MASTER'S THESIS

INTERNATIONAL BUSINESS LAW

"CHALLENGES FOR THE BUSINESS WHEN COMPLYING WITH THE GENERAL DATA PROTECTION REGULATION"

Author: Vyara Gocheva

ANR: 308791

u2001823

Supervisor: Vladimir Mirkov, LLM

Tilburg,

June 2017

Acknowledgements

I would like to express my gratitude towards my parents and my brother as during my education they were always by my side supporting me, had faith in me and allowed me to realize my own potential.

To Paul: for the love and encouragement throughout the past months.

To all my friends in Sofia, Ruse, Tilburg, and all over Europe: for always being there for me.

To my academic supervisor, Mr. Vladimir Mirkov, for giving me useful advice while I was writing my thesis.

Thank you!

"*Personal data is the new oil of the internet and the new currency of the digital world*"[1]. *Meglena Kuneva, European Consumer Commissioner, 31.03.2009*.

[1] http://europa.eu/rapid/press-release_SPEECH-09-156_en.htm

Table of Contents

Abstract

Privacy and data protection have always been a priority policy for the European Union law maker. The legislation gradually developed to reach the point of adopting of the General Data Protection Regulation. Claiming to promote the protection of fundamental rights the GDPR also supports lawful business[2] procedures in order to create a balanced environment.

This master thesis inquires whether the GDPR succeeds in its initial attempts to keep the harmony between citizens and companies. What is more it identifies current challenges that certain business structures would possibly encounter when complying with the Regulation. The research outlines certain reasons which could hinder the timely adoption of the new legal concepts in the framework of the corporations.

The research includes close examination of previous, current and new legislation in order to determine concepts that could have been formulated differently or not included at all. Furthermore the thesis provides with various perspectives of scholars and professionals with the intention of preparing a complete analysis.

[2] According to the Cambridge Dictionary the word "business" has a number of definitions. For the purpose of the current research will be used the following : *"a particular company that buys and sells goods and services"* .

Introduction

Changes in socio-economic environment require proper rules to regulate the new status quo. The rapidly developing technological domain poses issues for businesses regarding the information that could be accessed and used. On the other hand, for customers and users the biggest concern remains the privacy levels and the management of the processed personal data. This master thesis examines closely the General Data Protection Regulation (from now on in the work - "GDPR") which was adopted on 27 April 2016 and will be applied from 25 May 2018. More specifically, the research focuses on the compliance process that companies should conduct during the two-year transition period.

The GDPR builds upon many existing concepts in European privacy law and creates new rights for the users whose data is being processed[3]. The result is new compliance obligations for organizations handling data. The Regulation addresses two main ideas: to strengthen and unify data privacy rules for individuals in the European Union; and to widen the territorial scope of the data protection by regulating the export of personal data of European citizens outside of the EU. It is known that the main goal of the GDPR is for both citizens and business to benefit from the new rules – common welfare has always been first priority for the EU legislator. However, the question remains on how some of the models will be implemented in practice.

The research topic "Possible challenges that business could face when complying with the GDPR" has been chosen due to the fact that as it is the latest legislation in the European Union concerning privacy data it may raise potential concerns while being applied in practice. Technological advancement creates new challenges for the lawyers and advisors in order to find the balance between the companies' progress and data protection. The work attempts to keep up with the current trends in EU law by conducting a relevant and well-structured research in the field. The questions posed and analyzed represent the future

[3] Hintze, M. (2017). Viewing the GDPR Through a De-Identification Lens: A Tool for Clarification and Compliance.

tendency of developing a relation between well-performed business strategies and shielding citizens' privacy.

Due to the fact that the GDPR contains of various new notions and tackles wide range of issues the thesis cannot pose only one research question. The study will follow series of queries which will be answered subsequently:

- What was the previous legislation, what is the basis of the legislation and what were the reason for the Reform?
- What is the content of the GDPR and which novelties do specialists in the domain find most challenging when applying the new legislation?
- Is the business prepared when it comes to complying with the GDPR and which are the main issues that companies might face?

In order to perform a reasonable study and to answer the relevant general question – what impact the Regulation will have on the business environment-, the current research is based on several methodology approaches:

- Theoretical research - analyzing works of scholars, academic papers, opinions of practicing professionals;
- Descriptive analysis - assessing the particular articles of the GDPR;
- Quantitative method - concluding results from related studies.

The intention of the work is to use resources containing the most recent and relevant information regarding business and data privacy law. The main objective of the paper is to offer comprehensive information on the topic: Possible challenges that business could face when complying with the General Data Protection Regulation (GDPR).

The thesis is divided into five parts - Introduction, 3 chapters and Conclusion. Chapter 1 presents an overview of the previous regulation regarding data privacy - on European level,

on EU level and, in particular, what is the content of Data Protection Directive 95/46/EC[4] (from now on in the thesis "the Directive"). Subsequently the query why the European Council and European Commission did decide to repeal the Directive as it was not sufficient to serve the constantly evolving privacy data environment. The part closes with what was discussed by the EU Institutions but did not become an item in the adopted Regulation. In the second chapter the GDPR itself is explained – what does the regulation focus on; which are the major changes in the GDPR - explanation of one-stop shop; consent; Privacy Impact Assessment; the definitions of data protection by design and by default; who is under its scope; what will change for the business in means of new obligations. In the third chapter the research aims to point out the main possible complications that can occur for the business while complying with the GDPR - the broadened scope of the definition of personal data; compliance costs; etc. The main focus of this part is on the question why (according to various studies) a big part of the EU companies are not ready when there is approximately one year to the effective application. Moreover some solutions that scholars and professionals suggest are assessed critically and discussed in the sense of the current research. The last part of the work is the Conclusion which summarizes the main findings of the research.

[4] 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 - http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

CHAPTER 1

1. *Legal background of data protection*

As the leading topic of the thesis is GDPR and the challenges business could face when complying with it, it is necessary to understand what is considered as the legal basis of the data protection and privacy law. For this reason Chapter 1 presents an overview of the significant documents concerning data protection and data privacy. With the intention of conducting a proper research, an overview of the phases that led to the adoption of the new GDPR in 2016 will be presented. In this part will be subsequently addressed the relevant legislation on European level, on European Union primary law and the current Directive which is still in action for the privacy data issues in EU. This phase of the research will explain the reasons and motivation standing behind the decision of the EU institutions to adopt the GDPR.

1.1 European Level

The right of privacy for the individuals is laid down in article 8 of the *Convention for the Protection of Human Rights and Fundamental Freedoms* (or European Convention of Human Rights) serving as an international legal instrument:

> *"Everyone has the right to respect for his private and family life, his home and his correspondence. "*[5]

As a fundamental right it should be respected by the natural persons and the legal persons and guaranteed by the authorities.

In view of article 8 the European Court of Human Rights ruled decisions involving misusing of personal data by business entities - unlawful storage of data[6], monitoring of employees'

[5] European Convention on Human Rights
[6] Roman Zakharov v. Russia (no. 47143/06)

computer use[7], etc. The ECtHR stated that the states not only are obliged to guarantee the citizens that violations of the Convention will be ceased; but even positive obligations are created in reassuring the respect of private life.[8]

Another international document issued by the Council of Europe concerning the privacy data issues is the *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data,* which is signed in 1981 and effective since 1985. Known also as Convention 108 it states its objective in Article 1:

> *"The purpose of this Convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection").*"[9]

When reviewing this provision the European Court of Human Rights (ECtHR) has applied rather flexible manner which includes negative obligations (e.g. "right to be alone") and positive acknowledgements (e.g. the interest of having privacy over traffic data, e-mails sent, etc.).[10]

(Note: It is interesting to be mentioned in this part that "modernisation" changes are also planned in Convention 108. In recent proposals for revision, scholars note some inspirations from GDPR and even similarities in the provisions. [11] Working groups were working on the new document and it is explained that the Convention will contain stronger rules than the existing Convention; however, the Convention will remain more general and reserved compared to the GDPR.)

[7] Bărbulescu v. Romania (no. 61496/08)
[8] Handbook on European data protection law
[9] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data
[10] Lynskey, O. (2015). The Foundations of EU Data Protection Law. *Oxford University Press*, 107.
[11] Greenleaf, G. (2017). Renewing Data Protection Convention 108: The COE's 'GDPR Lite' Initiatives .

