection Directive [1995]*OJ L 281 /31* , art1 in comparison with General Data Protection Regulation, [2016] *OJ L 119/1*, art 1
[71] Data Protection Directive [1995] *OJ L 281 /31* , art 4

the Member States is considered to be the law that governs the Member State where the establishment is located , after the transposition of the DPD to domestic rules.[71] The GDPR being voted as a Regulation does not demand such transposition, but ensures the uniform applicability of its legal text across all Member States of the EU.[72]

Concerning the purpose limitation of the data processing, the DPD has set certain principles according to which personal data of the data subject can be processed. These principles are found in art. 6 of the DPD[73] and have regard the fair, lawful and in a specified manner processing. To this end, the GDPR goes one step forward and adds the term 'transparent' in the way that such data can be handled[74]. This essentially means that the new Regulation obligates the processors and data controllers to allow the data subject a full picture of the way their data are being used, in order to achieve a higher level of control over them.

Furthermore, the DPD sets forward the need for data minimization in the gathering of the data, which is interpreted in that the data that are processed should be adequate, relevant and in correlation with the purposes of the collection. The data minimization principle encapsulates the idea that subject to limited expectations, the corporation gathering the data should only process personal information that needs to process in order to achieve the aim for which the data are being collected.[75] The data minimization principle is being repeated in the GDPR , but is also enriched with a more restrictive obligation, so as the gathering of data will be limited only to what is necessary for the specific processing.[76] Whilst there are some additions to the aforementioned principles, the accuracy principle for the data to be as close to the truth and accurate as possible remains the same in both legal texts.[77]

When it comes to the data retention periods the DPD reads as follows:

---

[72] General Data Protection Regulation, [2016] *OJ L 119/1* , art 3
[73] Data Protection Directive [1995] *OJ L 281 /31* , art 6
[74] General Data Protection Regulation, [2016] *OJ L 119/1*, art 5 par.1 a
[75] Detlev Gabel; Tim Hickman, ' Chapter 6: Data Protection Principles- Unlocking the EU General Data Protection Regulation' (*White & Case*, 22 July 2016) <https://www.whitecase.com/publications/article/chapter-6-data-protection-principles-unlocking-eu-general-data-protection#> accessed on 22 June 2017
[76] General Data Protection Regulation, [2016] *OJ L 119/1* , art. 5 par.1c
[77] See Data Protection Directive [1995] *OJ L 281 /31* , art 6 par.1 c in comparison with General Data Protection Regulation, [2016] *OJ L 119/1*, art 5 par.1 d

"Members States shall provide that personal data are….. 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 shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use." [78]

The GDPR introduces two important new factors to the data retention periods. The first is that in cases where the processing of personal data takes place for historical, statistical or scientific purposes or in concern to the public interest, then the retention period can be longer than the usual.[79] The second is the introduction of the 'right to be forgotten'[80] which enables the data subject to request for an erasure of their personal data sooner than the end of the maximum retention period. This right has been recognized by the ECJ on one of its infamous decisions of Google v Gosteja [81], where the plaintiff requested the erasure of his data concerning his past dealings from the Google search engine, given that they damaged his reputation and were irrelevant to his present conduct of business. The ECJ granted Mr. Costeja his request for erasure , thus recognizing officially the time limitations and relevance of data during processing, and raising the 'right to be forgotten' to a principle that has been sought after ever since by many individuals wanting to erase their presence from the Google Search engine, subject to certain restrictions.

When it comes to the territorial application of the aforementioned legislative texts , the DPD has a more limited scope than the one in GDPR. The DPD rules state that if an establishment is located in a Member State of the EU or at least has a processor in an EU Member State then the data protection principles in accordance with the DPD apply.[82] The GDPR repeats these provisions and furthermore adds that even if a corporation provides only goods or services to EU citizens, or monitors their behavior then it is subject to full compliance under the EU data protection legislation.[83]

---

[78] Data Protection Directive [1995] *OJ* L 281 /31, art 6 par. 1 e
[79] Data Protection Directive [1995] *OJ* L 281 /31, art. 6 par 1 e
[80] General Data Protection Regulation, [2016] OJ L 119/1 , art.17
[81] C-131/12 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014] ECLI:EU:C:2014:317
[82] Data Protection Directive [1995] *OJ* L 281 /31, art. 4
[83] General Data Protection Regulation, [2016] *OJ L 119/1*, art. 3 par.2 a

In any case, organizations operating in the EU or with EU affiliates should be ready to implement the new data protection principles. If they fail to do so, processing of personal data under their supervision will be deemed unlawful and it is irrelevant to which sector of the industry these businesses operate in, since all types of corporations are affected. At this point it is important to note that mere website accessibility,with a third- country processor, does not trigger the implementation of the GDPR.[84]

One of the legal basis upon which data processing can take place is consent. Consent has a central role in the data protection environment as it allows the data subject to make an 'informed decision' upon which data will be processed and if he wishes for such processing to occur.[85] In the DPD, consent plays a central role to the processing of personal data [86], whereas the GDPR[87] enriches the meaning of consent with requirements of 'explicit consent', so as to avoid unambiguous consent. Moreover, if consent is given in a standard clauses form, it should be discernable from the rest of the text, easily accessible and in a plain and clear language, whereas if it is included in an electronic form, the consent checkbox should be unchecked. One topic that the GDPR does not clarify concerns the age of the child according to which it can freely give consent. Whereas, it is stated[88] that the child is eligible to freely give its consent at the age of 16, the GDPR allows for derogations from this principle to a lower age, as decided by each Member State. Despite the fact that this lowering of the base age of 16 cannot be under 13 years old, the GDPR creates an unambiguous environment and a non-uniform application across Member States for the enforcement of this rule.

The DPD makes a differentiation between personal data and sensitive personal data, prohibiting completely the processing of the latter, subject to certain exceptions. Such data are information that reveal a person's ethnic origin or social group, religion, race, political views, membership to trade unions and philosophical beliefs.[89] Sensitive data

---

[84] Detlev Gabel; Tim Hickman, 'Chapter 4: Territorial application – Unlocking the EU General Data Protection Regulation' (*White & Case*, 22 July 2016) <https://www.whitecase.com/publications/article/chapter-6-data-protection-principles-unlocking-eu-general-data-protection#> accessed on 22 June 2017

[85] de Hert; Papakonstantinou 'GDPR: A Sound System' (n 45)

[86] Data Protection Directive [1995] OJ *L 281 /31* ,art 7

[87] General Data Protection Regulation, [2016] *OJ L 119/1* , art 7

[88] General Data Protection Regulation, [2016] *OJ L 119/1* , art. 8

[89] Data Protection Directive [1995] *OJ L 281 /31* , art 8

should be held to a higher degree of protection given their nature , an opinion which was supported by a ruling of the European Court of Human Rights that found that domestic law should not only afford legislative protection for privacy according to the DPD but also take the appropriate measures to reinforce the security levels for access to sensitive personal data applied in a strict and sufficient way.[90] The reformed framework[91] expands the definition of sensitive personal data and incorporates the 'genetic data' , 'biometric data for the purpose of uniquely identifying a natural person' and the 'data concerning health'. This choice to include data concerning the health sector seems to some theorists to be inexplicable, given that the GDPR is a wider framework and in any case should avoid being seen as a specialized legislation, as in the electronic communications field.[92]

On a different note, both of the above legal acts uphold certain principles to be protected in the process of personal data. In DPD , principles like the necessary disclosure of the controller or representative , the right of access to the data of the data subject by the controller, the right to object to the processing of the data by the data subject and the right to confidentiality of the processing are being raised to primary rules upon the handling of the above information.[93] On the other hand, the GDPR repeats the aforementioned rights and elaborates on others like the right to restriction of processing under certain conditions[94], the right to be forgotten – as analyzed in previous paragraphs - and the right to data portability[96] . The right to data portability has two sections, the first being the right to copy the data from a data controller and the second to transfer it to another data controller. A prime example of such an endeavor would be the Google Takeout, which allows social media users to download their profile data that they have inserted in Google's social networking site Google ++ in various forms and

[90] Jari Raman 'European Court of Human Rights: Failure to take effective information security measures to protect sensitive personal data violates right to privacy – I v. Finland, no. 20511/03, 17 July 2008' [2008] Vol.24(6), Computer Law and Security Review: The International Journal of Technology and Practice,562-564
[91] General Data Protection Regulation, [2016] *OJ L 119/1* , art 9 par.1
[92] de Hert; Papakonstantinou 'GDPR: A Sound System' (n 45)
[93] Data Protection Directive [1995] *L 281 /31* ,art. 11-12,14, 16
[94] General Data Protection Regulation, [2016] *OJ L 119/1* ,art 18
[95] General Data Protection Regulation, [2016] *OJ L 119/1* , art.17
[96] General Data Protection Regulation, [2016] *OJ L 119/1* ,art 20

insert them into other internet services.[97]

