T.C.

MARMARA ÜNİVERSİTESİ

AVRUPA ARAŞTIRMALARI ENSTİTÜSÜ

AVRUPA HUKUKU ANABİLİM DALI

THE CERTIFICATION MECHANISM UNDER THE EU GENERAL DATA PROTECTION REGULATION

Yüksek Lisans Tezi

BİLGESU SÜMER

İstanbul - 2019

T.C.

MARMARA ÜNİVERSİTESİ

AVRUPA ARAŞTIRMALARI ENSTİTÜSÜ

AVRUPA HUKUKU ANABİLİM DALI

THE CERTIFICATION MECHANISM UNDER THE EU GENERAL DATA PROTECTION REGULATION

Yüksek Lisans Tezi

BİLGESU SÜMER

Danışman: DOÇ. DR. MUSTAFA TAYYAR KARAYİĞİT

İstanbul - 2019

TEZ ONAY SAYFASI

Marmara Üniversitesi
Avrupa Araştırmaları Enstitüsü Müdürlüğüne

Enstitünüz, Avrupa Birliği Hukuku Anabilim Dalı Türkçe / İngilizce Yüksek Lisans Programı öğrencisi **Bilgesu Sümer**, tarafından hazırlanan, **"The Certification Mechanism Under the EU General Data Protection Regulation"** başlıklı bu çalışma, 20./3.../.2019 tarihinde yapılan savunma sınavı sonucunda **OY BİRLİĞİ / ~~OY ÇOKLUĞUYA~~ "BAŞARILI"** bulunarak aşağıda isimleri yazılı jüri üyeleri tarafından Yüksek Lisans Tezi olarak kabul edilmiştir.

Jüri Üyeleri:

Doç. Dr. Mustafa T. KARAYİĞİT	Danışman	.....
Doç. Dr. Mesut Serdar ÇEKİN	Jüri Üyesi	.....
Dr. Öğr. Üy. Elif KÜZECİ	Jüri Üyesi	.....

Onay

Prof. Dr. Muzaffer Dartan
Müdür

25/03/2019 tarih ve 2019/06 sayılı Enstitü Yönetim Kurulu kararı ile onaylandı.

ABSTRACT

The thesis aims to evaluate the functions of the newly introduced certification mechanism under Article 42 of the GDPR, and its capacity to promote the principle of accountability, which is envisaged as one of the main functions of the mechanism. Furthermore, the thesis seeks to exhibit main technical and organizational elements that must be incorporated in the GDPR certification criteria, within the scope of the GDPR requirements. Finally, the thesis examines operability of the certification mechanism as an appropriate safeguard in trans-border data flows.

Key Words: The GDPR, The GDPR Certification, Data Protection Certification, Certification Criteria, EU Data Protection Law, Trans-border Data Flows, Principle of Accountability, Transparency of Personal Data Processing

ÖZET

Bu tez, Avrupa Birliği Genel Veri Koruma Tüzüğü'nun 42. Maddesi altında, yeni uygulamaya konulan veri koruma sertifikasının önemini ve bu mekanizmanın temel fonksiyonu olarak hedeflenmiş olan hesap verilebilirlik ilkesini gerçekleştirme kapasitesini değerlendirmeyi amaçlamaktadır. Ek olarak Avrupa Birliği Genel Veri Koruma Tüzüğü kapsamında sertifika kriterlerinde bulunması gereken temel teknik ve organizasyonel unsurları sunmayı amaçlamaktadır. Son olarak, tez sertifika mekanizmasının uluslararası kişisel veri akışında etkili bir tedbir olarak işlerliğini açıklamaktadır.

Anahtar Kelimeler: Avrupa Birliği Genel Veri Koruma Tüzüğü, Veri Koruma Sertifikası, Sertifika Kriterleri, Avrupa Birliği Kişisel Verileri Koruma Hukuku, Uluslararası Veri Akışı, Hesap Verilebilirlik İlkesi, Kişisel Veri İşlemede Şeffaflık

TABLE OF CONTENTS

TABLE LIST

FIGURE LIST

ABBREVIATIONS

AEDP	Agencia Espanola de Proteccion de Datos
Art	Article
Art 29 WP	Article 29 Working Party
CJEU	Court of Justice of European Union
CNIL	Commission Nationale de l'informatique et des Libertés
CPIL	Centre for Information Policy Leadership
DPIA	Data Protection Impact Assessment
DPC	Data Protection Certifications
DPO	Data Protection Officer
EDPB	European Data Protection Board
EDPS	European Data Protection Seal
EEA	European Economic Area
ENISA	European Union Agency for Network and Information Security
EU	European Union
et al.	And others
GDPR	General Data Protection Regulation
Ibid.	Above mentioned reference
IEC	The International Electrotechnical Commission
ISO	The International Organization for Standardization
OECD	The Organization for Economic Co-operation and Development
SCC	Standard Contractual Clauses
SH	Schleswig-Holstein
op. cit.	Previously mentioned reference

para.	Paragraph
p.	Page
TFEU	Treaty on Functioning of the European Union
The UK	The United Kingdom
ULD	Unabhangiges Landeszentrum für Datenschutz Schleswig-Holstein
US	The United States of America

INTRODUCTION

The rapid evolvement of the digital world brings both advantages and challenges in many aspects. It promotes global economy and electronic commerce while it provides an efficient environment to store information. Smart technologies connected to internet have become so advanced that they can even predict our basic desires or fears; they can be used for targeted marketing purposes or for the purpose of profiling or identifying us as the Court of Justice of European Union (hereinafter 'CJEU') stated:

"*those data… may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them"*.[1]

In many scenarios, technology can be used as a device to endanger the fundamental rights of the individuals, such that big data can be used for the purposes of affecting individuals' political decisions.[2] As data protection involves any processing activity from collection to transfer,[3] it is important to set rules that can protect the personal data, both in horizontal and vertical relationships.

However, in a borderless environment that has the power of transmitting the data anywhere very quickly, it is significantly more difficult to establish safeguards to protect

[1] Judgment of the Court (Grand Chamber), 8 April 2014, *Digital Rights Ireland*, C-293/12, EU:C:2014:238, para.27.

[2] Complaint and Demand for Jury Trial, State's Attorney Of Cook County, Illinois V. Facebook, INC., a Delaware Corporation, SCL GROUP LIMITED, a United Kingdom private limited company, and Cambridge Analytica LLC, a Delaware limited liability company, **https://www.cookcountystatesattorney.org/sites/default/files/files/documents/cook_county_sao-facebook_cambridge_analytica_complaint.pdf**, 10 October 2018.

[3]Elif Kuzeci, "İstatistiki Birimler ve Bilgilerin Geleceğini Belirleme Hakkı", **Insan Hakları Yıllığı**, Vol. 32, (53-75), 2014, p.65.

our personal data. Since the technology itself has no limits either, the solutions to be relied on must be as flexible as to address the problems that might occur in the future. One of the most overarching solutions to this has been recently introduced by the EU.