1.2 EU level

One of the significant purposes behind the Commission's decision to reconsider the EU data protection framework was the Treaty of Lisbon which entered into force in 2009. The Treaty serves as a primary law for all the Member States. It brought major changes - constitutional and legal in the structure of the European Union.[12] First, The Lisbon Treaty gives binding force to the Charter of Fundamental Rights of the European Union. This document sets the basis of the right of data privacy of the individuals (article 7) and of data protection (article 8). As the Lisbon Treaty recognizes the binding force of the Charter, both the right to privacy and the right to data protection have been fundamental rights in the EU legal order.

Second, the Treaty itself implements the data privacy and data protection policies. With regard to data protection, in Article 16 of the Treaty on the Functioning of the European Union (TFEU) relatable concept can be found. It states that everyone has a right to data protection and increased oversight of and participation in data protection policymaking by the European Parliament.[13]

When reviewing those documents it becomes evident that a special compliance obligation is created for the companies towards their clients, users, employees, and all other persons whose data is used during the business process on a highest legal level.

2. Directive 95/45/EC

When discussing the matter of the new Regulation it is without any doubt that the Directive 95/45/EC should be revised in order to find the reasons for the legislator to repeal it and adopt the GDPR.

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

[12] The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law
[13] The same.

movement of such data ("Data Protection Directive") consists of 34 articles dealing with data privacy and data protection regulations in a specific manner. It was created as a secondary legislation and was providing an implementation period for all member states of almost 3 years. Adopted in mid 90s the EU Directive on the Protection of Personal Data was designed to regulate the constantly developing relations in the digital world. It was the first document on European level to ever tackle the questions about the protection of the right to privacy with respect to the collection, processing, storage and transmission of personal data.[14]

Before starting to revise the specific provisions, strengths and weaknesses of the Directive it is necessary to outline the context of its adoption and what it meant for personal data governance and for business. The Directive was written at a time when data processing involved methods that seemed innovative in the 1990s - filing systems and computer mainframes. Avoiding the risks related to such configurations was relatively easy by creating obligations for processors and linking different procedures to the particular operations. Its main purpose was to harmonise the existing regulations of the different countries (Member States); to guarantee the right of informational data of the subject and to remove the obstacles for free movement of personal data on the European market. However, attention must be put on the fact that it was not amongst the objectives of the Directive to create a legal framework which could address future data processing and privacy challenges.[15]

The principles considering data privacy that the 1995 Directive (as legislation with general application) set are the following:[16]

- fair and lawful processing of personal data.
- collection for specific, explicit, and legitimate purposes;
- adequacy, relevancy, and proportionality with regard to the purposes of collection and processing;

[14] Yu, P. K. (2001). An Introduction to the EU Directive on the Protection of Personal Data.
[15] Robinson N., G. H. (2009). Review of the European Data Protection Directive. *Information Commissioner's Office*.
[16] 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 - http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046

- obtaining only what is necessary for the purposes for which their personal data were collected or for which they are processed.

The 1995 Directive has to some extent an extraterritorial effect. A provision that limits cross-border transfer of personal data that is meant to be processed after transfer is included in the text - the country to which the personal data are being transferred "ensures an adequate level of protection" for them.

The Data Protection Directive generally regulates (including an exhaustive list of exceptions for processing) the collection and processing of personal data. The regime of the Directive 46/95/EC applies to a wide range of data held by both public and private organisations, imposes serious restrictions on data processing by such entities, grants broad rights to data subjects, and requires government notifications and approvals for many processing operations. In relation with that an obligation for the processor of data is created - he bears the burden of proving that the processing that he performs is lawful. [17]

Taking into consideration the current analysis of the legislation and more specifically of Directive 95/46 made in the first chapter and the different technological and legal context it is undoubtedly noted by many scholars that the current law is not sufficient to regulate the constantly changing world of collecting, transferring, amending and reusing of privacy data. However, it indeed marks the beginning of the effective privacy and data protection regulation. As professor Paul M. Schwartz notes in his monograph "The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures" Directive 95/46 has "*shaped the form of numerous laws*", even outside of the European Union. Moreover, according to prof. Schwartz the Directive "*contributed to the creation of a substantive EU model of data protection, which has also been highly influential*."

[17] Bergkamp, L. (2002). The Privacy Fallacy: Adverse Effects of Europe's Data Protection Policy in an Information-Driven Economy. *EU Data Protection Policy*.

3. *Issues*

3.1 Why the Directive is not sufficient to regulate the data privacy issues now?

Using personal data by companies is a key drive to the economic growth - it leads to efficiency and stimulates innovation in the business world. However, with more innovation come new areas that need regulation and supervision in order for the misusing of data of individuals to be prevented and for business certainty to be created while taking part in the economic processes. Having in mind the context of the Directive and the constant fast innovation process, in this part the work will assess the arguments behind the decision of the European Union to prepare a new document on privacy law and data protection.

First, as already mentioned above, the Directive on Data Protection was created to regulate already existing issues when addressing the privacy law and data protection relations; it was not designed to face upcoming challenges of the developing technological world. As internet and mobile devices have become part both of private and public life the socio-economic environment changes. The EU lawmaker started facing other challenges considering privacy law which at the time of creating the Directive did not even exist. It is not reasonable to analyse the influence and magnitude of the Directive now, from the distance of time as in the 90s it was considered a progressive document. Additionally, the gap between the regulated issues (filing systems; computer mainframes) and the existing ones (machine-learning software; AI; Legal Tech) can be overcome only by adopting new relevant legislation.

After consultation with different subjects - private, individuals, companies, agencies, etc. in 2010 the European institutions released a Communication[18] in which the reasons why it was decided to undertake the data privacy reform were highlighted. The results of the research showed the current challenges for the business environment with the existing regulation on privacy law and data protection. The authors of the document were united behind the

[18] Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions - A Comprehensive Approach on Personal Data Protection in the European Union

concept that the leading principles of the Directive were still valid and applicable. On the other hand, they supported the opinion that there were certain issues that the main attention should be focused on:

- Private individuals and business entities indicated that a clarification was needed about the application of data protection principles regarding the impact of the new technologies;
- Multinational companies have expressed concerns about "the lack of sufficient harmonization between Member states";
- The issue of applicable law was pointed out by several stakeholders - outsourcing of data processing was increasing even outside of the EU boundaries;
- In order to ensure better enforcement of the data protection legislation the DPAs should be additionally empowered;
- "Improving the coherence of the data protection legal framework".

In the next chapters it will become evident that the EU lawmaker took into account the ideas and concerns expressed in those consultations. However, some notions were either left without discussion or not elaborated in the GDPR,

3.2 What was discussed during the process of creation of the Regulation but is missing?

The "Article 29 Working Party" [19] expressed in an opinion[20] certain worries that the Directive does not contain provisions on the establishment of time limits, review and other safeguards as the limitation of use of data for serious crimes, etc. The report provides examples in order to show the absence of certain important provisions. For instance, in the Regulation exist some obligation for the controller to inform the recipient in case of a need of processing restrictions; however, this requirement only applies to transfers to third countries. It is not

[19] Article 29 of the Data Protection Directive established the "Article 29 Working Party" - Data Protection Working Party. Its purpose is to provide the European Commission with independent advice on data protection matters and helps in the development of harmonised policies for data protection in the EU Member States. http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

[20] Article 29 Data Protection Working Party - Opinion 01/2012 on the Data Protection Reform Proposals; Adopted on 23 March 2012

clear why the Regulation does not include a similar rule when personal data is transferred between Member States of the Union.

Another example is connected to the breaches of data privacy and the obligation of the competent authorities regarding this rule. The Directive provides with a possibility not an obligation for the Member States to decide if the DPA are to be responsible for the supervising.

Probably the most controversial point from the negotiations around the creations of the GDPR was the initial 5% of the total revenue established for the fines (later reduced to 4%). That approach was viewed as too business-unfriendly and after discussions was reduced and included differently in the final draft.

When taking all the factors into consideration it was evident that a revolutionary change was needed in this area and the legislator had already taken the measures in order to ensure the design of a working legislation framework in the European Union. Although certain changes were made to the initial proposal of the Commission, the final draft stayed loyal to the main concept of the EU lawmaker. In spite of the critiques and controversial opinions the GDPR is considered to be a (r)evolutionary[21] act.