In order to observe the application of the DPD across all EU Member States, the Commission obligated the Member States to establish a domestic supervisory authority that would monitor the implementation of the rules for data protection. The Commission underlined the necessity for independence of these authorities from any other organization in order to succeed the best possible outcome in the course of the supervisory authority's activities.[98] The so called Data Protection Authorities (DPAs) have the power to investigate the course of business of corporations, to verify their compliance to the data protection rules and engage in legal proceedings when they locate any violation to the DPD. In order for the DPAs to commit to their duties, the controllers have the obligation to notify them before any activity of processing of personal data takes place.[99] The notification should include as stated in the DPD in a non-exclusive list the name and address of controller, the purpose of the processing , a description of the categories of data that are to be processed , the recipients to whom the data will be disclosed and a general description of the measures taken by the controller to secure the information that is being handled.[100] The notification principle, as described above, is mandated in other international legislations as well , like the U.S. Privacy Act, after the formation of a subcommittee from 1970 to 1974 that found that the existence, preservation and operation of data banks *"...should be put on a statutory basis with full and accurate reporting requirements, inherent privacy safeguards, subject to notification…"*.[101] To that end, the principle of notification of the controller when processing personal data was not an innovative notion, but a central one concerning the efficient vigilance in data protection.

In order to assist the work of the DPAs, the DPD provides for the creation of the WP 29 [102] that is composed of a representative of the supervisory authority

---

[97] Inge Graef and others 'Putting the Right to Data Portability into a Competition Law Perspective' [2013] Vol. Annual Review, The Journal of the Higher School of Economics, 53-63
[98] Data Protection Directive [1995] *OJ L 281 /31* , art 28
[99] Data Protection Directive [1995] *OJ L 281 /31* , art 18
[100] Data Protection Directive [1995] *OJ L 281 /31* , art 19
[101] Collin J. Bennet , *Regulating Privacy, Data Protection and Public Policy in Europe and the United States*, (Cornell University Press,1992) 69
[102] Data Protection Directive [1995] *OJ L 281 /31*, art 29

designated by each EU country, a representative of the authority ,established for the EU institutions and bodies and a representative of the European Commission.[103] The main responsibilities of the WP 29 is to provide the European Commission with opinions concerning data protection matters and help develop harmonized policies in collaboration with the domestic DPAs.[104]

The highlights of the GDPR include certain innovations that the DPD was lacking. The procedures according to which processing of personal data takes place are simplified since the enforcement of data protection rules will be supervised only by the national DPAs[105] , since the Commission is stripped of its enforcement authorities. Moreover, WP 29 will be replaced by the European Data Protection Board that will be designated to settle disputes only between the domestic DPAs[106] and issue opinions on matters concerning data protection. Moreover, under the GDPR the general notification requirements are abolished, thus enabling business activities to take place in a faster pace. Prior consultation and authorization requirements will concern only high risk processing of personal data, whereas it still remains a necessity to notify the supervisory authority in cases of security breach.[107]

A certain improvement of the GDPR in comparison to the DPD is the clear distinction between the controller and the processors, combined with the fact that the GDPR holds both these actors in data protection to a very high standard of compliance to the legislation concerning the security of personal data and their responsibilities to achieve such security. Due to this additions in GDPR, the controller is not the only one responsible to uphold a certain level of guarantees during the process, but the same burden falls upon the processor as well, providing for a multifaceted protection.[108] The negligence to uphold these responsibilities by the aforementioned data actors bare high fines and administrative fees as they are adjusted in the GDPR[109] , fines which the

---

[103] European Commission 'Article 29 Working Party'< http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083 > accessed on 5 May 2017
[104] European Data Protection Supervisor 'Article 29 Working Party' para 4 <https://edps.europa.eu/node/3095%23articlewp_en >accessed on 5 May 2017
[105] General Data Protection Regulation, [2016] *OJ L 119/1* , art 51
[106] General Data Protection Regulation, [2016] *OJ L 119/1*, art.63-65, 68
[107] General Data Protection Regulation, [2016] *OJ L 119/1* , art 33
[108] General Data Protection Regulation, [2016] *OJ L 119/1*, art 24, 28- 29
[109] General Data Protection Regulation, [2016] *OJ L 119/1*, art 82- 83

Commission found suitable for non-compliance to the rules that it laid down in order to deter the implementation of unsuitable security in the processing of personal data.

Furthermore, the GDPR makes a distinction in the security measures taken by businesses concerning data protection, separating to data protection by design and data protection by default.[110] While the legislation is not perfectly clear upon which technical measures should be taken for such security to be achieved, data protection by design means that an organization has to show that they have adequately security in place and that compliance is monitored, meaning that IT departments should take into consideration privacy matters during the course of business activities. On the other hand, data translation by default means that when a new costumer acquires a product or service, the strictest privacy settings should apply directly on them and no manual change to the privacy settings should occur from the part of the customer in order for them to have a wider coverage in privacy.[111]

Last but not least , the GDPR requires for the obligatory appointment of a Data Protection Officer where, amongst others, the activities of the business have to do amongst others with the processing of personal data and are in need of regular and systematic monitoring and in cases where such businesses handle sensitive information about one's person.[112] Under German law, this obligation existed prior to the voting of the GDPR and for this reason the appointment of the DPO is not a new development. However, the obligatory nature of this clause under the GDPR dictates for the appointment of a DPO who will be an independent supervisor to company's activities and if they comply with the GDPR , supervising and monitoring the course of business and the handling of personal data.[113]

It is important to note that the DPD has ruled the data protection scenery for the past 20 years. Its text has been tested in the course of time and its significance and

---

[110] General Data Protection Regulation, [2016] *OJ L 119/1* , art 25
[111] EU Data Protection Regulation 'Data Protection by Design and by Default' <http://www.eudataprotectionregulation.com/data-protection-design-by-default > accessed on 7 May 2017
[112] General Data Protection Regulation, [2016] *OJ L 119/1* , art. 37-39
[113] Paul Voigt 'The compliance burden under the GDPR – Data Protection Officers' (Taylor Wessing,September 2016) < https://www.taylorwessing.com/globaldatahub/article-compliance-burden-under-gdpr-data-protection-officers.html > accessed on 10 July 2017

foresight made it a valuable tool for data protection not only in Europe but also globally. It has created a standard for data transfers and a soft law for third countries who can follow its provisions in the drafting of their domestic legislation.

However, the rapid advancements of technology and the new needs that arise in this field quickly brought out the deficiencies of the DPD. For this reason, the reform of the data protection scenery with the GDPR is viewed with much excitement for the innovations that it brings, as presented in previous paragraphs, but also with some skepticism on whether or not its implementations will enable greater security for data subjects and more flexibility for companies to operate with clearer rules and little need for intervention to the circle of their business activities.

4. Analysis on the Legal Frameworks for Data Transfers to Third Countries Outside the EU/EEA Area

Internationalization and globalization have had a very large impact on data protection law. The increasing commercial value of the processing of personal data comes hand in hand with the necessity for abolishment of national legal borders. Although globalization complicates the maintenance of appropriate legal requirements, the Commission foreseeing these technological developments and legal issues that might arise, proceeded in the adoption of a series of frameworks that would enable the secure transfer and processing of personal data to third countries.