On 25 May 2018, the General Data Protection Regulation (hereinafter "the GDPR" or "the Regulation") entered into force within the European Union. [4] Under the GDPR, public and private entities or natural persons, which process personal data, must implement technical and organizational requirements, including the demonstration of their compliance with the GDPR. The data controllers and processors falling within the scope of the GDPR shall satisfy the rules stipulated by the Regulation. The aims of the GDPR are to enable the free flow of personal data between the Member States and to ensure trust[5] and accountability in data protection. In this regard, the GDPR has blazed a trail by introducing certification mechanisms and data protection seals and marks ("certification mechanisms") endorsed in Article 42.[6] Enhanced transparency and accountability were envisaged as the main yields of the inclusion of the certification into data protection legislations of the EU.[7]

Before the GDPR entered into force, Directive 95/46/EC ("the Directive") had been setting the global standards in the data protection domain, so that, many certification schemes were created based on the requirements enshrined in the Directive for data controllers.[8] However, each certification scheme established before the GDPR came into force, had had its own rules aiming different purposes, and thus it was not easy for the data subjects to rely on them.[9] The GDPR has introduced a new legal regime that handles

[4] 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).

[5] EU Commission, COM 2018/ 43, Commission Guidance on the Direct Application of the General Data Protection Regulation as of 25 May 2018, 24.1.2018, p.1.

[6] Article 42 of the General Data Protection Regulation (GDPR).

[7] Recital 100 GDPR.

[8] Irene Kamara and Paul De Hert, "Data Protection Certification in the EU: Possibilities, Actors and Building Blocks in a Reformed Landscape", Rowena Rodrigues and Vagelis Papakonstantinou (Ed.), in **Privacy and Data Protection Seals** (7-34), The Hague: TMC Asser Press, 2018, p. 9.

[9] Vagelis Papakonstantinou, "Introduction: Privacy and Data Protection Seals", Rowena Rodrigues and Vagelis Papakonstantinou (Ed.), in **Privacy and Data Protection Seals,** (1-6), The Hague: TMC Asser Press, 2018, p.4.

the certification issue as an integral part of the obligations of the data controller and processors.[10]

It has been seen that data protection certifications have a considerable amount of potential for ensuring accountability in data protection. However, there have been problems, including overlapping frameworks and regulatory gaps,[11] preventing deliverance of this function to the data subjects and hindering trust in data protection. Accountability is crucial for data protection to be effective since it empowers all the other principles in the field. Therefore, we can assume that if accountability is ensured by the data protection certifications ("DPCs"), significant advantages can be achieved by the certified entities, such as gaining a competitive edge in their sector and eventually making a profit. However, accountability is a "*very elusive concept*"[12] that encompasses many other concepts and prerequisites. Even though there have been many tools invented to promote accountability in data protection, did not many of them succeed in their missions. As Charles Raab points out,

"*Some innovations are of long duration, universal, respected, and implemented with varying success, while others are adopted by few and scorned by many, perhaps ultimately to be remembered only as fleeting presences on the fashion catwalks of regulatory history.*"[13]

Some authors in the domain have concerns that the newly introduced certification mechanism might remain as an inadequate regulatory measure with not considerable positive effect on the aspirations of the EU.[14] Therefore, it seems

[10] *Ibid,* p.2.

[11] Paolo Balboni and Theodora Dragan, "Controversies and Challenges of Trustmarks: Lessons for Privacy and Data Protection Seals", Rowena Rodrigues and Vagelis Papakonstantinou (Ed.), in **Privacy and Data Protection Seals** (83-111), The Hague: TMC Asser Press, 2018, p.86.

[12] Mark Bovens, "*Analysing and assessing accountability: a conceptual framework*", **European Law Journal**, Vol.13, No.4, (447–68), 2007, p.448

[13] Charles Raab, "The Meaning of 'Accountability' in the Information Privacy Context", Guagnin Daniel and Hempel Leon (Ed), in **Managing Privacy through Accountability** (15-31)**,** London: Palgrave Macmillan, 2012, p.15.

[14]Eric Lachaud, "Why the Certification Process Defined in the General Data Protection Regulation cannot be Successful", **Computer Law & Security Review,** Vol.*32*, No.6, 814-826, 2016; Douwe Korff **http://eulawanalysis.blogspot.com/2014/10/warning-eu-council-is-trying-to.html**, **(**2 September 2018).

questionable whether the GDPR certification will be able to promote accountability in data protection. Within this context, the thesis provides an insight into the problems recurring in the field, and explains the potential solutions, while evaluating the potential of the GDPR certifications to promote accountability.

Another problematic issue in the field has been the trans-border data flows. As the EU has predominantly improved the data protection rules by the GDPR, transfer of the personal data to the third countries that have less protection is likely to create conflicts. The GDPR accepts the certifications as appropriate safeguards to be relied on the trans-border data flows, when coupled with enforceable instruments. This contribution will be discussed in the last Chapter of the thesis with respect to the effectiveness of this specific tool in trans-border data flows.

1. THE METHODOLOGY AND THE SCOPE OF THE STUDY

In this study, the link between data protection certifications and their contribution to accountability is analyzed. Accountability is an umbrella term which should be analyzed in many aspects. The thesis implements an eclectic approach searching the best possible environment for DPCs to promote accountability in data protection. Accordingly, the concept has been broken down into pieces and it has been founded that there are many conditions needed to be met for ensuring accountability in data protection.

On the other hand, data protection certifications until quite recently did not attract the expected attention among scholars. Although there has been some research on certification in the fields other than data protection, such as food regulation and sustainable development,[15] the research has been very limited on the link between accountability and certifications. There are some valuable contributions made to the subject by a few scholars, but the matter still needs to be further elaborated and studied

[15] *Ibid.* Footnot 119.

particularly with regard to its relationship with accountability. The thesis proposes a useful insight into the GDPR while analyzing the various proved and envisaged contributions of the certification schemes to the data protection.

Theoretical research on the literature of data protection certifications, data protection law, privacy law, and case-law have been conducted, in order to understand what elements are envisioned to be protected under a DPC. Furthermore, to understand the current problems concerning the data protection certifications already in effect, empirical findings stated in studies have been regarded. In light of the studies on data protection certifications, I analyzed some certification schemes and pointed out their functional features that can be used as a reference to understand how the GDPR regulates the certification mechanisms.

One of the main aspects of accountability under the GDPR is the demonstration of compliance.[16] It is significant to indicate here that the certifications are not the only way to ensure the obligation of demonstrating the compliance stipulated in Article 5(2) of the GDPR. Code of conducts, which are regulated under Article 40, for instance, can be used as a means of such a demonstration. Obviously, the EU legislator has intended to make many options available for the data controllers and processors to select the best options to prove their accountability with regard to Article 5. The main point here is not in what way the compliance is being demonstrated, it is that the full accountability is demonstrated by choosing the most appropriate ways in accordance with the specific needs of the entity in question. Thus, it must be central for the entities to choose the most suitable means of demonstrating their compliance among the optional ways provided in the GDPR. However, the thesis only examines the GDPR certification mechanism, while occasionally comparing such tools with the certification mechanism, throughout the thesis.