[21] Mitchell, A. GDPR: Evolutionary or revolutionary? (2016); Journal of Direct, Data and Digital Marketing Practice

CHAPTER 2

1. *The General Data Protection Regulation.*

1.1. Brief chronology.

When discussing recently adopted legislation it is substantial to track the events that lead to this final step. The first stage of the process was the strategy set by the Commission in 2010. By publishing a communication, the EC showed indication that EU needs new rules to face the changing globalising world and to stay relevant to the innovative technologies. Also, the EC expressed intention to revise the Data Protection legislation as developments brought new challenges considering privacy of individuals.

Two years later, in 2012, the first proposal for Data Protection Regulation was published. The Commission's project included most of the rules that we can find now in the GDPR. However, some of them were viewed as overly restricting or on the contrary - too unbinding. That is why opinions of the Parliament followed after numerous discussions as well as amendments and new recommendations to the initial document.

Right before the Regulation was agreed on, a Trialogue meeting between the Commission, the Parliament and the Council took place. The discussions of the three institutions covered every chapter and problematic aspect until on the 15th of December 2015 the Parliament and the Council have come to an agreement. The institutions approved by voting the final draft in early April 2016.

1.2. Overview.

After years of discussion and preparation on 27 April 2016 *The Regulation (EU) 2016/679 Of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)* was adopted. It will start its application from 25 May 2018 and will repeal Directive 95/46/EC after the expiration of the two-year transition period. The GDPR

does not need additional enabling legislation to be implemented in the legislation by the Member States as it is a regulation and has a direct effect.

The GDPR was designed to modernise and harmonise the EU legislation regarding data protection. The development of technology and the innovative environment required significant changes regarding the privacy of the processed data. For the business the GDPR means undoubtedly, from one side, new obligations, structural changes and compliance costs but, from the other, most importantly, certainty and security; elimination of obstacles and the burdens concerning data transfers. By adopting the Regulation the EU institutions are acknowledging the innovation, entering the every aspect of the business system and are laying the foundations of modern legislation in harmony with the technologically advanced world.

2. Significant changes.

In this part will be commented those changes in the EU data protection legislation that are most significant for the companies. Scholars and practicing lawyers express their concerns regarding the compliance with the GDPR mainly with the below discussed concepts. There are other changes which will either only be mentioned or not discussed as they are regulated in the same manner in the previous regulation, or will not bring extreme difference in the business process.

2.1. Scope.

As a European Union direct legislation the GDPR applies to all processors/controllers in the EU. What is more, the Regulation aims to provide data protection, both for those in and outside the EU. Compared to the Directive, which focused on the "use of equipment", GDPR has an expansive approach by introducing a universal application of EU laws and regulations. When extending its scope of application to non-EU controllers or processors the new rules

bring the extraterritorial effect of the document.[22] By establishing Article 3 the GDPR is extending its scope of application to non-EU controllers or processors, where the processing activities are related to:

(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
(b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

In order to clarify the terms used by the EU legislator some scholars provide particular definitions on two slightly disputed elements of this definition. The first one - "offering goods or services"(a) implements more than simple access to a website or email address; it also might be evidenced by use of language or currency generally used in one or more Member States with the opportunity of ordering goods/ services there. The second element - "monitoring of behaviour" (b) will occur when users are tracked on the internet by algorithms which apply a profiling methods in order to enable decisions-making process. Including these two clarifications regarding processors/controllers outside the EU the legislator for the first time in EU history of legislation ensures to establish one set of rules (regarding data privacy and data protection) of the GDPR also for non-EU companies who are targeting EU citizens with marketing strategies. [23]

The Regulation will apply to companies which have EU "establishments", where personal data are processed "in the context of the activities" of such an establishment which is coming to say that regardless of the actual place of processing (EU or not) the GDPR will be valid. In the 2015 case Weltimmo v NAIH[24] the term "establishment" is revised by the Court of Justice of the European Union.[25] Some core concepts (which can be used as guiding) can be extracted from this decision:

- the concept of "establishment" is to be interpreted broadly;

[22] Burton C., De Boel L., Kuner C., Petraki A., Cadiot S., G. Hoffman S. (2016). The Final European Union General Data Protection Regulation. *Bloomberg Law: Privacy & Data Security*.
[23] Allen&Overy. (2016). The EU General Data Protection Regulation.
[24] Weltimmo v NAIH (C-230/14)
[25] Power, L. (2015). Weltimmo - The lesser-known decision of the Court of Justice of the European Union.

- the legal form of the establishment is not a determining factor - could be local agent, branch, subsidiary, sales office, etc.
- the place where the establishment is registered is not to be conclusive for the data processes;

As an additional obligation for the non-EU controllers and processors that are subject to EU data protection law an appointment of a representative in the EU is required. The role of the representative is to be addressed in addition to or instead of the controller or the processor. This rule is included mainly because of the new functions of the supervisory authorities. EU institutions intend to ensure compliance with GDPR and to guarantee that subjects of data processing are protected by having the opportunity to approach the representative regarding misuse of data. By undertaking this specific change, the legislator moves the focus of the rule on the relationship with the EU resident, rather than on the organization's place of operation.

2.2. Harmonising data protection rules.

One of the main purposes of the reform was to harmonise the data protection legislation for all Member States of the EU. In connection with that matter, there were discussions between the institutions what form exactly the legislation should be in. Taking into account the previous one - directive, now the legislator chooses the form of the regulation. The choice of legal instrument first indicates that the previous issues regarding harmonisation of EU data protection law will not exist anymore. On second place, it is evident that by including the legislation in a regulation, the Commission was pursuing the notion of having legislation that is directly applicable. Even though there is a certain period given between the adoption and the actual application of the document, the GDPR will be directly put into use and no transposition will be needed in the countries. The choice of legal instrument by the EU lawmaker illustrates the intentions of making data privacy and data protection EU concern.[26]

[26] de Hert P., P. V. (2016). The new General Data Protection Regulation: Still a sound system for the protection of individuals?. *Computer Law & Security Review*.

When the application of the GDPR starts it will harmonise data protection laws across all EU member states by applying the principle of "one single set of rules - one Union".[27] The new legislation will ensure protection of privacy in every Member state in a unified manner and will also permit free flow of personal data between the Member States.

This aspect of the change is influential not only on a citizens' level. In the globalized society that the world has turned to and respectively in harmony with the EU principles - *"free movement of goods, capital, services, and people"* (as described in the Treaty of Functioning of the European Level); there is barely a company that operates on one market. Data is constantly transferred from one point to another within the blink of an eye. By providing a harmonized legislation the EU institutions aim to grant business the opportunity to manage personal data in accordance with the same rules and principles in any territory that is under the scope of the GDPR. Moreover, the data processors/controllers will have the same obligations towards the data subjects regardless of the positions of both on the first and on the latter.

2.3. One-stop shop.

Related to the uniformity of the legislation regarding data protection is the so called "one-stop shop" provision. The concept of this rule can be found in different areas of regulation; its purpose is to avoid situations in which multiple regulators have responsibility for regulating the same activity by the same company in different Member State. In order to put in practice this rule a single, uniform decision-making process is provided.

In the context of the GDPR if a personal data controller/processor is established in two or more Member States, the EU Member State data protection authority of the place where the controller or processor has its main establishment would be able to supervise its data processing activities in all Member States.[28] Designed to ease administrative burdens for some businesses and to facilitate cross-border data transfer, the 'one-stop shop provision"

[27] CEPS Digital Forum. (2013). Online Personal Data Processing and EU Data Protection Reform.
[28] Voss, W. G. (2014). Looking at European Union Data Protection Law Reform Through a Different Prism: The Proposed EU General Data Protection Regulation Two Years Later. *Journal of Internet Law*.

saves time and money where a company is operating on territories of more than one Member State.

For multinational businesses, operating on more than one EU market, GDPR will represent a substantial change in communications with the data protection authorities. The 'one-stop shop' rule will allow companies to keep contact and predominantly deal with only one national data protection authority.[29] For instance, let us presume that a particular business is operating in all Member States; however, bigger part of the assets is located in the Netherlands. According to the GDPR this means that "the main establishments" of the company is there and the Dutch DPA will be responsible for regulating and supervising the data processes in this organisation. In order to avoid further issues the companies should concentrate the efforts on leveraging the one-stop-shop mechanism. The business will be able to consult with one leading DPA in order to design a privacy strategy based on one set of privacy risks.[30] The result is EU offices which are well-grounded and applying valid and equal management policy.