4.1. Data Transfers to Third Countries under the Data Protection Directive and the General Data Protection Regulation

The primary legal act that enables the safe data transfer from the EU/EEA area to third countries is the DPD. According to its provisions, in Chapter IV of the DPD it reads that any data transfer to third country outside the EU is prohibited unless adequate protection was shown for the transfer.[114] This adequacy standard can be upheld through certain frameworks which are established through articles 25 and 26 of the DPD and later on repeated in the GDPR.[115]

4.2. Adequacy Decisions

One of the ways the Commission ensures that a third country outside the EU can ensure an adequate level of data protection by reasons to its domestic laws and international obligations it has entered into is by issuing 'Adequacy Decisions'.[116] 'Adequacy Decisions' comprise of a stamp of approval by the Commission that a third country-applicant has the necessary legislation in place to safeguard the protection of data that will be processed / transferred there from the EU/EEA area. The procedure for an 'Adequacy Decision' to be adopted starts with a proposal from the Commission for a country that it considers possible to acquire an eligibility status. Then an opinion by the

[114] Data Protection Directive [1995] *OJ L 281 /31*, art 25-26
[115] General Data Protection Regulation, [2016] *OJ L 119/1* , rec. 103-107 , art 44-45,47
[116] See Data Protection Directive [1995] *OJ L 281 /31* , art 25 par. 6 in comparison with General Data Protection Regulation, [2016] *OJ L 119/1*, art 45

Member State's DPAs and the EDPS are requested, followed from an approval of "Art.31 Committee" after the examination procedure is concluded. Finally when the College of Commissioners reaches a conclusion to the adoption of the decision, the third country is considered to have acquired the eligibility status for data transfers.[117] The Commission, after a proposal by the Council or the European Parliament, has the right to withdraw the adequacy status from a third country that has been granted such status, if the circumstances in the legal landscape of that country change or there is lack of enforcement to the rules that are set in place. 'Adequacy Decisions' cover only data transfers from/to organizations or businesses and do not include data transfers in the law enforcement sector.

This framework constitutes a simple solution to the transfer problem. When it comes to the adequacy standard , the Commission is not concerned as much with the existence of law protecting processing of data by third countries, but is predominantly occupied with the actual protection that such third countries offer .For this reason, it would be more accurate to assume that it is a case by case study upon which the Commission makes its decisions on which country to grant such eligibility , and not a checklist that a third country has to follow to acquire such status.[118]

So far, endorsement had to do only with countries and not locations. In WP 29 Opinions imply that under DPD locations that do not exercise sovereignty with respect to data protection laws are precluded from acquiring an adequacy standard.[119,120] Under GDPR this territoriality scope will change and will be complimented by not only countries acquiring 'Adequacy Decisions', but also a specific territory, processing sectors , even organizations located in a country that does not have adequate data protection laws in place.[121]

---

[117] Commission ' Adequacy Decisions' (n 59)
[118] Working Party 29 'First orientations on Transfers of Personal Data to Third Countries -Possible Ways Forward in Assessing Adequacy' (Discussion Document, 26 June 1997), XV D/5020/97-EN final, WP4 <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1997/wp4_en.pdf > accessed on 18 March 2017
[119] For example a local State within a Federal State.
[120] Peter Blume 'EU adequacy decisions: the proposed new possibilities'[2015] Vol.5(1) , International Data Privacy Law, 34-39 < https://search-proquest-com.uaccess.univie.ac.at/docview/1751047428?OpenUrlRefId=info:xri/sid:primo&accountid=14682 > accessed on 17 July 2017
[121] General Data Protection Regulation, [2016] *OJ L 119/1* , art 41 par.1

4.3. Privacy Shield Program

A form of an 'Adequacy Decision' concerning the U.S. was the 'Safe Harbor Program' that regulated data transfers between the U.S. and the EU/EEA area and was adopted by the Commission on 2000. One and a half decade later, on October 2015 the ECJ found the 'Safe Harbor' program to be invalid[122] on the basis that it restrained the capacities of the national authorities of the Member States to fully implement data protection laws, given that the Commission had already ruled on the eligibility of a country (the U.S.) for the processing and transfer of data from the EU/EEA area to the U.S.[123]

To ensure the adequacy standard for data transfers between the U.S. and the EU/EEA area, the Commission replaced the 'Safe Harbor' program with the 'U.S. –EU Privacy Shield' Program with its Decision on 12th of July 2016.[124] This replacement was a necessary means to an end, given of the importance and necessity for the transatlantic relationship of the transfers of personal data, especially in today's globalized digital economy. The 'U.S-E.U Privacy Shield' framework repeats some of the rights that can be found in the DPD like the right of access and correction, the right of erasure and the security safeguards to be taken by corporations during the handling of personal information[125], reassuring the data subjects that the same data protection principles that are upheld in the EU/EEA area are also covered when their data are being transferred to the U.S.

In order to barricade the data subject's rights based on the 'Privacy Shield' program, this framework allows for the filling of complaints in a variety of entities that are in place to safeguard its implementation. Some of these mechanisms have to do with filing directly a complaint against the company the handles the data subject's personal

---

[122] C-362/14 Maximillian Schrems v Data Protection Commissioner [2015] ECLI:EU:C:2015:650
[123] ECJ 'The Court of Justice declares that the Commission's US Safe Harbour Decision is invalid' [6 October 2015] No 117/15 (Press Release) <https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf > accessed on 10 July 2017
[124] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield [2016] OJ 207/1
[125] European Commission 'Guide to the EU-U.S. Privacy Shield' http://ec.europa.eu/justice/data-protection/files/eu-us_privacy_shield_guide_en.pdf > accessed on 10 July 2017, 9-13

information or turning to the National Data Protection Authority that the 'Privacy Shield' company has designated as its DPA. Complaints can also be filed at the Federal Trade Commission and the Department of Commerce of the U.S., whereas in some cases the individual can turn to arbitration proceedings in cases where the complaints remain unresolved even after using previous redress mechanisms.[126]

The implementation of the new framework that regulates the data protection scenery between the U.S. and Europe may however not be based on solid ground. There are many critics that have addressed that the issues for which the previous 'Safe Harbor' program was revoked have not been resolved under the 'Privacy Shield' framework. It is implied that the Commission has failed to provide an overall assessment of the U.S. legal order and whether or not it provides the safeguards and institutions for the resolve of data protection issues and conflicts[127] , despite the fact that it provides for conflict resolution mechanisms when a company is in breach of its obligations under the current framework.

4.4. Binding Corporate Rules

Another mechanism for the secure transfer of personal data to third countries outside the EU/EEA area is the Binding Corporate Rules that are regulated in both the DPD[128] and the GDPR[129]. BCRs are internal rules for multinational companies that safeguard the data transferring from one corporate entity of the group to another in order to achieve a global privacy policy within the corporate group. To that extent, they ensure that the same and adequate protection of transfers of personal data between the corporate group companies are set in place Despite the fact that BCRs are considered to be a mechanism for data transfers to third countries, they also serve as a basis for a company's compliance with national data protection laws.[130] The requirements for adopting BCRs are firstly that the rules laid down by them should comply with the DPD (and later on with the GDPR) meaning that the BCRs should enclose the same principles that the

[126]Commission 'Guide to the EU-U.S. Privacy Shield' (n 125), 16
[127] Xavier Tracol 'EU–U.S. Privacy Shield: The saga continues'[2016] Vol 32(5),Computer Law & Security Review: The International Journal of Technology Law and Practice, 775-777
[128] Data Protection Directive [1995] *OJ* L 281 /31, art 26 par. 2
[129] General Data Protection Regulation, [2016] *OJ L 119/1* ,art 47
[130] Kuner (n 16) 219

DPD secures e.g. transparency, data quality, security and secondly that these rules should have a binding and legally enforceable nature through audits, complaint handling system , dispute resolution mechanisms etc.[131] The Commission has the capacity to overview the procedure of adoption of BCRs and whether or not they offer sufficient safeguards. BCRs can be either standard contractual clauses or ad hoc contractual clauses, based on the case by case transfer of data.[132]

In comparison to other legal frameworks concerning the protection of personal data, BCRs allow for a more flexible environment compared to the standard contractual clauses[133]. Despite the fact that standard contractual clauses bring a status of legal certainty , given the fact that they are voted by the Commission , this is at the expense of flexibility that does not necessarily cover all the individual contract's needs.[134] The procedure for the adoption of BCRs from a multinational company requires, as is instructed by WP 29 to, the appointment of a coordinating lead authority in order to avoid the approval procedure with each national DPA. The second step is for the company to draft a BCR according to working papers and opinions[135] of the WP 29 that meets the requirements of the current applicable legislation on data protection. After the drafting, the lead authority circulates the proposed BCR to the DPAs of the countries where the corporation has affiliates and when the procedure is closed under mutual recognition of the implementation of the rules that are laid down, the company can seek for authorization to circulate data according to the rules that are laid down by the BCR.[136]

---

[131] Stefan Schuppert ,'The EU Parliament Vote on the EU General Data Protection Regulation – The Death of Binding Corporate Rules for Processors?' [2014] ,Vol. 15(2), Computer Law Review International Review International, Verla Dr. Otto Scmidt, 40-44

[132] Kuner (n 16)192

[133]The Standard Contractual Clauses or 'Model Contractual Clauses' are analyzed in Part. 4.5 of this thesis.