[16] Article 5(2) of the GDPR.

Also, the thesis does not aim to evaluate the GDPR criteria since there have not been any approved criteria under the GDPR. Hence it only includes suggestions on how to refine the GDPR requirements into criteria.

2. THE OBJECTIVES AND THE OUTLINE OF THE RESEARCH

It is significant to test whether the determined tools to achieve or promote data protection are convenient to reach the goals they are directed to.[17] From this point of view, the thesis is structured based of the following research question:

How and to what extent could the GDPR certification be effective in promoting accountability as much as intended by the EU legislator?

The Chapter 1, aiming to address the historical and legal background of the data protection law, in particular its evolution in the EU legal order, tries to answer the following sub-questions:

- What is privacy, right to privacy, and right to data protection?
- What are the international instruments and principles previously developed in the domain?
- How did the data protection law evolve in the EU legal order, including within the case-law of the CJEU? How does the Court interpret the meaning of personal data, processing and the concepts of controller and processor?

Chapter 2 examines the concept of data protection certifications, seals and marks and provides an overview of Article 42 and 43 of the GDPR. A few DPCs in Europe are considered comparably effective than the others; Schleswig-Holstein, EuroPriSe and

[17] Christian De Simone, "Pitting Karlsruhe Against Luxembourg? German Data Protection and the Contested Implementation of the EU Data Retention Directive", **German Law Journal**, Vol. 11, No: 3, (291-317), 2010, p. 296.

CNIL certifications are mentioned briefly regarding their useful features. Thus, Chapter 2 aims to holistically analyze the main functions of the GDPR certification and tackle the following questions:

- What is the importance of data protection certifications?
- What is accountability and transparency and how do they relate to data protection certifications, and to each other?
- What are the problems recurring in the DPC market?

Hereafter, the thesis mainly focuses on the ability of the data protection certifications to promote accountability. It tries to exhibit the main prerequisites for accountability to test whether the GDPR provides an efficient framework that can ensure such prerequisites. In light of the literature developed on accountability in data protection, several preconditions can be determined for effective accountability. Chapter 3 first breaks the concept into pieces to show those prerequisites and each section discusses the sub-requirements for an effective DPC scheme. Therefore, the Chapter makes suggestions on how to build a DPC that can promote accountability. Chapter 3 addresses the following questions:

- How to ensure accountability through data protection certifications?
- What are the prerequisites for a certification mechanism to promote the principle of accountability?

The GDPR is considered revolutionary in the sense of its comprehensive data protection content. Thus, the GDPR certification criteria are expected to have the most protective ones in the market. To evaluate and appraise the mechanism, it is indispensable to take a holistic approach with its all aspects, including the GDPR certification criteria. That is why, the thesis provides criteria recommendations in a general sense.

Chapter 4 tests the GDPR certification against the conditions set in Chapter 3 and indicate whether these conditions can be achieved in the current system. Chapter 4

also covers suggestions to improve accountability in the current system. The last section of the Chapter scrutinizes the procedural provisions introduced for the approval of the criteria.

Chapter 5 focuses on the recurring problems in trans-border data flows from the EU to third countries, and the potential of the GDPR certification to ensure accountability in the field. It is worth to discuss what role of the data protection certifications play in trans-border data flows since the tool might be the determinant on the international conflicts of jurisdictions. Following questions are tackled in the last Chapter of the thesis:

- What are the most common accountability issues encountered within the scope of trans-border data flows?
- How and with what mechanisms does the EU try to solve these problems, particularly concerning the EU-US data flows?
- What is the function of the GDPR certification in trans-border data flows under Article 42(2) of the GDPR?
- What is the approach and procedure of the GDPR in certifying third country organizations?
- Under which circumstances, in comparison with the other safeguards, is the GDPR certification preferable by the organizations in the EU or and the third countries?
- Does the new framework provide sufficient enforceable rights to the individuals in case of breaches of the GDPR?

Throughout the thesis where necessary, the potential benefits of the GDPR certification for entities are touched upon. Finally, the thesis reaches an overall evaluation of the GDPR certification in the section of conclusion. It should be noted that, due to the nature of the subject, there is no one research question to answer and therefore there will be many answers.

CHAPTER 1: EVOLUTION OF THE EU DATA PROTECTION LAW

In order to understand whether and to what extent the GDPR certification can promote accountability in data protection, the key concepts of the domain should be analyzed in light of the developments in both international and the EU law. Section 1, starting with defining the concepts of privacy and data protection; and their differences, goes into how they have gained their current meaning and protection under international law. Section 2 presents the gradual development of data protection under the EU primary and secondary law and it briefly analyzes the importance of the GDPR. As the CJEU has remarkably contributed to the evolution of the EU data protection law, the important cases have been referred to, in relation to their contribution to the development of the key concepts, such as personal data, processing, controller and processor, in the domain.

1. PRIVACY AND DATA PROTECTION UNDER INTERNATIONAL LAW

Privacy can be described as "*a limitation of others' access to an individual*".[18] The origins of the right to privacy date back to the Roman law. However, in Roman law, the notion was not called "*privacy*" and it did not have any specific legal definition.[19] Privacy started to be seen as a value to be protected only at the end of the 19th century[20] upon repercussion effects of the French revolution. Thus, individuals have gained another

[18] Ruth E. Gavison, "Privacy and the Limits of Law", **The Yale Law Journal**, Vol. 89, No. 3, pp. 421-471, (May 2012), p.428.

[19] Bernardo Periñán, "The Origin of Privacy as a Legal Value: A Reflection on Roman and English Law", **American Journal of Legal History,** Vol.52, No.2., 183–201, 2012, p.183.

[20] Mario Viola de Azevedo Cunha, ***Market Integration Through Data Protection: An Analysis of the Insurance and Financial Industries in the EU***, 1st Edition, Dordrecht Heidelberg New York London: Springer, 2013, p.1.

personal field of life that must be legitimately protected.[21] After the end of the Second World War, the categorical framework of human rights has been enhanced and many rights have gained the status of human rights, including the right to privacy. [22]

Although privacy and data protection are not interchangeable concepts, it is reasonable to consider that the concept of data protection has emerged from the necessity to protect privacy.[23] Also, it seems practical to accept the "*human dignity*" as a mutual value to be protected both under privacy and data protection.[24]

Lynskey describes right to data protection as "*a proactive right to manage one's own personal data*".[25] Data protection aims to preserve the natural person's interest in restraining the manipulation of personal information related to them. Thus, such protection differs from the protection of privacy and goes beyond it.