The method through which DPAs cooperate to contribute to the consistent application of the Regulation is called "consistency mechanism". In order to reach the full capacity of this mechanism EU Commission and the European Data Protection Board[31] will monitor the work of the DPA. As this is accomplished, this business avoids the situation where DPAs from different Member States establish inconsistent decisions and practices regarding the same issues.

2.4. Consent.[32]

The consent related requirements are believed to change the model of processing the data of users as GDPR enhances the conditions under it is obtained by the subjects. As in the Directive, in GDPR consent remains a lawful basis to transfer data. Despite the fact that it

[29] (2017). *Is GDPR Good or Bad News for Business? - White Paper.* ESET.
[30] Mhungu R., S. A. (2016). GDPR Top Ten: #10 - One Stop Shop. *Deloitte*.
[31] As from 2018 the Article 29 WP will transform into the European Data Protection Board. It will similarly consist of the heads of the national supervisory authorities and the EDPS. The EDPB unlike the Article 29 WP will be a independent body of the EU with its own legal personality.
[32] Maldoff, G. (2016). Part 3 – Consent. In *Top 10 operational impacts of the GDPR.* IAPP

was included in the previous law, the Regulation changes significantly the model of the definition. Compared to the Directive, GDPR makes it more difficult for companies to obtain valid consent. The previous provisions under particular circumstances allowed controllers to rely on implicit and "opt-out" consent. With the GDPR the rules become more restrictive as the companies should obtain the consent by the subject in the form of "a statement or a clear affirmative action".

According to the provisions of GDPR the consent should be: *freely given, specific, informed and unambiguous.* In order to clarify the meaning of the new definition its four elements will be analyzed.

- "*freely given*" - the consent should be given by the data subject without any pressure, threats or additional stimulation; between the data subject and the controller should exist balance; what is more the controller must not provide a service conditional upon a consent, unless, obviously, the particular processing is necessary for the service;
- "*specific*" - the given consent should be specific to each data processing operation; there are particular specificity requirements considering the consent in Article 7 of which important and relevant for this research are the consent to be "clearly distinguishable" and to be provided in an "intelligible and easily accessible form";
- "*informed*" - the data subject should be aware of the identity of the controller and of the purpose of this data processing;
- "*unambiguous*" - the consent should be expressed by "a statement or by a clear affirmative action"; the Regulation even explicitly indicates the cases which should not be viewed as an unambiguous consent: "silence, pre-ticked boxes or inactivity," are presumably an inadequate manner to confirm consent.

With those requirements the legislator creates additional hurdles for the companies to reach to the agreement of the users their data to be processed. What is even more, the Regulation is making consent more difficult at a time when technological advances such as the "big

data" analytics, machine learning engines, Artificial Intelligence, FinTech, LegalTech are making reliance on consent increasingly impractical.[33]

2.5. Controllers, joint controllers, processors.

The GDPR continues the previous trend to assign most data protection obligations and responsibilities to data controllers. Differently from the Directive, the GDPR clearly states that joint controllers could share the compliance responsibilities between them; however the users may exercise their rights against each of them.

The definition for "processors" remains the same - natural or legal person, public person, public authority, agency or other body which processes data on behalf of the data controller. However, the GDPR sets another new point connected with their responsibilities data breach reporting, direct liability towards data subjects.[34] Apart from that the processors are obligated to maintain a written record of processing activities carried out on behalf of each controller and designate a data protection officer if required. [35]

2.6. Privacy by design/by default.

The Regulation recognises two complex concepts: "privacy by design" and "privacy by default. These kinds of approaches are comparatively new to the data protection on EU level-privacy by design/by default were not included in the Directive; however, some characteristics could be found in it. According to the GDPR, in a business context the companies become the subject of an obligation according to which they should consider data privacy of the users at the very first design stages of a project as well as to the whole course of data processing.

[33] Hintze, M. (2017). Viewing the GDPR Through a De-Identification Lens: A Tool for Clarification and Compliance

[34] Voss, W. G. (2017). European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield, and the Right to Delisting. *Business Lawyer*.

[35] Allen & Overy (2016). The EU General Data Protection Regulation.

For the purpose of a better understanding and analysing of the two concepts they will be separately explained[36]:

- Privacy by design - by its means the organizations need to consider implementing the appropriate technical and organisational measures considering privacy law at the initial design stages and throughout the complete process of the new products, processes or services that involve personal data.
- Privacy by default - it indicates that when a system or a service includes choice of the data subject on the matter to what level his/hers data could be shared with other individuals, the default set should be the most privacy friendly one.

The legislator acknowledged the notion that privacy cannot be guaranteed only in legislation. By choosing to include the two new concepts (by default/by design) the EU institutions endorsed the fundamentality of privacy as a component in the design and processing of data and as a mechanism of operation for each company and organization.

2.7. Notification of breaches.

For the first time in the EU legislation the GDPR introduces a European-wide data breach notification obligation. Article 33 of the Regulation states that the authorities should be notified by the organisation within 72 hours after the breach or after becoming aware of it. This is unless the company can establish that the data breach has not caused any actual risks for data subjects. If failing to do so the controllers/processors could face fines up to 4% of global turn over or up to 20 million euro. The same fines are assigned to be paid by businesses if a DPA investigates the company and finds that the measures taken by the organisation for protection of privacy data are insufficient and therefore inadequate to the potential risk.

By setting the notification requirements in the GDPR the legislator is not only making the business obliged to share the information that an attack on privacy data has happened. What is in fact implied in the Regulation is that the companies should include categories of data, records touched, and approximate number of data subjects affected; therefore a

[36] Danon, S. (2017). GDPR Top Ten: #6: Privacy by Design and by default. *Deloitte*

detailed intelligence on what the hackers or employees are doing should be performed.[37] Moreover, data breaches requirements are not new to the legislation worldwide - they are introduced in USA, Australia; even in some Member States: UK, Italy; however the scale of the GDPR which is supported and guaranteed by the high fines takes the data breach notification to a different level and broadens the definition.

Main challenge that is posed by this requirement is the assessment of the seriousness of the data breach the company should perform. In the most common cases the information about the data breach that the company knows for is discovered in the first weeks after the actual breach. Although even if the organization is aware that there is a violation of the recordings or any other form of attack the deadline of 72 hours could appear insufficient for the organization to estimate properly the consequences for individuals. In that context it will be of a big importance for the companies, before the GDPR starts to apply, to be able to develop a scheme for assessing whether a breach poses a high risk and as a result having to be notified. It will be challengeable for business to conform to the requirement and the belonging timeframe.

2.8. Demonstrating compliance with the GDPR.

The following sections of the GDPR are as well new to the data protection legislation. They are grouped in a separate part because all of them assist organisations to demonstrate compliance with the previously discussed provisions and concepts, and with other parts of the GDPR.

2.8.1. Codes of conduct.

The idea of codes of conduct as a way of proving compliance with the data privacy law has been included in the Directive. The essential purpose of the codes of conduct stays the same in GDPR as well - they exist and are applied to the organisations so they can improve general compliance with the Regulation. However there are several new points that should be mentioned as they concern business.

[37] O'Brien, R. (2016). The new European data protection regulation and it's data breach notification requirements. *Business Information Review*.

First, more obligations are created for the DPAs considering the publication of codes of conduct. The Regulation states that drafts of the codes of conduct should be submitted to the competent DPA and approve it or amend it if necessary after which publish it. Another responsibility of the DPAs is the enforcement of the codes - the relevant Authority may appoint an independent body which should monitor the implementation of the code.

Second, in connection with the cross-border data transfers, non-EU controllers and processors can use adherence to approved codes. This provision creates opportunity for developing business internationally as it makes compliance simpler for companies that are aiming to widen their market or to connect with other non-EU partners.

2.8.2. Certification.

Certification is probably the most controversial and analyzed change that the GDPR offers for data protection. Unlike the Directive, GDPR officially recognises the certification as a legal instrument. It is one of the self-regulatory tools included in the Regulation. The certification will serve as a useful signal for consumers that certain business is trust-worthy when it comes to data protection and this business has undertaken particular measures in order to ensure that the processed data is protected. As the process is voluntary, the EU legislator promotes using third-party's schemes in order to demonstrate compliance with the data privacy law.[38]

The certification process is to be performed by an accredited certification body. In case of both granting and withdrawing the certification from the company this body should inform the supervisory authority with sufficient reasoning for such decision.