[134] Olivier Proust; Emmanuelle Bartoli 'Binding Corporate Rules: a global solution for international data transfers' [2012] Vol.2(1) International Data Privacy Law, 35-39 <https://search-proquest-com.uaccess.univie.ac.at/docview/1564009535?OpenUrlRefId=info:xri/sid:primo&accountid=14682 > accessed on 17 July 2017 (BCRs)

[135] Working Party 29 'Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers' (Working Document, 3 June 2003) MARKT/11639/02/EN, WP74 <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp74_en.pdf > accessed on 18 March 2017

[136] European Commission 'BCR Procedure' <http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/procedure/index_en.htm > accessed on 18 June 2017

4.5. Model Contractual Clauses

BCRs as we mentioned above, are adopted by multinational companies but are not the only instrument of compliance for global corporations. On the basis of art. 26 par. 4[137]of the DPD the European Parliament and the Council have given the Commission the authority to decide on whether certain standard contractual clauses or 'Model Contractual Clauses' carry all the safeguards for the transfer of personal data to third countries. The Commission has issued so far to sets of standard contractual clauses for controllers[138,139] and one set for processors[140]. The essence of the standard contractual clauses is that they for the data controller- company to adopt them and is situated in a EU/EEA Member State to transfer, following all the necessary security safeguards, information to another controller or processor that is located in a third country that does not have the 'adequacy status' according to the DPD.

The procedure for the adoption of standard contractual clauses by the Commission initiates with a proposal from the Commission, followed by an opinion of the Member States DPAs and the EDPS . The third step is to go through an examination procedure and acquire the approval of Art. 31 Committee, which is a body composed of representatives of Member States. Finally, after the adoption of the decision by the College of Commissioners as well, the standard contractual clauses are adopted as a legal framework capable to protect the information of the data subject during the transfer of such data to third countries.[141]

Despite the fact that the 'Model Contractual Clauses' have a legal advance compared to the BCRs, given that they bring higher legitimacy since they are voted by the

---

[137] Data Protection Directive [1995] *OJ* L 281 /31, art 26 par. 4
[138] Commission Decision of 15 June 2001on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC [2001] OJ L 181/19, Set 1
[139]Commission Decision of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries [2004] OJ L 385/74, Set 2
[140] Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council [2010] OJ L 39/5
[141] European Commission 'Model Contracts for the transfer of personal data to third countries' < http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm> accessed on 10 June 2017

Commission, one of their primary drawbacks is the lack of flexibility which occurs from the fact that if a clause is amended or omitted from the contract, then the DPAs reserve the right to reject the new version, bringing the whole legal construction into collapse.[142]

All the aforementioned legal frameworks are put in place to offer protection for the transferring of personal data to third countries in ways that are efficient and involve adequate security. In some cases, these frameworks overlap the one the other –for example one country is covered by an 'Adequacy Decision' framework and the company that is operating in this country has adopted also BCR for its other affiliates. This multifaceted legal protection can ensure that the companies have made the first step towards acknowledging the need for compliance to the rules set for data protection and are ready to adopt a data security plan to put into implementation a scheme that will cover the legal responsibilities that they have taken up.

[142]Proust;Bartoli 'BCRs' (no 134)

5. Risk Management for Corporations

The protection of personal data is a process that requires apart from very high vigilance and expertise, an in depth knowledge of IT-systems in conjunction with legal knowledge on data protection. The legal frameworks which should be taken in consideration in the handling of personal information and have been analyzed in previous paragraphs constitute only a structure under which companies are instructed to operate. This legal framework in order to 'gain consciousness' should transform into a security plan that will embody the rules established under the current applicable legislation. In other words, there are two responses to the need for security. The first is to declare that a conduct is illegal like e.g. in cybercrime statutes that typically seek to protect the security of corporate data by outlawing offenses or practices that fail to comply with the principles of confidentiality, integrity and availability etc. The second response is the requirement for the protection of data through the formation of a security plan[143] or as it is alternatively called 'risk management' that will mitigate and prevent any kind of threats in the process of personal data.

The need for risk management in data protection has increased in recent years due to the ever increasing transfer of personal data from one corporate entity to another. The fact that many companies even to this day have not a security plan in place has created many problems in the corporate environment and generated financial loss and reputation discredit. According to Richard Thomas, Information Commissioner for the U.K. , there has been a "frankly horrifying" list of breaches over recent years, despite the "toxic liability" that exists for the safeguarding of information and requires organizational changes and proper care of records. Such breaches can be showcased by the fact that big companies like the HMRC have lost 25 million records on 2 discs and in the course of the investigation that followed by PWC's Kieran Poynter it has been pointed out that there is a need for staff training and assumption of accountability from the side of HMRC.[144]

---

[143] Smedinghoff (n 18) 31

[144] Kieran Poynter 'Review of information security at HM Revenue and Customs-Final report' [June 2008] < http://roselabs.nl/files/audit_reports/PwC_-_HM_Revenue_and_Customs.pdf > accessed at June 15 2017

In order to explain the term of risk management, it is important to break down this expression and describe its components. To start with, risk is "a measure of the extent to which an entity is threatened by a potential circumstance or event, and is typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence."[145] In simpler words, risk means that any lack or omission of security in a corporation can cause corporate loss , which will result either from third malicious parties exploiting this vulnerability or internal employee negligence concealing information. Along with 'risk' comes the term of 'management' meaning the way in which such a vulnerability can be dealt with, if not eliminated.

Risk management is a process under which protecting measures for personal data security are being adopted in order to achieve maximum capability in the safeguarding of the IT systems in which such data are being secured and support the corporation's needs. Such measures are being balanced for their economic and operational costs and implemented due to the corporate needs for reduction of negative impacts from data loss. In other words, risk management allows corporations to establish a structured, consistent basis for making decisions in order to tackle non-speculative risks, otherwise called 'pure' or permanent risks, which can only reduce the value of the assets and information that a corporation holds.[146]

The objectives of risk management are the following[147]:

- Elimination of risks through the discontinuation of the activity that is causing the risk.
- Reduction of the risks that cannot be eliminated to acceptable levels by implementing safeguards either directly –restriction of access- or indirectly - identification mechanisms.
- Risk retention, meaning the existence of risks in the corporate environment but

[145] National Institute of Standards and Technology(NIST) 'Guide for Conducting Risk Assessment-Information Security) NIST Special Publication 800-30 Revision 1 < http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf > accessed on 10 June 2017, 6

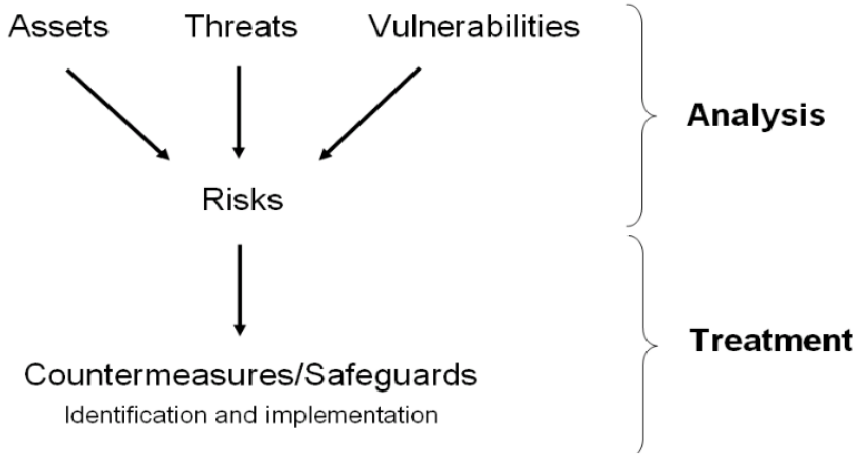
[146] Alan Calder;Steve G. Watkins, *Information Security Risk Management for ISO27001/ISO27002,* (Cambridgeshire , IT Governance Publishing, 2010),17

[147] Feiler (n 17) 64

exercising regular controls over them to keep them to an acceptable level.

- Transfer of risk by means of insurance or from one entity to another either directly – civil liability- or indirectly –mandatory disclosure.

Risk management comprises of two phases: Risk assessment and risk treatment. These two phases succeed the one the other and both of them are subprocesses of risk management. The diagram that follows showcases the relationship between the procedures:



148

As is showcased in the above diagram, the identification of assets, threats and vulnerabilities that should be taken into consideration as a possible problem are processed in the analysis-assessment phase. Any action, decision or deliberate lack of both that comes after the first assessment, belongs in the risk treatment phase.