Nevertheless, both of the concepts have been developed under international human rights law. The Universal Declaration of Human Rights, which was adopted by the General Assembly of the United Nations, dated 10 December 1948, has recognized the right to a private and family life in Article 12 and right to freedom of expression in Article 19. The Declaration, thereby, is considered as a starting point and the very basis of European data protection laws.[26] On the other hand, the Declaration is not legally binding, and it does not grant absolute rights to individuals as it states:

"*In the exercise of his rights and freedoms, everyone shall be subject only to such limitations as are determined by law solely for the purpose of securing due*

[21] Periñán, p.188-189.

[22] Cunha, p.2.

[23] "The Charter dedicates two articles to privacy" writes Francesca Bignami, "The Case for Tolerant Constitutional Patriotism: The Right to Privacy before the European Courts", **Cornell International Law Journal**, Vol.41, No.8, 2008, p.225.

[24] Orla Lynskey, ***The Foundations of EU Data Protection Law***, 1st Edition, Oxford University Press, 2015, p.94.

[25] *Ibid.*, p.130

[26] Sian Rudgard, "Origins and Historical Context of Data Protection Law.", Eduardo Ustaran (Ed.). in **European Privacy, Law and Practice for Data Protection Professionals**, (3-17), Portsmouth: International Association of Privacy Professionals (IAPP), 2012, p.4.

recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society".[27]

European Convention on Human Rights (ECHR) entered into force in 1953 by the initiative of the Council of Europe have a similar approach. Although the protection of privacy, family life, home, and correspondence are enshrined in Article 8, those can be constrained under the law, on the grounds of:

"*national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health and morals, or for the protection of the rights and freedoms of others"*.[28]

The first data protection law in a state level was adopted in the State of Hesse/Germany as "*Datenschutzgesetz*" in 1970. The German word "*datenschutz*" has been directly translated into English as "*data protection*".[29] In 1973, it was followed by the Swedish Datalag ("*Data Act*") which was the first national law regulating automated data processing.[30] By 1978, in Portugal, Spain and Austria data protection was recognized as a fundamental right in the Constitution.[31]

In 1980, the Organization for Economic Co-operation and Development (OECD) and the Council of Europe published the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD Guidelines). Because trans-border flows of the personal data that are not subject to any international rules would harm the privacy, the OECD Guidelines has sought to boost the international trade and economy, while setting minimum standards to protect the privacy and the rights of freedoms of

[27] Article 29(2) of the. Universal Declaration of Human Rights

[28] Article 8(2) of the European Convention on Human Rights

[29] Eleni Kosta, ***Consent in European Data Protection Law***, 3rd Edition. Boston: Martinus Nijhoff Publishers, 2013, p.44.

[30] Gloria González Fuster, **The Emergence of Personal Data Protection as a Fundamental Right of the EU**, 1st Edition, Dordrecht Heidelberg New York London: Springer Science & Business, 2014, p.58.

[31] Rudgard, p.6.

individuals.[32] Even though the OECD membership was not limited to the European States,[33] the non-binding nature of the Guidelines did not generate the expected impact on the data protection.

In 1981, the Council of Europe adopted the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108) with the purpose of particularly protecting the data stored in computerized files.[34] Convention 108 was the first internationally legally binding document which has set standards in the field of data protection.[35] Despite being not sufficient to ensure a coherent implementation across the Europe, it still remains the only legally binding international document which extends beyond the members of the Council of Europe.[36]

2. THE EVOLUTION AND LEGAL BASIS OF DATA PROTECTION LAW IN THE EU LEGAL ORDER

2.1. Directive 95/46/EC (Data Protection Directive)

The need for legislation in the field of data protection emerged at the beginning of the 1990s, from the fact that data protection laws were divergent across Europe. Although some Member States had their own data protection laws, some of them did not have any legislation in the field. For instance, France provided a relatively high level of protection to its citizens, while Italian citizens were deprived of any sort of data protection of their personal data.[37] This fact particularly was effective in hampering trans-border data flows because of the differences among the level of protection between the Member States.

[32] Council of Europe, The Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD Guidelines), Preface, Part 1, p.6.
[33] Rudgard, p.7.
[34] Rudgard, p.9.
[35] Rudgard, p.9.
[36] Rudgard, p.11.
[37] Francesca Bignami, "Cooperative Legalism and the Non-Americanization of European Regulatory Styles: The Case of Data Privacy", **American Journal of Comparative Law**, Vol.59, No.2, 411–461, 2011, p.422.

Directive 96/45 has played an important role in rendering the EU the leader in the field of personal data protection.[38] Two objectives were attributed to the Directive. The first objective was to protect the personal data; Article 1(1) of Directive established that "*Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data"*. Noticeably, Directive had enshrined data protection as a subset of the right to privacy. The second objective was to ensure the free flow of data, as stated in Article 1(2) the Directive, "*Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1*".

Article 29 of the Directive 96/45 regulated "*a Working Group on the Protection of Individuals with regard to the Processing of Personal Data*" (hereinafter the Art. 29 WP). Although the Art. 29 WP has been replaced by the European Data Regulation Board, the statements, opinions, and guidelines published by it should be considered valid as long as the Board does not publish a statement conflicting with any statement of the Art. 29 WP.

While it had been a considerable step for its own time, Data Protection Directive did not produce the intended protection, since it was not able to harmonize data protection rules across the EU.

2.2. Charter of Fundamental Rights of the European Union

In 2009, the Charter improved the status of the right to protection of personal data to the level of a fundamental right. The Charter, which has established the right to

[38] Christopher Kuner, "Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future", **OECD Digital Economy Papers**, No. 187, **http://dx.doi.org/10.1787/5kg0s2fk315f-en**, p.16.

data protection as another fundamental right, different from the right to privacy, [39] has been deemed as a binding primary law along with the Lisbon Treaty.

Article 7 Charter of Fundamental Rights of the European Union states that:

"*Everyone has the right to respect for his or her private and family life, home and communications*".

Article 8 provides that:

"1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law.

Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified."

Addition to the Charter, Article 16(1) of the TFEU also provides that *"Everyone has the right to the protection of personal data concerning them."* This means that not only the categorization of the right was changed, but also its legal status was altered by the EU legislator to ensure further protection to the right to protection of personal data. Similar to the previous documents on the issue, the relativity of the right was preserved under the Directive and the Charter.