From a legal point of view, Eric Lachaud in his article "Why the certification process defined in the General Data Protection Regulation cannot be successful" gives two explanations of the certification - *"special trademark"* and *"management system".* Both of these definitions are relevant to text of the GDPR. As a "trademark" the certification guarantees the rights of the third parties, and as a "system" it marks this process or its results. However in his paper

[38] Lachaud, E. (2017). The General Data Protection Regulation Contributes to the Rise of Certification as Regulatory Instrument.

Lachaud argues if the initial concept of including the certification in the Regulation was reached by its provisions. Main reasoning of the author is that the described process is not in harmony with some of the existing EU regulation and it does not offer sufficient incentive for the business to invest in this procedure (especially for the small and medium companies). What is more the author underlines that the certification is a private attestation without legal consequences which could be problematic for the real apply of the process.

The certification process can be seen as a both burden and opportunity for business. Undoubtedly, it is connected with costs, additional documentation and reasoning. On the other hand, the required accredited certification body could create additional new business opportunities for third parties.[39] Furthermore, as business is constantly developing and cross-border data transfer is an every-day matter, this procedure will ease trade relations with countries that have already established certification (such as the USA) and could eventually lead to lower costs.

2.8.3. Data Protection Officer.

Under the GDPR certain private and most of the public organisations will be obliged to appoint a Data Protection Officer ("DPO"). The role of this position will be to monitor the companies' data processing operations. There are special thresholds set according to which organisations should mandatory appoint the DPO:

- The processor is a public authority, or
- the controller/processor performs processing which requires regular and systematic monitoring of data subjects on a broad extent;
- the controller/processor processes on a large scale of special categories of data under Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.

It is important to note that an earlier draft of the Regulation contained a different threshold - appointment of DPO was mandatory for companies with more than 250 employees. The EU

[39] Heimes, R. (2016). Part 9 - Codes of conduct and certifications. In *Top 10 operational impacts of the GDPR*. IAPP.

lawmaker most likely estimated that the criterion should not be based on quantitative measures but qualitative assessment.

As it was unclear when only reading the provisions of the Regulation what exactly would be the position of the DPOs in business. That is why in December 2016 the Article 29 Working Party published "Guidelines on DPOs" on the operation of the GDPR's provisions regarding the requirement for controllers and processors to appoint a DPO. In this document is discussed the designation, the position and the tasks of the DPO considering his/hers role in the corporate structure.

2.8.4. Data Protection Impact Assessment.

In order to evaluate the potential risks that could emerge from any new processing activity, the GDPR requires companies to conduct a Data protection impact assessment ("DPIA")). Although there some basic requirements for organisation to asses potential high-risk procedures in the old Directive, the obligation under the Regulation is new for most EU businesses.

This rule is included in the GDPR primarily because of the new technologies that are starting to take over the market. Innovation and development are "conquering" the users and unfortunately, individuals are not always entirely aware to what kind of processing they are submitting their data. The reasoning behind the new privacy legislation is complex. By assessing the potential high risks coming with the processing activity before actually applying it the controllers avoid (subsequent to the negligence) data breaches and respectively - the high fines.

For the purpose of the current research regarding the impact on business it is necessary to compare two similar procedures. The DPIA should not be confused with the general procedure of risk management.[40] What they have in common is the risk assessment - the organisation should evaluate if there is a potential high risk. What is more important is the difference - the DPIA under Article 35 of the GDPR addresses the risk for the individuals; as

[40] Bieker F., Friedewald M., Hansen M., Obersteller H., Rost M. (2016). A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation.

for the general risk management - it concerns organisations and activities. This comparison comes to say that while some risk situation under the latter could be evaluated as justifiable, there is no justifiable risk when it comes to processing of individuals' data and interfering into personal space.

2.9. New rights for the individuals.

All of the above mentioned provisions are designed to guarantee, first, the rights of the individuals and, second, to ease business-making and make it more accessible. With this in mind the analysis of the GDPR in the light of business challenges has to tackle the issues with the new rights granted to individuals. As can be observed from the research, there are certain changes mainly increasing the intensity of rights or granting completely new privileges to EU citizens. The purpose of those opportunities given to the data subjects is to involve them in the data process and not leaving them indifferent towards their own data. To put it differently, individuals are granted more functioning rights in order to take back the control of their own privacy.

2.9.1. The right to be forgotten.

The Regulation significantly broadens the opportunity of the user to demand from the controller/processor the erasure of his/hers personal data from its system and digital and written registers. If the data is no longer needed, if its unlawful to the legislation, if the subject withdraws his/hers consent, etc. the individual can call for "the right to be forgotten". The rule creates additional compliance requirement for the business as they face broader spectrum of erasure requests. Alongside this is an additional obligation to take adequate and timely actions to notify third parties that the individual has requested erasure of any references to that data.

The rationale of the institutions to include this particular procedure in the GDPR could be found in the decision of *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González* from 2014. The case put the foundation of the "right to be forgotten" as it opened the question of the liability of processors and controllers in searching engine regarding personal data. By ruling this decision the Court of Justice established a

general principle which is updated and clarified according to the changes in the digital world and is included in the GDPR.

Here another key point which often overlooked by scholars but expressed as a concern by professionals is the lack of mechanism in the business structures which can be used for performing the "erasure" of data. Alongside with this rule, organisations which are processing information on large scales should have software which determines the value of data in the light of its usage - can it be saved or it should be deleted.

2.9.2. "Pseudonymization"

The Regulation introduces another new concept for EU data protection law which is neither revealing data nor entirely identifying data when processing. The pseudonomyzation allows organisations to hold certain data so that it can be identified without additional information where both sets of data are held separately. This procedure allows the individual's identity to be preserved because the data cannot be linked to the user. For businesses it maintains the utility of the process as it allows data to be used without revealing individual's personality and reduces the risks of data breaches.

2.9.3. Data portability.

Important right that the GDPR grants to data subjects is the right to data portability. Its purpose is to provide the customer with the opportunity to obtain, reuse and transfer his/hers personal data from one data controller to another; from one IT environment to another.[41] Worth noting here is that this is viewed as one of the first steps to the so-called "Digital Single Market".[42]

Companies must provide the data in a "machine-readable" and relevant format, and data subjects have the right to transmit that data to any other controller or even under certain

[41] Guidelines on the right to data portability - Article 29 Data Protection Working Party; Adopted on 13 December 2016

[42] The "Digital Single Market" strategy has been adopted in 2015 by the European Commission. The purpose of the concept is that it will bring benefits both to business and consumers. It is believed to promote innovation, contribute nearly 500 billion euro to the EU economy each year and create numerous jobs.

circumstances controller might be required to transmit the data directly to a competitor. As this rule creates corresponding obligation for the controller it is not unlimited for the business. The GDPR specifies that there is no duty on the company to adopt particular processing systems in order to be technically compatible to transfer the data.

CHAPTER 3

1. *The concept of "data" in business context.*

Personal data included in the GDPR does not differentiate greatly from the one defined in the Directive. Generally, any expression of opinion about the individual and any indication about the individual - names, addresses, and contact details - fall under the scope. In order to let information be personal it should have the possibility to be related to an identified or identifiable natural person.[43] In the same manner as the Directive, the GDPR follows a "black/white approach" - the data are either personal or not.[44] Therefore if the data has a personal reference/identifier, all data protection rules apply; and if not, it is not under the GDPR's scope.

This approach towards the definition of 'personal data" opens two other substantial discussions - about the assessing if data is personal or public; the other one is more associated with the distinction of different types of personal data.

In the privacy law doctrine the conflict between public and private data has been widely analysed. As it is impossible to define every piece of data that is likely to occur in both psychical reality and the digital world the business should appreciate the way that the legislator choose to define "personal data". However this method creates certain unpredictability regarding the processed data. Certain information could be considered personal as well as public depending of the processor of data and of the subject of the processing.

The second point worth discussing is the "sensitive data". The text of the GDPR forbids by establishing a general prohibition on the processing of this type of data. For the purpose of understanding the essentials of the restriction we should analyse what the EU legislator

[43] *Handbook on European data protection law* (2nd ed.). (2014). European Union Agency for Fundamental Rights.