5.1. Risk Assessment

Risk assessment is a procedure during which the people responsible in a corporation for data protection test the data environment for possible threats to their security. This process consists of the identification of possible threats and estimation of the likelihood

[148]Calder;Watkins (n 146),18

of those threats exploiting a lack in the corporate system, as well as an evaluation of the impact of such an event occurring.[149] In order for risk assessment to be as efficient as possible, a repetitive approach needs to be taken into consideration. This would allow for an increase of depth and detail in the assessment process during each repetition with the consequence of minimizing the time and the effort in identifying the risk.

In the process of risk assessment, companies conduct tests upon the security systems that are placed in various categories of data. These security systems – either in vitro or concerning the workforce of the company- are under scrutiny for their performance in data protection. However, due to budget and time restrictions, there are some limitations to the auditing in information security. For this reason, it is important for certain critical areas to be targeted first. Such tests are the following[150] :

- On broad categories of security audits, operators can conduct passive assessments such as verification against prefabricated checklists or active assessments meaning vigorous searches for vulnerabilities.
- Assessments audits on categories of data depending their degree of sensitivity (sealed-unsealed data) and possibility to acquire them.
- Assessment audits based on vulnerability tests such as internal audits that check for gaps in security that is in place, and penetration tests like emulation of malicious third parties.
- Social engineering tests which would consist of interviewing employees involved in different forms of social engineering and assessing their training in data protection and access to personal data e.g. getting into the server room, accessing company premises, retrieving configuration files etc.

5.2 Risk Treatment

Risk treatment is the process of responding to identified risks and is subsequent to the risk assessment procedure, meaning that it comprises of any action taken after the loss

[149] Stefan Schiebek 'An approach to continuous information security risk assessment focused on security measurements' (Dissertation, Vienna University, 2014)
[150] Andrew A. Vladimirov and others , *Assessing information security : strategies, tactics, logic and framework* (2nd edn, Ely, Cambridgeshire, IT Governance Publishing, 2014)

or tampering of personal data. According to the DPD[151] the data controller should adopt all the necessary security safeguards in order to avoid such occurrences and even the case of an attack against the corporate systems should have a plan in place to avoid significant data breach. The GDPR , moving a step further to that direction, recognizes the potential loss of data and apart from the remedies, liability and sanctions against the data controller which are mentioned also in the DPD[152,153] adds the notification requirement in cases of data breach[154] under which the data controller should notify the supervisory authority *"…without undue delay and where feasible not later than 72 hours after having become aware of it…"*.

It is apparent that the corporate entity-controller has in any case the responsibility both under the DPD and the GDPR – along with the other applicable legal frameworks for data transfers outside the EU/EEA area- to demonstrate the existence of controls that are set in place for the protection of personal information or at least that the risk for data tampering has been reduced to an acceptable level.

The process of risk treatment is usually identifiable in economic terms since any threat to the data protection framework established by businesses translates into loss of value of the corporate assets, both tangible and intangible. The criterion used to determine whether a threat is between the risk tolerance level is as follows:

- Risk level < risk acceptance criteria, then 'accept risk'
- Risk level > risk acceptance criteria, then 'treat risk'

The types of control that can be set in place during the risk treatment phase vary from corporation to corporation according to its needs and standards of procedure. These controls are separated primarily into three big categories: preventive controls that secure the protection from vulnerabilities in the system, corrective controls which reduce the impact of threats and detective controls which discover attacks and trigger the two aforementioned mechanisms.

---

[151] Data Protection Directive [1995] *OJ L 281 /31*, art 17
[152] Data Protection Directive [1995] *OJ L 281 /31*, art 22-24
[153] General Data Protection Regulation, [2016] *OJ L 119/1*, Chapter VIII
[154] General Data Protection Regulation, [2016] *OJ L 119/1* , art.33

That being said, the types of control vary greatly, having although as an ulterior outcome the three aforementioned actions: prevention, correction, detection. Such other control types are the technical controls, meaning security mechanisms on hardware and software, cryptography, authentication, management controls such as employee traineeships, drafting of policies , and operational controls that tackle daily issues, like information back- ups. These types of controls should take into consideration certain constraints like time, legal constraints and financial constraints etc. that might hinder their effectiveness but nevertheless are impossible to overcome. In the cases that there is a risk untreated and is considered to be below the threshold of risk acceptance, this is considered to be residual risk and does not trigger any kind of corrective mechanisms.[155]

Some companies nowadays choose the option of risk transfer through signing insurance policies that are specialized in addressing information security issues. This comes as no surprise as it is an efficient way to outsource liability to third parties for any data loss, while in the same time minimizing the loss of value and reputation of the company.

To conclude, a risk treatment plan through any of the means that are available as described above is the keystone to the smooth operation of a company. By having a treatment plan in place for any threats that might obstruct the standard course of business, companies can feel secure and be prepared for the potential loss that might suffer, and respond quickly and with no major harm for their value and assets. In other words, a risk treatment plan offers to a company options through which they can tackle the problems that occur in their data protection operations and help them act more confidently towards the future of their operations.

---

[155]Calder;Watkins (n 146) ,148-150

6. The Role of the Corporate Data Protection Officer

With the introducing of the new legal framework for data protection in Europe, the role of the DPO became a necessity for every corporation that handles personal data and is located in the EU/EEA area or bound by its legislation. The primary role of the DPO is to assist the corporation in meeting with the requirements that are set by the GDPR. If a company fails to do so, the new framework mandates for the imposition of fines that can mount up to 20 million or 4% of the annual turnover of the business' activity.

The designation of a DPO is mandated in art. 35 par. 2 and in art. 37 par. 1 of the GDPR that reads:

"…The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment…."[156]

"...The controller and the processor shall designate a data protection officer…"[157]

According to the GDPR , data protection compliance obligations apply to all kinds of corporations , regardless of their scope of business or their size and it is of no relevance if they are processors or controllers of the data.[158] The assessment for the appointment of a DPO is based on the kind of data that are being handled and on whether or not they are considered to be of "high risk" to the rights and freedoms of the data subject.[159] Specifically the appointment of a DPO is necessary with the following categories of data are being processed: [160]

- When systematic or extensive evaluation of personal data takes place.
- In cases where sensitive data and data related to criminal offenses on a large scale are being processed.
- On occasions where systematic monitoring of publicly accessible areas occur.

---

[156] General Data Protection Regulation, [2016] *OJ L 119/1*, art 35 par. 2
[157] General Data Protection Regulation, [2016] *OJ L 119/1* , art 37 par. 1
[158] Paul Lambert, *The data protection officer : profession, rules, and role (*Boca Raton Florida, CRC Press, 2017), 4
[159] General Data Protection Regulation, [2016] OJ L 119/1 , art 35 par. 1
[160] General Data Protection Regulation, [2016] OJ L 119/1, art. 37 par.1

Companies can hire DPOs permanently or on a contract basis depending on their needs for the time frame of their operations. Despite the fact that DPOs are considered to be employees in a company, given that they are on their payroll, they are independent organs of the business and do not follow directions given by the management but on the contrary they perform their own tasks without third party influences.[161] Due to this fact, DPOs cannot be dismissed or penalized for failing to follow guidelines given by the management, in opposition to their tasks and functions.[162]

DPOs report to the highest level of management[163] and more specifically to the management board director, which will be their primary reporting point. In this way, the role of the DPO will not be downgraded to an advisory function, but taken seriously without any undermining by layers of internal bureaucracy thus strengthening the weight of the data protection message. The primary function of this organ is to ensure the protection of rights of the data subject and despite the fact that the DPO is working for the company that hired him her, they should not be inclined to find any legal loopholes in GDPR or facilitate shortcuts.