2.3. The GDPR

Due to the fact that the method of implementation of the EU directives was left in the discretion of the Member States, there had been differences in the levels of protection existing in the in the Member States. Those discrepancies were evidently hampering the harmonization of the data protection rules across the EU, to such an extent

[39] Charlotte Bagger Tranberg, "Proportionality and Data Protection in the Case Law of the European Court of Justice", **International Data Privacy Law**, Vol.1, No.4, 239–248, 2011, p.240.

that the issue was mentioned by the European Commission as "*one of the main recurring problems*" which the data controllers operating in different Member States confront.[40]

On 25.01.2012, European Commission submitted a proposal for a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Subsequently, Directive 95/46/EC of the European Parliament and of the Council aiming to harmonize the national laws regarding the protection of personal data and to ensure the free flow of information within the EU was replaced by the Regulation 2016/679. The Regulation aims to abolish the differences in the level of protection regarding personal data in the Member States, remove the obstacles before economic activities that stem from those differences, and prevent any distorted competition in the Union.[41]

However, the GDPR does not completely harmonize the data protection rules across the EU. According to Recital 10, the GDPR allows the Member States to adopt more specific rules and further "*conditions under which the processing of personal data in lawful*". This provision provides "*a margin of manoeuvre*" for the Member States to adopt different regulations in some cases (i.e. "*sensitive data*") regulated in Article 9. Hence, one can simply claim that the aim of harmonization within the EU has not been fully accomplished by the GDPR.

Nonetheless, the GDPR has introduced more detailed and stricter data protection rules than the Data Protection Directive, as regards the matters of consent, the designation of data protection officer (DPO), data protection impact assessment, and the most important, the increased amounts of the fines in case of breaches. Further, in line with the Recital 4, which states that the personal data should be processed in order to serve the mankind, data subjects' rights under the GDPR has been enhanced to include new rights,

[40] European Commission, Commission Staff Working Paper, Impact Assessment, **https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012SC0072&from=EN**, Brussels, 25.1.2012, 72 final, Annex 2.21, 2012, p.17

[41] Recital 9 of the GDPR.

such as right to be forgotten and to data portability; the GDPR clearly grants more control to data subjects over their personal data.

Moreover, the GDPR introduces the principle of accountability to personal data protection in Article 5(2) which requires data controllers and processors to comply with the other principles enshrined in Article 5 and to be able to demonstrate this compliance. One of the most visible reflections of the principle appears to be the certification mechanism under Article 42.

Another crucial issue is that the GDPR expands the scope of its application beyond the EU; under Article 3(2), which regulates the territorial scope of the Regulation, controllers, and processors that are located outside the EU can still be responsible, if they provide or even envisage providing services and products in the EU or they monitor the behaviors of the individuals in the EU, including profiling. In such cases, under Article 27, the controller or the processor must appoint in writing a representative in the EU.

It brings changes not only with regard to the context of the data protection laws but it also differs from the former legislation with respect to its form and impact since the regulations are capable of being "*parachuted*" into the national laws of the Member States, unlike the directives.[42] This means that the EU regulations have an immediate impact on the legal systems of all the Member States when they once entered into force. However, the right to the protection of personal data is not an absolute right under the GDPR as well as under the other legal documents, since it may be restrained under certain circumstances in conformity with the principle of proportionality.[43]

2.4. Overview of the Case Law by the CJEU and the Key Terms

EU's developments in the field of data protection do not only consist of statutory codes, but it has been also formed in light of the case law of the European Court of Justice.

[42] Paul Craig and Grainne De Búrca, **EU Law : Texts, Cases and Materials**, 6th Edition, Oxford: Oxford University Press, 2015, p.108.
[43] Recital 4 of the GDPR.

Under the Directive, the Court had authorized national courts to decide the margins and necessity of the data protection rules;[44] this approach was discernably contradicting the harmonization-aspired objective of the directive. In this section, some of the seminal judgments of the CJEU will be summarized by their main points and the key terms of the data protection law will simultaneously be presented. Although the judgments that are mentioned hereinbelow were given under the Directive, they form the core values protected under the GDPR. The GDPR maintains the same definitions of "*personal data", "processing*" and "*controller*" with the Directive.

2.4.1. What is Personal Data?

To understand what constitutes personal data is crucial to apprehending the scope of both the GPDR and the GDPR certification mechanism. The Regulation maintains the definition given by the Directive. Personal data constitutes one of the components of the material scope of the GDPR and it is defined as "*any information relating to an identified or identifiable natural person (data subject)*".[45] In order to consider any data as personal data, the data concerned should belong to a living individual. Also, personal data may consist of several pieces of data that separately do not identify an individual. The Court found in *Breyer* Case that "*there is no requirement that all the information enabling the identification of the data subject must be in the hands of one person*".[46] Hence, in case there are more than one pieces of different information belonging to a specific person, the pieces must identify that particular person when they are collected together.[47] In *Linqvist* Case, it stated that working conditions and hobbies of a natural person constitutes the personal data. [48] Furthermore, the Court decided in *Nowak* Case that "*the written answers to a test, as well as the examiner's comments on those answers",* are considered as personal data. Moreover, the image of a person

[44]Judgement of 20 May 2003 *Österreichischer Rundfunk,* joined Cases C-465/00, C-138/01 and C-139/01 EU:C:2003:294, para. 88.

[45] Article 4(1) GDPR.

[46] Judgment of 19 October 2016 *Breyer*, C-582/14, EU:C:2016:779, para.43.

[47]European Commission, What is personal data ? **https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en** ,date accessed 3 May .2018.

[48] Judgment of the Court of 6 November 2003, *Linqvist,* C-101/0, *EU:C:2003:596, para.24.*

recorded by a camera in *Rynes,*[49] information related to income of natural persons in *Tietosuojavaltuutettu,*[50] records of working hours of employees in *Worten,*[51] ISP (Internet Service Provider) addresses in *Scarlet,*[52] fingerprints of individuals in *Schwarz,*[53] information related to tax in *Bara,*[54] were interpreted as personal data by the CJEU.

2.4.2. What is Processing?

Another element falls within the material scope of the GDPR is "*processing*". According to Article 4(3), *"processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means"*. Some of the processing activities are listed in Article 4 as the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction or the personal data.

Loading personal data on an internet page in *Linqvist* [55] and *Weltimmo,*[56] communication of personal data in *Jordana* cases, [57] were acknowledged by the Court as processing operations.

The Court, in *Google Spain* case, pointed out that although the processing activities carried out by a search engine differs from the ones carried out by the publishers

---

[49] Judgment of the Court (Fourth Chamber), 11 December 2014, *František Ryneš v Úřad pro ochranu osobních údajů,* C-212/13**,** EU:C:2014:2428, para. 22.

[50] Judgment of the Court (Grand Chamber) of 16 December 2008, *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy*, C-73/07, EU:C:2008:727, para. 35.

[51] Judgment of the Court (Third Chamber), 30 May 2013, *Worten*, C-342/12, EU:C:2013:355 para.19.

[52]Judgment of the Court (Third Chamber) of 24 November 2011, *Scarlet*, C-70/10, EU:C:2011:771, para. 51.

[53] Judgment of the Court (Fourth Chamber), 17 October 2013, *Michael Schwarz v Stadt Bochum,* C-291/12, EU:C:2013:670, para.27.

[54] Judgment of the Court (Third Chamber) of 1 October 2015, *Smaranda Bara and Others v Casa Națională de Asigurări de Sănătate and Others, C*-201/14, EU:C:2015:638, para. 29.