[44] Prof. Dr. Spindler G., S. P. (2016). Personal Data and Encryption in the European General Data Protection Regulation.

understands when it comes to sensitive data. There are certain criteria that the GDPR poses in order to categorize data as sensitive: explicit consent; vital interests; the capacity of the processor; the purpose of the processing. The organisation who are holding and processing such data according to the GDPR will be subjects to more restrictions and additional requirements. In both cases - defining whether data is public or not; and sensitive or not - in order to avoid being liable and subject of the fines, the business structure should perform the DPIA as it is fundamental, especially when there is potentially high risk of violations.

As expected when the data protection strategy was set in 2010, in the GDPR the material scope of the term "personal data" has been broadened. The main purpose of the EU lawmaker was to include as much as possible information that could be related to the individual as well as some extensive implications for online tracking. The changes in the range of personal data specifically includes 'online identifiers' showing the subject's online browsing behaviour - cookies, the advertising IDs seen in the mobile eco-system, IP addresses searches.

In relevance to the innovation in business-making and the new methods of assessing information a recent case will be assessed in the research. Patrick Breyer v Germany (Case 582/14) decision is tackling the issues considering what the EU understand when it comes in to personal data. According to the ruling of the Court of Justice of the European Union it is confirmed that in certain circumstances the IP addresses are personal data. The justification of the Court could influence business environment. If a controller (company) has enough information to link an IP address to a particular user then the IP is considered personal data. This could turn out challengeable for business as they should revise their policy of the methods of handling IP in various marketing and advertising activities. Bearing in mind this decision and Recital 26 of the GDPR - identifiably of subjects - the business should be cautious when estimating specific information as sufficient to disclose the identity of an individual.

Personal data has become driving power of the economy as it is used for different legal purposes such as big data analytics[45] , marketing, advertising, etc. Those activities have put business-making into other dimensions. Leading tech companies have been able to convert data into profit which turns data, according to many scholars in the business and in the tech field, into the currency of the new world. According to the researches, the value of European citizens' personal data has the potential to grow to nearly €1 trillion annually by 2020.[46]

To put it differently legislation revolution was vital for both companies and individuals. By strengthening the rules of data protection the EU law maker aims to provide the business-customer relation with balance.

2. *Possible challenges.*

2.1. New obligations for business.

By all means complying with the new obligations will be the most challenging step for companies. The GDPR changes the way how business manages data in a developing environment. Before starting the processing of data companies will have the duties to:

- According to the so called "privacy by design"- to implement in the project techniques in order to guarantee data protection to the individual. When fulfilling this requirement of the EU legislation organization must adopt significant new technical and organizational measures which will often include new software, IT specialist involved in the process and current employees' being educated by the new rules.
- As discussed in the previous chapter consent should be obtained from the subject lawfully; however, as the law is changing now it will mean for business that many of the "Terms and Conditions", "Privacy Policy", "Disclaimers" and other notices should be re-drafted in order to be relevant. Coupled to that is the rule to later demonstrate how decisions to use data for processing purposes have been given by the individual. Another point related to the consent given in advance is that It should be informed

[45] Big data refers to large amounts of data produced very quickly by a high number of diverse sources. - https://ec.europa.eu/digital-single-market/en/big-data
[46] The EU Data Protection Reform and Big Data - Fact sheet, March 2016

and intelligible. It is unlikely that consent will meet these requirements if it is given in a foreign language that the individual does not understand. When viewed from the prospective of the territorial scope context, if a consumer is "targeted" in a particular EU jurisdiction it should be assumed that the terms should be translated into the local language beforehand - this poses yet another administrative burden for the already existing data management structures. However this analytics is still a hypothesis as it is not yet clear from the provisions of the Regulation.

During the processing of data the companies should show that they are complying with the new Regulation and they are performing data governance properly:

- By appointing a DPO (mandatory or voluntarily) in certain circumstances companies demonstrate that they are relevant to the new data protection rules. Some qualitative studies (PYYKKO; LLOYD; GOLDFARB & TUCKER) suggest[47] that appointing such a figure in a company will increase the regulatory burden. Moreover, the role of the DPO could be seen as quite evasive to the companies' matter. That is why there are certain risks involved when an outside company is hired for this purpose.

  Another requirement that could be estimated as a challenge is set by the article 29 Working Party in the guidance for appointing a DPO. As the assigning of the figure is not compulsory in every case, the companies that are not obliged to appoint one are recommended to elaborate on why they are not subjects to the DPO criteria. Interestingly such a condition similar to the "comply-or-explain rule" is not included in the text of the Regulation but after its publication which means it could lead to unintentional violating the data protection rules.

- Several challenges could be outlined when a controller appoints a processor. Logically the processor should be compliant with the GDPR; however it establishes significant new conditions that must be part of each one of the data processing agreements. We could observe that processors located outside the EU will oppose to embrace these new obligations, which will result in impediments for companies to appoint their

[47] Ciriani, S. (2015). The Economic Impact of the European Reform of Data Protection.

desired processors lawfully, leading to more complexity in negotiating the contracts.[48]

- Companies should keep a full overview (documented accordingly) of the processing activities that take place and be ready to give access to those records to the DPA at any time. The organizing of records of every data processing activity in the business structure could pose certain challenges provided that in medium and big companies these kinds of processing take place in different departments and implementing certain methods could require additional effort.

When requested a termination of the data processing by a controller could take place and rights for the individuals (respective obligations for business) come into effect. They will be often connected with "the right to be forgotten" and "the right of data portability". The duty to erase the data of a subject that has requested is bond with the obligation to require from every third party handling this information to undertake the same actions. For that to be accomplished the company should again turn to its records and consult them in order to comply. Also, data should be erased when "unlawfully" processed; however this causes complications because the GDPR sets numerous reasons for unlawful processing. As there will be exemptions drafted by the Member States it creates environments for competitors to choose DPA under which supervision their cases will be administered. After choosing to erase data from a particular controller, the data subject could choose to be transferred to another one. As the "Digital Single Market" is still a strategy and not legislation there could occur some difficulties because the data will be most likely passed on to a competitor from the same area.

As the GDPR sets strict requirements regarding the data portability even in the Guidance by the Article 29 WP there is lack of clear instructions towards this rule - on the encryption requirements; on the logging and monitoring when data is transferred. All of those "gaps" create opportunities for hackers to obtain the data which, regarding the liability provisions, will be considered as an issue for the company

[48] Dr. Gabel D., Hickman T. (2016). Chapter 10: Obligations of controllers. In *Unlocking the EU General Data Protection Regulation.* White & Case.

2.2. Compliance costs.

For many companies the GDPR means more efforts and money in order to comply. The worth burden is expected to outweigh its benefits according to economic assessments of the EU data protection reform.[49] In 2013 the UK Ministry of Justice published a report [50] claiming that adjusting to the new rules will be costly for companies. They evaluate the obligations to appoint a DPO, to carry DPIA and to notify breaches as the most burdening for organisations. Moreover in the process of adopting software for data management and other new operations, additional IT specialists will be involved bringing more expenses to the organisations.

Major risk of processing personal data for the business is losing the trust of the data subjects. When undertaking different operations regarding data the companies will be monitored by the DPAs. However if a data breach is enacted or not reported to the authorities investigations and audits take place. If a non-compliant is detected this will be immediately seen by the society and in particular customers (potential data subjects of the organization).

In the event that a violation of law has been discovered not only the publicity but also severe fines will follow for the business. Recent research found that more than two-thirds of firms may face this fate.[51] Since the proposal for the GDPR from 2012 high fines have always been discussed by scholars and professionals. According to the adopted law a two-tiered sanctions regime will apply. Breaches of some provisions by companies, which the EU legislator have estimated to be most important for data protection, could lead to fines of up to €20 million or 4% of global annual turnover for the preceding financial year, whichever is the greater (for infringement of Articles 5, 6, 7 and 9). The DPA could enforce fines on businesses for the second category of violations of up to €10m or 2% of global annual turnover for the previous year, whichever is greater (for violation of articles 8,11, 25-39, 42 and 43).

[49] Ciriani, S. (2015). The Economic Impact of the European Reform of Data Protection.
[50] (2013). *Implications of the European Commission's proposal for a general data protection regulation for business.* London Economics.
[51] Two-thirds of firms may break data laws. (2016). *Network security*.