DPOs are usually working in close relationship with the IT departments of the company as they are "preaching to the quire", meaning to employees who can understand better the guidance of the DPO since they are the ones that are required to transform the legislation on data protection to practical methods – technological security systems- in order to preserve the integrity of data. In previous years, the role of a DPO was assumed by an IT person, usually lacking the legal background, but in any case trying to ensure the security of personal data from malicious threats. The upgrading of the role of the DPO resulted in the drafting of policies and developing of security policies in close cooperation with the IT department. The common interests between these two functions of the company revolve around data collection, use, context,

---

[161] EU Data Protection Regulation, 'The Data Protection Officer' <http://www.eudataprotectionregulation.com/data-protection-officer> accessed 5 June 2017
[162] Lambert (n 158) 72
[163] General Data Protection Regulation, [2016] *OJ L 119/1* , art 38 par. 3

classification, data separation, data ring-fencing , data containment, risk appraisal etc.[164]

The tasks of the DPO, as laid down in the GDPR[165], can be resumed in the following:

- Creates policies and procedures in order to bring the company in compliance with the Regulation.
- Monitors the implementation of aforementioned policies.
- Is the primary contact point for supervisory authorities and data subjects.
- Keeps management informed regarding its obligations towards the GDPR and the security measures that are taken in compliance to the GDPR.
- Ensures the training of all employee stuff regarding data protection issues, assigns responsibilities and consults in privacy issues.
- Is responsible for monitoring, notifying and communicating information about personal data breaches[166] and documenting public and regulator's request regarding the removal, destruction and accessibility of data.
- Due to the access right of the data subject as instructed by the GDPR[167] , the DPO is also responsible to confirm to the data subject that its personal data are being processed, the purpose of the processing and the content of the data that are being processed.[168]

The GDPR sets a standard for the appointment of the DPOs requiring them to have "expert knowledge of data protection law and practices" and the ability to fulfill the tasks as set out by the GDPR.[169] This vague standard of competency comes as a surprise to an otherwise detailed legal framework. One can assume that this expert knowledge derives from years experience in the data protection environment and can be associated only with long practice of data protection law, since the GDPR does not provide for the proof of competency in other means. Some theorists are of the opinion

---

[164] Lambert (n 158) 87
[165] General Data Protection Regulation, [2016] *OJ L 119/1* ,art 39
[166] General Data Protection Regulation, [2016] *OJ L 119/1* ,art 30-31
[167] General Data Protection Regulation, [2016] *OJ L 119/1* art 15
[168] Lambert (n 158) 235
[169] General Data Protection Regulation, [2016] *OJ L 119/1* , art 37

that a certification mechanism would benefit the appointment of DPOs.[170] However, it remains to be seen after the implementation of the GDPR on how this procedure will form itself in the future and what further requirements will be requested by future employers.

[170] Eric Lachaud, 'Should the DPO be certified?' [2014] Vol. 4(3) International Data Privacy Law , 189-202

Conclusion

Much like the fugue in music, where a specific music theme that has been introduced in the beginning of the composition is imitated in later stages in higher pitches during the course of the play, data protection is comprised of an ever ending circle that goes back to its primary cause of existence: the individual's right to privacy. However, like in music, with every turn of the fictional circle, the protection environment is being enriched with new findings and legislative constructs that allow the fuller, better and multifaceted understanding of how the right to privacy and its specific expression, the right to data protection, can be upheld.

Going back to the beginning of this paper, data protection essentially is a set of legislative frameworks that are set in place to protect the personal data of individuals that are being stored in corporate entities or other kind of data controllers or processors – like governments, organizations etc– from unlawful or unauthorized access and tampering. In the process of safeguarding personal information, the aforementioned entities should bear in mind to sustain three pillar principles. These are the principle of confidentiality, meaning the protection from unauthorized disclosure or access, integrity in systems meaning the implementation of protection through security mechanisms and secondly in data, meaning accuracy of the data gathered to the individual that the concern and lastly, availability of the information to the data subject so as to enable it to have access and knowledge of which personal data of the subject are being used, to what extent and for which purposes.

In today's European societies, the right to data protection is expressed through much legislation that ensures that European citizens can enjoy services and products without having to give up a portion of their privacy in order to do so. The processing of their data in using these services and products in a globalised market is taking place under supervision, either from the European instruments themselves or from internal corporate employees who are instructed to put forward corrective mechanisms in order to achieve maximum levels of data protection.

Despite the elaborate system that has been developed in recent years for the achievement of this protection, a general mistrust against any kind of personal data

handling is evident in the European communities. This stems from the fact that much of the legislation that has been explained in previous chapters comprises of an intricate system of clauses and exemptions that are difficult to be comprehended by the average citizen. Moreover, the advancements in new technologies and the expansion of e-corporations allow for mishandlings of personal data either due to the lack of training of the human resources in these businesses or the development of malicious threats which develop in the antipode of positive and useful of technologies. The solution to this issue of mistrust by the side of individuals is expressed by Commissioner Vera Jourova that reads:

"…*I will launch a massive information campaign by January at the latest. It should tell people about the new rights that the data protection reform brings to them…..I do not want people to be paranoid. I just want them to know who is handling their data and what he or she will do with their data. I want people to give really conscious consent that can be withdrawn if they so wish*…". 171

For the Commissioner, the solution to the citizen's feeling of discomfort in the processing of their personal data is acquiring information and education through which they can fully comprehend their rights on data usage and how they are able to claim back their data and be awarded damages for any unlawful use. On the other hand, it is also important other than individuals knowing how they can claim back control of their personal data that corporations set up protection mechanisms that enable for such protection of the primary data actors – the corporations who are controlling the purposes of processing and the processing itself – to take place.

This thesis focuses on the responsibility that companies have towards their customers and the individuals whose data are being stored for further usage, a responsibility that stems not only due to the existing legislation and the necessity for the corporate actors to uphold the principles and doctrines of this legislation , but also due to the fact that companies have social responsibility towards the data subjects. This responsibility

---

[171]Lukáš Hendrych , 'Jourová: I will launch a massive information campaign on data protection' (Euroaktiv, 5 May 2017) < https://www.euractiv.com/section/data-protection/news/jourova-i-will-launch-a-massive-information-campaign-on-data-protection/ > , accessed on 2 July 2017

translates to customers' trust of the services and products of businesses and which in turn allows for the engrossment of corporate profits.

Nevertheless, as seen in previous chapters, for businesses to comply to the conundrum of legislation that there is, it is a project often difficult to be achieved given the complexity of situations at hand and often the deviations from Member State to Member State on the applicable legislation. Corporations acting in their capacity as a processor or a controller have to comply with two sets of legal frameworks, depending on the location of their activities, meaning where the processing takes place and the location of their customers whose data are being processed. These two types of protection are divided to data transfers within the EU/EEA area and for data transfers outside the EU/EEA area, to third countries.

One often questions if the applicable legislation for data transfers is enough to ensure the maximum protection concerning these activities. This insecurity stems from the fact that despite the existence clauses in the legislation that foresee for the imposition of fines and remedies in cases where data protection rules are disregarded, these kind of sanctions mechanisms are difficult to be imposed either due to the immense number of corporations that are dealing with data processing, a number which cannot be adequately monitored if the highest vigilance is not in place, or due to Member State's lack of corrective mechanisms that decelerate the remedial process.

For this reason, the new reformed data protection legal framework, under the umbrella of the GDPR, instructs for the necessary designation of the DPO, a compliance officer who will assume the role of bringing the company's policies to alignment with the responsibilities it has towards its customers and the laws governing the data protection landscape. Even though the role of the DPO is not a new invention, since many countries preceding to the instructions of the GPPR have domestic laws on data protection which are encouraging for the appointment of such an employee, it constitutes however a step forward and an amelioration to the previous legislative regimes governing the way companies should function in order to achieve data protection.

Despite the fact that the DPO is considered to be an employee for the company, he or she is responsible primarily for the compliance of the company to the existing European regulations. For this reason as has been previously mentioned, the DPO responds only to the Board of the company and the Manager Director. The reformed framework for data transfers ensures in this way the highest level of compliance to the data protection rules as it enables for a vigilant eye to exist in every corporation that does not have to answer to lowest levels of hierarchy within a company and whose commands and decisions are not second guessed.

The DPO is also responsible to coordinate with the IT team in order for these two functions to develop in coordination system security plans. During this process, the DPO has the responsibility to oversee the legal requirements of the plan and to explain to the IT department in which way, to what extent and from what kind of threats should the data be protected and in its turn the IT team realizes the instructions of the DPA through the development of a tangible security plan.

The question that concerns the law theorists and practitioners and the individual's whose data are being processed is the following; Will the reformed data protection legislation with its current applicable rules establish stronger and time lasting strongholds concerning the protection of personal information for the individuals, or will the new rules add to an already complex system of legislation that in many cases fails to secure the rights for which it has been adopted?

The new framework, under the GDPR and the applicable rules for third country transfers is as complete as any legislation can be. Given that data protection is a right that stems from the need to protect a society in which technology is ceaselessly developing, it is easy to deduct that absolute protection can never be achieved. The European legislative instruments recognize this fact and are providing for rules that can be at the same time flexible , in order to be applied as well in future technological advancements , and strict in the sense that the core rights for individuals are respected in any kind of developments in new technologies that deal with personal data.