[55] *Linqvist* case. para.25.

[56] *Weltimmo* Case, para. 37.

[57] Judgment of the General Court (Eighth Chamber) of 7 July 2011, *Gregorio Valero Jordana v European Commission,* T-161/04, EU: T:2011:337, para.91.

of websites,[58] the activity of a search engine must still be considered as the processing of personal data.

2.4.3. What are Controller and Processor?

Mr. González, a Spanish national resident in Spain, lodged a complaint with Agencia Espanola de Proteccion de Datos (AEDP)[59] against La Vanguardia Ediciones SL (La Vanguardia), a company publishes daily newspapers particularly in Catalonia, for including Mr. González's name in a publication for a real-estate auction associated with attachment proceedings that had been completely resolved years ago.[60] Therefore the information provided on those web pages were irrelevant. Mr. González requested from the AEDP that La Vanguardia to be required to remove his personal data from that announcement; and secondly, he requested that Google Spain and Google Inc., to be required to remove the personal data relating to him, appearing in the results of the Google search.

The AEDP found that the complaint against La Vanguardia should be considered in the context of whether the personal data was processed on a legitimate basis. The process was legally justified because the publication had been made upon order of the Ministry of Labour and Social Affairs. However, the AEDP ruled that the operators of search engines are subject to data protection legislation since they process personal data and "*act as intermediaries, in the information society*" [61] Upon the decision of the AEDP, two separate actions brought before the Spanish National Court (Audiencia Nacional), by Google Spain and by Google Inc. were joined by the National Court.[62] The Spanish National Court requested for a preliminary ruling, under Article 267 TFEU, with regard to the obligations of the search engine.

---

[58] Judgment of the Court (Grand Chamber), 13 May 2014, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González,* C-131/12, EU:C:2014:317, para. 35.

[59] Spanish Data Protection Agency.

[60] *Google Spain* Case, para. 14.

[61] *Google Spain* Case, para. 17.

[62] *Google Spain* Case, para. 18.

The Court held that the search engines must be considered as controllers since they collect, retrieve record, store, organize, disclose personal data, even in cases where the data were initially published by a third party.[63] As a consequence, Google was found responsible as a controller, even though it was only ranking the search results. *The Google Spain* judgment is deemed as a milestone in data protection law since the Court has established the notion of "right to be forgotten" and the obligations of search engines with regard to the protection of personal data.

Three elements must be regarded to test the status of the controller: [64]

1- The controller must be a natural or legal person, public authority, agency or other bodies;

2- The controller determines the purposes and means of data processing;

3- The controller may act alone or jointly with others.

Therefore, in order to consider a natural person or entity as a "controller", one should first evaluate whether this natural person or entity determines the purposes and means of the processing of personal data. It should be noted that the controller does not have to process the personal data by itself; the data can also be processed by a processor which means a natural or legal person who processes personal data on behalf of the controller.[65] Processors act upon the written instructions of the controller, they demonstrate their compliance with the GDPR to both supervisory authorities and the controllers on which they process personal data behalf.[66] The processors may appoint sub-processors, provided that the controller provides written consent to this appointment.[67]

3. CONCLUSION

[63] *Google Spain* Case, op. cit. 48. para 21-41.

[64] Art.29 WP, WP 169, 2010, Opinion 1/2010 on the Concepts of Controller and Processor, 16 February 2010, p.7.

[65] Article 4 (8) GDPR.

[66] Article 28(1) - (3); Recital 81 GDPR.

[67] Article 28 (2)-(4) GDPR.

This Chapter has explained the personal data protection and the key terms with regard to conceptual, legal, historical aspects of the domain, in order to provide the essential information to the reader. It has been explained that privacy and data protection are different concepts developed under the international human rights law, that the right to the personal data protection is not an absolute right. The Chapter also sought to exhibit the key terms in the GDPR, which is seen revolutionary as regards with its impact on personal data protection and with its direct applicability in all of the Member States.

CHAPTER 2: DATA PROTECTION CERTIFICATIONS

1. INTRODUCTION

The aim of this Chapter is to analyze the concept and the main functions of the DPCs and the reasons behind the recurring problems in the market. For this reason, this Chapter will first discuss the general concept and functions of data protection certifications, by exhibiting the main features of some effective schemes operating in the EU (i.e. CNIL, Schleswig-Holstein and EuroPriSe Certifications). Subsequently, the reasons why the GDPR certification was introduced by the EU legislator and the context of Article 42 will be briefly analyzed. Additionally, the key terms that are used in the relevant literature will be explained in this Chapter. The last section of the Chapter focuses on the recurring problems in the market and their reasons.

2. THE CONCEPT

Certification mechanisms have been used to create public trust in the field of data protection since the 1990s.[68] Nevertheless, to define the concept is difficult due to the vast diversity existing in the organization of certification mechanisms.[69]

One of the most common adopted definitions for certification is "*third party conformity assessment*".[70] According to this view, the certification criteria are issued by a recognized authority, and the assessment is carried out by an external and accredited

[68] Papakonstantinou, p.1.

[69] Lachaud, *Why the Certification Process Defined in the General Data Protection Regulation cannot be Successful* p.3.

[70] *ISO/IEC 17067:2013 (EN) Conformity assessment -- Fundamentals of product certification and guidelines for product certification schemes*, https://www.iso.org/standard/55087.html (7 July 2018).

auditor.[71] If the assessment comes out successfully, then the formal attestation of conformity may be issued. [72]

Conformity assessment is defined as "*demonstration that specified requirements related to a product, process, system, person or body are fulfilled*".[73] Two main components are required for a conformity assessment to be called a certification.[74]

Another approach asserts that the certification is an "*attestation of conformity*".[75] Although this definition can be accepted, it misses the point that the assessment of conformity is a must in order to ensure the conformity of the subject matter to be tested.[76] A more inclusive definition also incorporating the term "conformity assessment" seems more preferable.

On the other hand, Wojtowicz defines the certification as "*the confirmation of qualities of a target of evaluation based on an existing framework*".[77] This definition seems more reasonable since it includes all of the elements required for certification. Even though I agree almost with the same definition, I would prefer defining it as "*the confirmation of certain qualities about a target of evaluation based on specific criteria by an impartial third-party*". This definition incorporates the elements of conformity assessment, scope, and target of evaluation and '*the confirmation*' here refers to '*attestation of conformity'* which is the last phase of any certification mechanism.

---

[71] Philip Eijlander et al., ***De Inkadering van Certificatie en Accreditatie in Beleid en Wetgeving***, Schoordijk Instituut, Centrum voor Wetgevingsvraagstukken, Universiteit van Tilburg, 2003, p.12, cited in Eric Lachaud, "The General Data Protection Regulation and the Rise of Certification as a Regulatory Instrument", **Computer Law & Security Review: The International Journal of Technology Law and Practice**, 2017, doi: 10.1016/j.clsr.2017.09.002, p.2.