2.3. The effect of GDPR in non-EU countries.

In the previous chapter the elements of the territorial scope according to the GDPR have been analyzed. Despite being a Regulation and its aim is to harmonise EU data protection law across all Member States, the GDPR allows them to legislate in many areas. Although this may be true it comes as a binding confirmation of the existing limits on the EU legislator to interfere in internal affairs of the Members. For instance the consequences of this policy may challenge the GDPR's aim of consistency, including employee and consumers data processing. That is why recently many professionals advice their clients to "keep an eye" on the requirements which the local DPAs may pose and the guidance that are expected to be published by the European Data Protection Board.

The effect that the new legislation has on the legislation in Member States is without any doubt; however expected from the essential changes in this matter other countries will be equally influenced. Non-EU data controllers and processors must understand that by having clients from EU they have entered a new realm of data protection.

When talking about outside EU cross-border transfer of data it is essential to mention the effect that the GDPR will have on US companies. According to the new rules if a company has an establishment in the EU or is processing EU citizens' data it is under the scope of the GDPR. The currently applied "EU-US Privacy Shield" states that participating companies should have adequate levels of data protection in order to be able to transfer data. With this in mind there should be not hindrance for US companies to comply with the GDPR. On the other hand, amongst the professionals is popular other opinion. Compliant with the "Shield" is not always compliant with the GDPR as it covers only one part of the Regulation - cross-border data transfer; for instance user consent or DPOs are no included. This issue makes it clear to understand that signing up to this regime is only one of the techniques to secure the lawfulness of international data transfers.

Interesting is the case with the United Kingdom. After the positive vote on the referendum on exiting the EU ("Brexit") many businesses, scholars and professionals have indirectly started a dispute on whether or not UK should comply with the GDPR. Not only there is a

discussion over the situation but researches showed that 25% of the companies cancelled their preparations regarding the compliance.[52] In spite of all the controversies around this procedure (evoked for the first time in the EU) it is a fact that the start date of the application of the GDPR has been stated - 25.05.2018; contrarily, there great uncertainties when and how the UK will leave the Union. While studying the situations two main valid conclusions might be extracted. First, most likely UK will stop being part of the EU after the start of application of the GDPR which automatically means that UK companies should comply with the rules until its leaving; otherwise they will face the severity of the high fines. Second, even after leaving transfers of personal data outside the EU can only be performed lawfully due to the need to ensure relevant protection to personal information which under certain circumstances means direct compliance with the Regulation.

2.4. "New digital ethics".

In 2015 discussions on the "new digital ethics" started base on the opinion "Towards a New Digital Ethics" of the independent European Data Protection Supervisor". Analyzed by academics [53] this new concept is believed to facilitate the actions of adapting to the changing legislation. When it comes to processing of data all parties - processors, controllers, users - should be involved and take responsibility for their actions.

The Opinion clearly states its concern of using the so-called "mechanical compliance" - method of compliance in which the organisations strictly follow the letter of the Regulations and create checklists supporting them during the embrace of the GDPR. In order to prevent misusing of personal data the EDPS suggests the notion of the "new digital ethics" to be adopted throughout purely fundamental approach. This comes to say that the GDPR should not only be embraced on paper but its core principles should be incorporated into the design of informational systems, which assist the process of integrating the new technological advancement in the legal system. The report also underlines that aligning the data management systems with preserving users dignity might be beneficial for economic growth.

[52] Rossi, B. (2017, March 30). 1 in 4 UK businesses have CANCELLED preparations for GDPR. *Information age*.
[53] Jasmontaite, L. (2016). The European Data Protection Supervisor (EDPS) Opinion 4/2015 'Towards a New Digital Ethics':A Remedy for the EU Data Protection Framework? *European Data Protection Law Review*.

3. Data protection strategy.

Having in mind that the revolutionary legislation requires certain adjustments in the business structure, doubtlessly a data protection strategy should be developed by companies. Different scholars include numerous stages of the planning method. In this paper we are reducing them down to 5 main as defined in the Forrester's Data Security and Privacy Playbook (nevertheless they will be analyzed in a modernized context and through the perspective of the GDPR). First, the data privacy scope should be defined. By launching this step companies should consider what is the scope of their business and especially, what kind of data and where is processed. Also, how and where this data is stored and most importantly is the data that the company holds being processed lawfully and for the purpose of the business. For non-EU companies this means revising of all data-involved procedures considering EU citizens.

Second, the business should define organizational roles and responsibilities. Through the lens of the GDPR it includes appointing a DPO, a representative (for non-EU companies), etc.

Third, mapping the Regulation into the business requirements will facilitate internal control for the organisations. In this stage businesses should consider assessing the risk of data processing by conducting DPIAs.

Fourth, the companies should embed the GDPR in the already existing strategy. Analysing and "filling the gaps" of the missing requirements alongside with setting strategies (consistent with the business type) for the new notions will definitely be beneficial.

Finally, after all the previous stages are accomplished the lawfully developed process should be improved and adapted by monitoring and evaluation.

4. Consequences of non-complying.

> *"Will there be a grace period? No. You will not hear talk of grace periods from people at the ICO. That's not part of our regulatory strategy."*

This statement belongs to Information Commissioner's Office Head of International Strategy & Intelligence Steve Wood. Clearly from which could be extracted that the supervision on whether or not companies are complying with the GDPR will start from day first of the

effective application of the legislation. However, for the completeness of the research the consequences for business in case of non-complying with the new data protection provisions should be discussed.

As already mentioned as a part of the different challenges described, biggest concern for the companies appears to be the high administrative fines (up to 20 million euro or up to 4% of the turnover for the last year). Those kinds of penalties will be imposed by DPAs after comparatively (to the Directive) broad investigative and enforcement powers have been given to them by the GDPR.

Point often overlooked by companies is the right of the individual to complain to a DPA and respectively, after that to a court (established even by the CJEU in Schrems[54]). A challenge here could pose the fact that the venue of the proceedings against the DPA must be brought where it is established (not necessarily the leading DPA for the company) and proceedings against the company, logically, often will be brought to the place where the data subject resides. When complying with this rule the business could encounter difficulties because if interpreted accordingly the text of the GDPR the organisation may become a subject of proceedings of an unfamiliar jurisdiction outside the location of its main establishment.

Worth mentioning is as well the possibility of imposing criminal sanctions as it will pose significant risks for organisations. However, this rule is left on the judgement of the Member State whether or not and how to be included in the national legislation.

5. What challenges will encounter the "new" companies?

In the first Chapter we discussed the points that were discussed but were not included in the final draft of the GDPR. In this last stage of the research we will analyze the new challenges that stand before new innovative companies which are entering the market. As those businesses will doubtlessly affect the process on the data managing stage in the next decade it is essential to note what effect the GDPR will have on working companies which are

[54] Case C-362/14

adopting Artificial Intelligence (AI) software in their working process and start-ups which are actually offering AI.

Some authors believe that the roots of the AI revolution and the revolutionary legislation set in the Regulation are in the need to understand, manage and protect the enormous amount of data streaming.[55] The growth of AI raises questions about the safeguarding of the information flow and liability issues and at the same time as the trends show that operating data processes by machine-learning software opens up new business opportunities. This comes to say that companies relying on handling of personal data such as Google, Facebook, Apple, etc. will be massively exposed to risks if a third party fails to comply with the GDPR. Here comes the main concern - is the whole data collected by the AI legally processed? Is the information that the machine-learning gathered with consent of the individual for every single operation? What will happen in case of wrong decisions by the AI based on a hacked system? Which company will be liable in those cases?

As an answer to those questions could be viewed the so called "right of explanation". Its purpose is to improve the transparency when it comes to automated decision-making. The characteristics of the legal consent that was explained in the previous chapter will be valid for the AI systems as well. However, certain scholars argue the efficiency of this rule. [56] It is believed that GDPR does not provide with clarification on what will be the elements of this right. What is more there is lack of working shield against taking those automated decisions. Some scholars conclude that the efficiency of the GDPR when it comes to AI is at risk and the Regulation could not serve as a legal pillar in that matter. However, that is to be determined when the GDPR comes into force.