When all is said and done, the answer to the question that has been posed could be summarized in the words that many law professors often repeat to their students; it

depends. Certainly, the framework at place is an extensive set of rules that attempts to cover all the parameters to the data protection necessity and the broader right to privacy. The Commission in the reformed framework, with the adoption of rules that requires for the necessary designation for DPO in every company dealing with data – which could be said for every company existing at least in the last decade in every kind of industry sector- has made a step forward to the direction of higher compliance of the companies towards the applicable data protection rules. Moreover, the risk management plans that can be developed under these conditions would enable for a better assessment of risk concerning the tampering of loss of corporate data and through this assessment, the risk treatment and remedial process would be easier to be achieved. The Commission is hopeful to that end and has given plain and sufficient instructions for the implementation of the new frameworks. Any deficiencies that exist in the paneuropean legislation may be corrected from specified rules of each Member State that follow the essence of the Commission's suggestions and voted legislation on data protection.

Bibliography

Legislation

- Convention for the Protection of Human Rights and Fundamental Freedoms (European convention on Human rights, as amended) (ECHR) [1950]
- Consolidated version of the Treaty on the Functioning of the European Union (TFEU) [2012] C326/47
- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive) [1995] *L 28 /31*
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119/1
- Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L 119/89
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L201/37
- Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield [2016] OJ 207/1
- Commission Decision of 15 June 2001on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC [2001] OJ L 181/19, Set 1

- Commission Decision of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries [2004] OJ L 385/74, Set 2
- Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council [2010] OJ L 39/5

Case Law

- L.H. v. Latvia Ap no. 52019/07 (ECtHR , 29 April 2014)
- S.and Marper v. The United Kingdom no.30562/04 and 30566/04 (ECtHR, 4 December 2008)
- C-131/12 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014] ECLI:EU:C:2014:317
- C-362/14 Maximillian Schrems v Data Protection Commissioner [2015] ECLI:EU:C:2015:650

Books

- Christopher Kuner, *European data protection law : corporate compliance and regulation* (2 edn, Oxford, Oxford Univ. Press, 2007)
- Lukas Feiler, *Information security law in the EU and the U.S. : a risk-based assessment of regulatory policies* (Wien,Springer, 2011)
- Thomas J.Smedinghoff, *Information security law : the emerging standard for corporate compliance* (Ely, IT Governance Pub, 2008)
- Collin J. Bennet , *Regulating Privacy, Data Protection and Public Policy in Europe and the United States*, (Cornell University Press,1992)
- Alan Calder;Steve G. Watkins, *Information Security Risk Management for ISO27001/ISO27002*, (Cambridgeshire , IT Governance Publishing, 2010)

- Andrew A. Vladimirov and others , *Assessing information security : strategies, tactics, logic and framework* (2nd edn, Ely, Cambridgeshire, IT Governance Publishing, 2014)
- Paul Lambert, *The data protection officer : profession, rules, and role (*Boca Raton Florida, CRC Press, 2017)

Online Journals

- Vijay Basani , '9 Important Elements to Corporate Data Security Policies that Protect Data Privacy' (*Security magazine*, 10 May 2016) <http://www.securitymagazine.com/articles/87113-important-elements-to-corporate-data-security-policies-that-protect-data-privacy> accessed on 6-5-2017
- Stephen Saxby, 'Data protection directive gets its first progress report', [2003] Vol 19 (4), Computer Law & Security Report,271 ,< http://www-sciencedirect-com.uaccess.univie.ac.at/science/article/pii/S0267364903004011?via%3Dihub> accessed 15 May 2017
- Peter Blume 'EU adequacy decisions: the proposed new possibilities'[2015] Vol.5(1) , International Data Privacy Law, 34-39 < https://search-proquest-com.uaccess.univie.ac.at/docview/1751047428?OpenUrlRefId=info:xri/sid:primo&accountid=14682 > accessed on 17 July 2017
- Olivier Proust; Emmanuelle Bartoli 'Binding Corporate Rules: a global solution for international data transfers' [2012] Vol.2(1) International Data Privacy Law, 35-39 <https://search-proquest-com.uaccess.univie.ac.at/docview/1564009535?OpenUrlRefId=info:xri/sid:primo&accountid=14682 > accessed on 17 July 2017

Print Journals

- Rebecca Wong , 'The Data Protection Directive 95/46/EC: Idealisms and realisms'[2002] Vol. 26(2-3) International Review of Law, Computers & Technology, Routledge, 229-244

- Elizabeth Kennedy; Millard Christopher 'Data security and multi-factor authentication: Analysis of requirements under EU law and in selected EU Member States' [2016] Vol.32 (1) Computer Law & Security Review: The International Journal of Technology Law and Practice, 91-110
- Paul de Hert; Vagelis Papakonstantinou, 'The new General Data Protection Regulation: Still a sound system for the protection of individuals?' [2016] Vol.32 (2) Computer Law & Security Review: The International Journal of Technology Law and Practice, 179-194
- Jari Raman 'European Court of Human Rights: Failure to take effective information security measures to protect sensitive personal data violates right to privacy – I v. Finland, no. 20511/03, 17 July 2008' [2008] Vol.24(6), Computer Law and Security Review: The International Journal of Technology and Practice,562-564
- Inge Graef and others 'Putting the Right to Data Portability into a Competition Law Perspective' [2013] Vol. Annual Review, The Journal of the Higher School of Economics, 53-63
- Xavier Tracol 'EU–U.S. Privacy Shield: The saga continues'[2016] Vol 32(5),Computer Law & Security Review: The International Journal of Technology Law and Practice, 775-777
- Stefan Schuppert ,'The EU Parliament Vote on the EU General Data Protection Regulation – The Death of Binding Corporate Rules for Processors?' [2014] ,Vol. 15(2), Computer Law Review International Review International, Verla Dr. Otto Scmidt, 40-44
- Eric Lachaud, 'Should the DPO be certified?' [2014] Vol. 4(3) International Data Privacy Law , 189-202

Press Releases

- European Commission, 'European Commission launches EU-U.S. Privacy Shield: stronger protection for transatlantic data flows' [12 July 2016] IP/16/2461 (Press Release) < http://europa.eu/rapid/press-release_IP-16-2461_en.htm > accessed on 6 May 2017

- European Commission 'Joint statement by Commissioner Věra Jourová and Haruhi Kumazawa, Commissioner of the Personal Information Protection Commission of Japan on the state of play of the dialogue on data protection' [4 July 2017] STATEMENT/17/1880 (Statement) <http://europa.eu/rapid/press-release_STATEMENT-17-1880_en.htm> accessed on 10 July 2017

- ECJ 'The Court of Justice declares that the Commission's US Safe Harbour Decision is invalid' [6 October 2015] No 117/15 (Press Release) <https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf> accessed on 10 July 2017

Internet sources

- Data Protection Commissioner, 'Data Security Guidance' <https://www.dataprotection.ie/docs/Data-security-guidance/1091.htm> accessed 6-7-2017
- European Commission, 'Protection of Personal Data' <http://ec.europa.eu/justice/data-protection/> accessed on 23 April 2017
- European Commission , 'What benefits for businesses in Europe' (Data Protection Reform Factsheets, 16 January 2017) <http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=52404> accessed on 23 April 2017
- European Commission, ' Protection of Personal Data' <http://ec.europa.eu/justice/data-protection/ > accessed on 10 June 2017
- European Commission, 'The EU-U.S. Privacy Shield', <http://ec.europa.eu/justice/data-protection/international-transfers/eu-us-privacy-shield/index_en.htm> accessed on 5 March 2017
- International Trade Administration U.S. Department of Commerce, 'Privacy Shield Overview', <https://www.privacyshield.gov/Program-Overview> accessed on 6 May 2017
- European Commission 'Commission decisions on the adequacy of the protection of personal data in third countries' < http://ec.europa.eu/justice/data-

protection/international-transfers/adequacy/index_en.htm > accessed on 6 May 2017

- European Commission 'Overview on Binding Corporate Rules' < http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/index_en.htm > accessed on 6 May 2017
- European Commission, ' Model Contracts for the transfer of personal data to third countries' <http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm> accessed on 15 July 2017
- Detlev Gabel; Tim Hickman, ' Chapter 6: Data Protection Principles- Unlocking the EU General Data Protection Regulation' (*White & Case*, 22 July 2016)<https://www.whitecase.com/publications/article/chapter-6-data-protection-principles-unlocking-eu-general-data-protection#> accessed on 22 June 2017
- Detlev Gabel; Tim Hickman, 'Chapter 4: Territorial application – Unlocking the EU General Data Protection Regulation' (*White & Case*, 22 July 2016)<https://www.whitecase.com/publications/article/chapter-6-data-protection-principles-unlocking-eu-general-data-protection#> accessed on 22 June 2017
- European Commission 'Article 29 Working Party'< http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083 > accessed on 5 May 2017
- European Data Protection Supervisor 'Article 29 Working Party' para 4 <https://edps.europa.eu/node/3095%23articlewp_en >accessed on 5 May 2017
- EU Data Protection Regulation 'Data Protection by Design and by Default' <http://www.eudataprotectionregulation.com/data-protection-design-by-default> accessed on 7 May 2017
- Paul Voigt 'The compliance burden under the GDPR – Data Protection Officers' (Taylor Wessing,September 2016) <https://www.taylorwessing.com/globaldatahub/article-compliance-burden-under-gdpr-data-protection-officers.html > accessed on 10 July 2017
- European Commission 'Guide to the EU-U.S. Privacy Shield' http://ec.europa.eu/justice/data-protection/files/eu-us_privacy_shield_guide_en.pdf > accessed on 10 July 2017, 9-13