[72] *Ibid.*, p.2.

[73] ISO/IEC 17000 Conformity assessment — Vocabulary and general principles, **https://www.iso.org/obp/ui/#iso:std:iso-iec:17000:ed-1:v1:en**, Section 2.1.

[74] *ISO/ IEC 17067 : 2013*, p.2.

[75] Lachaud, *Why the Certification Process Defined in the General Data Protection Regulation cannot be Successful* op.cit. 7, p.2. ; ISO/IEC 17000 : 2004, https://www.iso.org/obp/ui/#iso:std:iso-iec:17000:ed-1:v1:en

[76] Lachaud *Why the Certification Process Defined in the General Data Protection Regulation cannot be Successful* op.cit. 7, p.3.

[77]Monika Wojtowicz, The Idea of Data Protection Seals in Germany An Overwiev, https://dzlp.mk/sites/default/files/u4/Agenda_52179_1.pdf , 2014, Tuvit, p.4-5.

It can be noticed that the term "*privacy seal*" is widely used in the literature. A seal is defined as "*a certification mark or a guarantee issued by a certified entity*".[78] It visibly confirms the compliance of the target of evaluation with the specific standards.[79] Although the term "*privacy certification mechanisms and seals*" is commonly used in the literature, I prefer using the term *"certification"* that includes certification mechanisms, seals and marks, and "*data protection certifications*" ("DPCs") since the main focus of the thesis is the data protection certification mechanism under the GDPR.

Certification schemes may be voluntary as well as they may be mandatory. Services, products, processes and even persons can be evaluated and certified.[80] When it comes to the result of a successful certification process, there is no uniformity in practice. The outcome may be a certificate or a seal or both.[81]

3. THE DATA PROTECTION CERTIFICATIONS IN THE EU

In terms of data protection, there are already many certification schemes existing across the European Union such as, Cloud Security Alliance,[82] CNIL Label (France), ePrivacy Seal,[83] ESRB Privacy Online Certification,[84] EuroPrise, Privacy Mark System, [85] TrustArc [86] and Trustify-me Privacy Certification Seal.[87]

---

[78] Rodrigues et al., "EU Privacy Seal Project," **Inventory and Analysis of Privacy Certification Schemes**, Final Report Study Deliverable 1.4, Luxembourg: Publications Office of the European Union, 2013, p.100.

[79] *Ibid*, p.100.

[80] Wojwoticz, p.5.

[81] European Union Agency for Network and Information Security (ENISA), **Recommendations on European Data Protection Certification**, 2017, **https://www.enisa.europa.eu/publications/recommendations-on-european-data-protection-certification**, p.10.

[82] **https://cloudsecurityalliance.org/star/#_overview** , accessed on 14 July 2018.

[83] https://www.eprivacy.eu/en/privacy-seals/eprivacyseal/, accessed on 14 July 2018.

[84] http://www.esrb.org/privacy/, accessed on 14 July 2018.

[85] https://privacymark.org/, accessed on 14 July 2018.

[86] **https://www.trustarc.com/products/implement/** 14 July 2018.

[87] **http://trustifyme.org/** 14 July 2018.

Germany leads the way in the field of data protection certifications by having more than 40 certification schemes.[88] Although there is a number of active certification projects in several member states, there are only four certification projects, in Europe, founded by the public authorities.[89] According to the studies and to my own observations, three data protection certification schemes, operating in the EU, attract notice: Schleswig-Holstein, EuroPriSe and CNIL.[90]

Data Protection Act of German land of Schleswig-Holstein[91] has set the pace in the field of data protection certification by providing Unabhangiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)[92] with competence to audit, appraise and further certify the compliance of hardware, software, automated procedures and services[93] of the public institutions upon the request.[94] This certification scheme, as the oldest one, was established 15 years ago, and until 2016 it certified the compliance of 200 public bodies with the respective data protection law.[95]

EuroPriSe, as an EU-funded project, certifies the compliance of IT products and IT-based services, throughout the EU. The project took the German certification experience of Schleswig- Holstein as an example and it offers a trans-European privacy Trustmark.[96] The certification procedures of these two schemes are quite similar, the

[88] ENISA, p.23.

[89] Lachaud, *Why the Certification Process Defined in the General Data Protection Regulation cannot be Successful*, p.5.

[90] Marit Hansen, "The Schleswig-Holstein Data Protection Seal", Rowena Rodrigues and Vagelis Papakonstantinou (Ed.), in **Privacy and Data Protection Seals**, The Hague: TMC Asser Press, 2018, (35-48); Michelle Chibba, and Ann Cavoukian, "Privacy Seals in the USA, Europe, Japan, Canada, India and Australia", Rowena Rodrigues and Vagelis Papakonstantinou (Ed.), in **Privacy and Data Protection Seals** (59-82). The Hague: TMC Asser Press, 2018, p.70.

[91] According to Article 43.2 of the Data Protection Act, "Public authorities may request the ULD to audit and appraise their data protection concepts", « Öffentliche Stellen können ihr Datenschutzkonzept durch das Unabhängige Landeszentrum für Datenschutz prüfen und beur- teilen lassen », **http://www.dsb.m.itkcms.de/dokumente/160/151010084146Schleswig-Holstein.pdf**, 10 July 2018.

[92] Schleswig-Holstein Independent National Center for Privacy.

[93] Rodrigues et al., The Future of Privacy Certification in Europe: An Exploration of Options under Article 42 of the GDPR, p.16.

[94] Lachaud, *Why the Certification Process Defined in the General Data Protection Regulation cannot be Successful*, p.5.

[95] *Ibid*, p.1.

[96] *Ibid*., p.5.

applicants can even apply for a combined certification when they comply with both criteria.[97]

Another example is the French Commission Nationale de l'informatique et des Libertés (the CNIL). CNIL Label is a voluntary data protection certification which is granted by the French Data Protection Authority (CNIL) to the entities qualified, with regard to their personal data processing activities. CNIL Label operating since 2011, derives its legal basis from the Loi Informatique et Libertés Act No78-17 of 6 January 1978 on Information Technology, Data Files and Civil Liberties (the French Data Protection Act). [98]

Palut writes that CNIL Label exhibits "*a tried and tested system*" with a proven approach, indicating confidence and proof of compliance with the French Data Protection Act.[99] CNIL Label is considered one of the most successful certification schemes in the market, and it will co-operate with the EDPB to create the GDPR certification scheme. The most significant aspect of this particular scheme is that the CNIL Label is awarded for those who comply with more than necessary under the law. Thus, it goes beyond the mere compliance requirement.[100]

3.1. THE GDPR CERTIFICATION

In 2010, the Commission in its Communication on a Comprehensive Approach on Personal Data Protection in the EU identified the need for certifications in data protection and emphasized the importance of trustworthiness of such certification.[101] In the same year, the Commission was asked by the European Parliament to advance a model

[97] Hansen, p.43.