At the same time when attempting to regulate the upcoming technologies the EU law maker is clearly facing the Collingridge Dilemma.[57] According to it the legislator is having difficulties

[55] Rossi, B. (2017, March 21). Why businesses should be more concerned with GDPR and AI than Brexit. *Information age*. making does not exist in the General Data Protection Regulation.
[55] Moerel, E. M. L. (2014). Big data protection: How to make the draft EU Regulation on Data Protection Future Proof. Tilburg: Tilburg University.
[56] Wachter S., M. B. (2017). Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation.
[57] Moerel, E. M. L. (2014). Big data protection: How to make the draft EU Regulation on Data Protection Future Proof. Tilburg: Tilburg University.

predicting the possible effect certain novelty could have on the law system. On the other hand, once established and become part of everyday life the new technology is not easily changeable or "regulatable" or even impossible to undo or eliminate. This paradox comes to say that new and developing trends are complicated to govern or administer in legal context before they are permanently established.

From legal and ethical prospective it would be highly challenging for companies to deal with the coming technologies in the context of the GDPR as it barely tackles these kinds of issues. However, if implemented timely the appropriate data protection strategy could prevent the risk of violating the Regulation.

Conclusion

Adopting of the General Data Protection Regulation has indicated the readiness of the EU law maker to embrace the new notions in legal context. Although it is also true that the modernised legislation poses challenges for the business which they should overcome by the final step of the process of the new data privacy law - coming into force of the GDPR on 25.05.2018.

Having as a legal basis European and European Union legislation the Regulation goes further than the general terms and provides with modern concepts corresponding to the technological advancement and the legal issues it brings. Following the development of the study the thesis answered the question of the foundation of the GDPR and reasons that European institutions, academics, professionals and business itself considered as objective to seek for a legislative change in data protection - there was lack of sufficient harmonization between the Member States and the Directive was not relevant to the changing business environment.

The research also provided an examination of the important changes in the provisions of the GDPR - new definitions (privacy by design/be default), new procedures (certifications, DPIA), new obligations (appointing of DPO, obtaining of consent, notifications of breaches). The last set of research queries studied the influence that the GDPR will have on business entities in different scopes. By setting high fines, connecting the compliance with significant costs and laying new obligations for the companies the Regulation complicates the actual application of the data protection legislation and hinders the development.

As the research proved some of the companies have a long way to go before being fully ready to comply. Some of the discussed steps include appointing of a DPO; training the current staff members; investment in well-designed data protection strategies; preparing proper documents in case reporting a data breach is needed. All of the measures the business should take will enhance the corporate image of the organization.

It is evident that the GDPR incorporates new notions and unregulated before concepts which professionals and academics mark as possibly challengeable. However, the Regulation is designed to contribute to balancing the relation between a client and a company. Not only is that relevant but according to the opinion of some scholars the GDPR is believed to be beneficial for companies despite of the substantial investment before and during the compliance period.

What is important at the end of the day is if business is responsible in processing; transparent in its action and uses information properly in order to both guarantee individuals security and to maintain a better image for its brand. And will the companies be a trust worthy complaints of the GDPR only the approaching date of effective application will show.

Bibliography

Monographies and Articles

- Bergkamp, L. (2002). The Privacy Fallacy: Adverse Effects of Europe's Data Protection Policy in an Information-Driven Economy. *EU Data Protection Policy*.
- Bieker F., F. M. (2016). A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation.
- Burton C., D. B. (2016). The Final European Union General Data Protection Regulation. *From Bloomberg Law: Privacy & Data Security*.
- Burton C., De Boe L.l, Kuner C., Pateraki A., Cadiot S. and Hoffman S. (2016). The Final European Union General Data Protection Regulation. *Bloomberg Law: Privacy & Data Security*.
- Ciriani, S. (2015). The Economic Impact of the European Reform of Data Protection.
- de Hert P., P. V. (2016). The new General Data Protection Regulation: Still a sound system for the protection of individuals?. *Computer Law & Security Review*.
- Greenleaf, G. (2017). Renewing Data Protection Convention 108: The COE's 'GDPR Lite' Initiatives .
- *Handbook on European data protection law* (2nd ed.). (2014). European Union Agency for Fundamental Rights.
- Hintze, M. (2017). Viewing the GDPR Through a De-Identification Lens: A Tool for Clarification and Compliance .
- (2013). *Implications of the European Commission's proposal for a general data protection regulation for business.* London Economics.
- Jasmontaite, L. (2016). The European Data Protection Supervisor (EDPS) Opinion 4/2015 'Towards a New Digital Ethics': A Remedy for the EU Data Protection Framework? *European Data Protection Law Review*.
- Kuner, C. (2012). The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law. *Bloomberg BNA Privacy and Security Law Report*.

- Kuner, C. (2014). The European Union and the Search for an International Data Protection Framework. *Groningen Journal of International Law*.
- Lachaud, E. (2017). The General Data Protection Regulation Contributes to the Rise of Certification as Regulatory Instrument.
- Lynskey, O. (2015). The Foundations of EU Data Protection Law. *Oxford University Press*, 107.
- Mitchell, A. (2016). GDPR: Evolutionary or revolutionary? *Journal of Direct, Data and Digital Marketing Practice*.
- Moerel, E. M. L. (2014). Big data protection: How to make the draft EU Regulation on Data Protection Future; Proof. Tilburg: Tilburg University.
- O'Brien, R. (2016). The new European data protection regulation and it's data breach notification requirements. *Business Information Review*.
- (2013). *Online Personal Data Processing and EU Data Protection Reform.* CEPS Digital Forum.
- Power, L. (2015). Weltimmo - The lesser-known decision of the Court of Justice of the European Union.
- Prof. Dr. Spindler G., S. P. (2016). Personal Data and Encryption in the European General Data Protection Regulation.
- Robinson N., G. H. (2009). Review of the European Data Protection Directive. *Information Commissioner's Office*.
- Schwartz, P. M. (2013). "The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures".
- (2016). *Top 10 Operational Impacts of the GDPR.* International Association of Privacy Professionals (IAPP).
- Voss, W. G. (2014). Looking at European Union Data Protection Law Reform Through a Different Prism: The Proposed EU General Data Protection Regulation Two Years Later. *Journal of Internet Law*.
- Voss, W. G. (2017). European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield, and the Right to Delisting. *Business Lawyer*.
- Yu, P. K. (2001). An Introduction to the EU Directive on the Protection of Personal Data.

White papers

- (2017). *Article 29 Working Party guidance on GDPR.* Taylor Wessing.
- (2017). *GDPR Top Ten.* Deloitte.
- (2017). *Guide to the General Data Protection Regulation.* Bird & Bird.
- (2017). *Is GDPR Good or Bad News for Business? - White Paper.* ESET.
- Allen & Overy (2016). The EU General Data Protection Regulation.
- (2016). *The compliance burden under the GDPR – Data Protection Officers.* Taylor Wessing.
- (2016). *Unblocking the EU General Data Protection Regulation.* White & Case.

Case law

- *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González* (Case C-131/12) - judgment of the Court of Justice of the European Union
- Weltimmo v NAIH (C-230/14) - judgment of the Court of Justice of the European Union
- Patrick Breyer v Germany (Case 582/14) - judgment of the Court of Justice of the European Union
- Bărbulescu v. Romania (no. 61496/08) - Decision of the European Court of Human Rights;
- Roman Zakharov v. Russia (no. 47143/06) -Decision of the European Cpurt of Human Rights;

Legislation and documents from institutions

- 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)
- Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data
- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28.I.1981

- European Convention on Human Rights
- Charter of Fundamental Rights of the European Union
- (n.d.). Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions - A Comprehensive Approach on Personal Data Protection in the European Union.
- Laudati, L. (2016). *Summaries Of EU Court Decisions Relating To Data Protection 2000-2015.* OLAF.
- Opinion 01/2012 on the Data Protection Reform Proposals of the Article 29 Data Protection Working Party; Adopted on 23 March 2012;

Internet sources

- Rossi, B. (2017, March 30). 1 in 4 UK businesses have CANCELLED preparations for GDPR. *Information age*.
- Rossi, B. (2017, March 21). Why businesses should be more concerned with GDPR and AI than Brexit. *Information age*.
- Two-thirds of firms may break data laws. (2016). *Network security*.
- http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083
- European Commission sets out strategy to strengthen EU data protection rules: http://europa.eu/rapid/press-release_IP-10-1462_en.htm?locale=en
- http://europa.eu/rapid/press-release_SPEECH-09-156_en.htm