- European Commission 'BCR Procedure' <http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/procedure/index_en.htm > accessed on 18 June 2017
- European Commission 'Model Contracts for the transfer of personal data to third countries' < http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm> accessed on 10 June 2017
- Kieran Poynter 'Review of information security at HM Revenue and Customs-Final report' [June 2008] < http://roselabs.nl/files/audit_reports/PwC_-_HM_Revenue_and_Customs.pdf > accessed at June 15 2017
- National Institute of Standards and Technology(NIST) 'Guide for Conducting Risk Assessment- Information Security) NIST Special Publication 800-30 Revision 1 <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf> accessed on 10 June 2017, 6
- EU Data Protection Regulation, 'The Data Protection Officer' <http://www.eudataprotectionregulation.com/data-protection-officer> accessed 5 June 2017

Assessment papers

- Working Party 29 'First orientations on Transfers of Personal Data to Third Countries -Possible Ways Forward in Assessing Adequacy' (Discussion Document, 26 June 1997), XV D/5020/97-EN final, WP4 <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1997/wp4_en.pdf > accessed on 18 March 2017
- Working Party 29 'Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers' (Working Document, 3 June 2003) MARKT/11639/02/EN, WP74<http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp74_en.pdf > accessed on 18 March 2017

Soft Law

- Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data[1980 as amended in 2013] OECD Council <http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm> accessed 8 March 2017
- Opinion 4/2007of the Working Party 29 on the concept of personal data [20 June 2007] 01248/07/EN , WP 136
- Opinion 1/2010 of the Working Party 29 on the concepts of "controllers'' and "processors" personal data [16 February 2010] 00264/10/EN ,WP 169

Dissertations

- Stefan Schiebek 'An approach to continuous information security risk assessment focused on security measurements' (Dissertation, Vienna University, 2014)

Online Newspapers

- Lukáš Hendrych , 'Jourová: I will launch a massive information campaign on data protection' (Euroaktiv, 5 May 2017) < https://www.euractiv.com/section/data-protection/news/jourova-i-will-launch-a-massive-information-campaign-on-data-protection/ > , accessed on 2 July 2017

English Abstract

The aim of this paper is to introduce the applicable legislation concerning data protection for European citizens and the ways in which these rules shape the responsibilities of the companies dealing with personal information.

The right to data protection stems from the right to privacy and was introduced as a separate right in the Treaty of the Functioning of the European Union and later on validated in the EU Charter of Fundamental Rights. Its necessity is ever evident, especially in today's modern societies where vast amounts of personal data are daily transferred from corporation to corporation in their function as a processor or a controller of such data, in order to conduct their daily activities. The right to data protection essentially signifies the fact that personal information has value not only to the individual that it concerns in order for him or her to ensure the fortification of his or hers private life, but also to corporations who in the case of loss or destruction of the data that are being dealt, risk the loss of business profit.

The legislative instruments of the European Union have set a variety of legal frameworks that protect the processing of data of European citizens from any third party threats and malicious actors. These frameworks are divided into two categories , the first concerning the protection concerning data transfers within the borders of the European Union and the second dealing with data transfers to third countries either relating to European corporations or concerning citizens located in the European Union.

Further on, the thesis examines in which way the rules set by the European legislative instruments shape the compliance responsibilities for businesses that are dealing with personal data. These responsibilities are encompassed in the security plan that each corporation has to adopt in order to assess the risks that might threaten the integrity of its stored data and the ways in which such risks can be treated in the case of a threat occurring . Moreover, the role of the Data Protection Officer is analyzed and underlined for its necessity, being the key enabler for every corporation to be in compliance with the applicable legislation and securing the smooth operational activities.

The result of the thesis is that data protection has become an unquestionable right to today's technologically advanced societies with more and more citizens using the

services and products of corporations that base their business activities on the gathering of data from individuals. Data protection can be achieved by strengthening the already applicable rules that apply on the field – steps to that direction have been taken with e.g. the necessary appointment of the Data Protection Officer- and with the development and implementation of security plans according to the past and currently voted reformed legislation on data protection.

Deutsche Zusammenfassung

Das Ziel dieser Masterarbeit ist die anwendbaren Rechtsvorschriften im Bereich des Datenschutzes der europäischen Bürger und die Art und Weise, wie diese Regeln die Pflichten von Unternehmen begründen einzuführen.

Das Recht zum Datenschutz ergibt sich aus dem Recht auf Privatsphäre und es wurde als ein selbständiges Recht mit dem Vertrag über die Arbeitsweise der Europäischen Union (AEUV) eingeführt. Später wurde das Recht auf Privatsphäre in der EU – Grundrechtecharta weiter bestätigt. Seine Notwendigkeit ist offensichtlich, besonders heutzutage in der modernen Gesellschaft, wo riesige Menge von persönlichen Daten täglich von Unternehmen zu Unternehmen in der Funktion von Datenverarbeiter oder Datenverantwortlicher bei der Ausführung der täglichen Aktivitäten übertragen wird. Das Datenschutzrecht im Wesentlichen bedeutet, dass die persönliche Information Wert nicht nur als Befestigung des Privatlebens für die individuelle Person, die sie betrifft hat, aber auch für Unternehmen die im Fall von Verlust oder Zerstörung der persönlichen Daten, die sie benutzen, das Risiko eines Verlusts von Gewinn tragen.

Die Gesetzvorschriften der Europäischen Union haben eine Vielzahl von rechtlichen Rahmenbedingungen zum Schutz der Verarbeitung der persönlichen Daten europäischer Bürger von externen Bedrohungen oder bösartige Aktivitäten dargestellt. Diese Maßnahmen können in zwei Kategorien verteilt werden: die erste Kategorie betrifft den Schutz der Datenübertragung innerhalb der Grenzen der Europäischen Union und die zweite Kategorie beschäftigt sich mit der Datenübertragung zu Drittländern verbunden mit europäischen Unternehmen oder mit Bürgern dieser Drittländer, die sich innerhalb der EU befinden.

Weiterhin beschäftigt sich die Masterarbeit mit der Art und Weise, wie die europäischen Gesetzvorschriften die Konformitätsanforderungen für Unternehmen die mit persönlichen Daten arbeiten bestimmen. Diese Anforderungen müssen in einen Sicherheitsplan eingetragen sein. Jedes Unternehmen muss einen solchen Sicherheitsplan übernehmen. Mit diesem Plan werden die Risiken bewertet, die die Vollständigkeit der gespeicherten Daten bedrohen können. Zusätzlich enthält der Sicherheitsplan die Art und Weise, wie die Risiken im Fall einer Bedrohung zu behandeln. Als ein weiteres Thema analysiert diese Masterarbeit die Rolle des

Datenschutzbeauftragten. Seine Notwendigkeit muss betont sein, weil er die Grundvoraussetzung für die Konformität mit der geltenden Gesetzgebung und für die Sicherstellung eines reibungslosen Ablaufs der Tätigkeit von jedem Unternehmen ist.

Die Schlussfolgerung der Masterarbeit ist, dass das Datenschutzrecht in der heutigen technologisch anspruchsvollen Gesellschaft ein unbestreitbares Recht geworden ist. Immer mehr Menschen benutzen die Dienstleistungen und Produkte von Unternehmen, die ihr Geschäft auf der Basis der Datenerfassung von einzelnen Personen führen. Ein wirksamer Datenschutz kann durch Verstärkung der schon existierenden Regeln in dem Feld erreicht werden. Ein wichtiger Schritt in diese Richtung ist die erforderliche Anstellung eines Datenschutzbeauftragten. Eine weitere Maßnahme ist die Entwicklung und die Umsetzung eines Sicherheitsplans gemäß den alten und neuen Gesetzvorschriften in dem Feld von Datenschutz.