[98] Rodrigues et al., The Future Of Privacy Certification In Europe: An Exploration Of Options Under Article 42 Of The GDPR, p.16.

[99] Johanna Carvais-Palut, "The French Privacy Seal Scheme: A Successful Test", Rowena Rodrigues and Vagelis Papakonstantinou (Ed.), in **Privacy and Data Protection Seals** (49-58), The Hague: TMC Asser Press, 2018, p.51.

[100] *Ibid.*, p.51.

[101] European Commission, Communication 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, COM 609 final, Brussels, 4 November 2010.

Privacy Seal certifying a website's compliance with data protection laws.[102] The Council has supported this initiative by introducing EU certification schemes and self-regulatory initiatives involving close cooperation with industrial stakeholders, aiming higher level of data protection and raising awareness.[103]

The GDPR regulates the certification mechanism in Article 42 and Article 43. [104]Article 42(1) states that:

"*The Member States, the supervisory authorities, the [European Data Protection] Board and the European Commission shall encourage, in particular at the Union level, the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors. The specific needs of micro, small and medium-sized enterprises shall be taken into account*".

The recently introduced certification mechanism is seen as a novelty, as for the first time, the EU legislator has formally recognized, endorsed full certification and accreditation processes.[105] By virtue of its voluntary nature,[106] the certification shall be "*encouraged*" by the cooperation of Member States, the supervisory authorities, the Board and the Commission.[107]

4. THE ELEMENTS OF CERTIFICATION

Three main aspects are considered indispensable for the certification schemes: (i) target of evaluation (ii) certification criteria and (iii) evaluation approach.

4.1. Target of Evaluation (ToE)

[102] European Parliament Resolution on the Impact of Advertising on Consumer Behavior, 15 December 2010.

[103] Council of the European Union, A Comprehensive Approach on Personal Data Protection in the European Union, Council Conclusions on the Communication to the European Parliament and the Council Brussels, 2011.

[104] See also Recitals 77, 81,100, 166, 168 and Articles 24(3), 25(3), 28(5), 32(3), 46(1)(f), 57(1),(n),(p),(q), 58(1)(c), 58(2)(h), 58(3)(e) and (f), 64(c), 70(n),(o),(q), 83(2)(j).

[105] Lachaud, *The General Data Protection Regulation and the Rise of Certification as a Regulatory Instrument,* p.7.

[106] Article 42(3) of the GDPR

[107] Article 42(1) of the GDPR

A target of evaluation, or the object of certification, is the element that determines what is covered in the scope of a certification mechanism.[108] The ToE of a certification mechanism can be various. In general terms, three main components forming the scope of the GDPR certification shall be assessed during the certification process in order to assess the conformity of the ToE in question:

-Personal data (material scope);
-Technical systems (hardware and software);
-Processes and procedures related to the processing operations.[109]

The ToE can also be a specific subset of these components. The scope of the certification should not be confused with the ToE. Under Article 42, processing operations or sets of operations constitute the scope of the certification. On the other hand, the ToE varies depending on the context of each certification scheme. It can be, for instance, a part of a software or an operating system, or both, as the ToE of EuroPriSe which consists of IT products and IT-based services.[110] For example, in the context of online banking, secure log-in and online banking services constitute different ToEs.[111] It is important that the ToE is meaningful. The claims made by the certification should not be irrelevant to what certification actually certifies. It should not misguide the data subjects with respect to the qualities of the relevant products and services.[112] A proper conformity assessment can be realized only if the target of evaluation is clearly and completely defined. The ToE might be already defined by the approved criteria where a competent supervisory authority approves a specific set of criteria with regard to a specific type of activity.[113]

[108] EuroPriSe Criteria Part 1, **https://www.european-privacy-seal.eu/EPS-en/Criteria**, p.13. (8 July 2018)
[109] EDPB, p.11.
[110] Common Criteria for Information Technology Security Evaluation, Part 1, **https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf**, (8 July 2018), p.34.
[111] European Data Protection Board (EDPB), *Guidelines 1/2018* on Certification and Identifying Certification Criteria in Accordance with Articles 42 and 43 of the Regulation 2016/679, 25 May 2018, p.13.
[112] *Ibid.*, p.13
[113] *Ibid.*, p.14.

4.2. Certification Criteria

According to Article 42(7), certifications can only be issued to controllers and processors. In case that a data controller is responsible under the scope of the GDPR, after fulfilling the substantial requirements (criteria), it can apply for the certification in accordance with Article 42 and 43.

Certification criteria reflect the substantive requirements determined by an individual certification scheme. The source of the criteria varies. It can be legislation(s), or private certification bodies may develop their own criteria. When the criteria are derived from legislation, they shall correspond the requirements and principles that that legislation demands. For example, the certification criteria of Schleswig-Holstein have been developed in the light of the provisions of both the Schleswig-Holstein Data Protection Act and Data Protection Directive. [114]

4.2.1. Evaluation Process

Although the components of the evaluation stages may widely differ, certification schemes, in general, pursue the same sequence of application, evaluation, decision, the award of certification, follow-on audits and revocation if necessary.[115]

In the first stage, the entity, which has the intention to become certified (the applicant), declares its intention to the certification body either online or by means of a traditional post.[116] The applicant, in this very stage, also need to demonstrate its relevant processing activities, products or services (ToE) which can be certified under the scope of the certification scheme applied for. Typically, a committee operating under the certification body examines the admissibility of the application, pursuant to such examination if it is found admissible the evaluation stage may commence. For example,

[114] Hansen, p.36.
[115] Rodrigues, et al., *EU Privacy Seal Project,* ***Inventory and Analysis of Privacy Certification Schemes***, p. 44-45.
[116] *Ibid.,* p. 44.

the application procedure of the SH certification, starts when the applicant chooses a legal and a technical expert from a list of admitted experts, and contacts with them. The admissibility of the chosen experts is previously determined by the admission board. The following evaluation of the ToE by the admitted experts constitute the first part of the conformity assessment process. The application for the CNIL label can be submitted either by post or by online means. After the application is completed, the admissibility of the application is determined within two months.

The standards and methods for evaluation vastly differ among the existing certification schemes. Predominantly, the certification body tests the ToE against its criteria. Nonetheless, some certification schemes also assist the applicant in developing an appropriate ToE which corresponds to the criteria of the scheme. Trustify-me, for example, operates as a policy consultant as well as a certifier. Additionally, some schemes bestow extra services or guarantees to their recipients.[117]

A successful evaluation usually confers the right to use the certification to the applicant upon entering into a contract with the issuer (certification agreements) regarding the conditions on the appropriate usage of the certification. [118]

[117] Carvais – Palut, p. 44.

[118] Rodrigues, et al., *EU Privacy Seal Project,* ***Inventory and Analysis of Privacy Certification Schemes***, ap. 44.

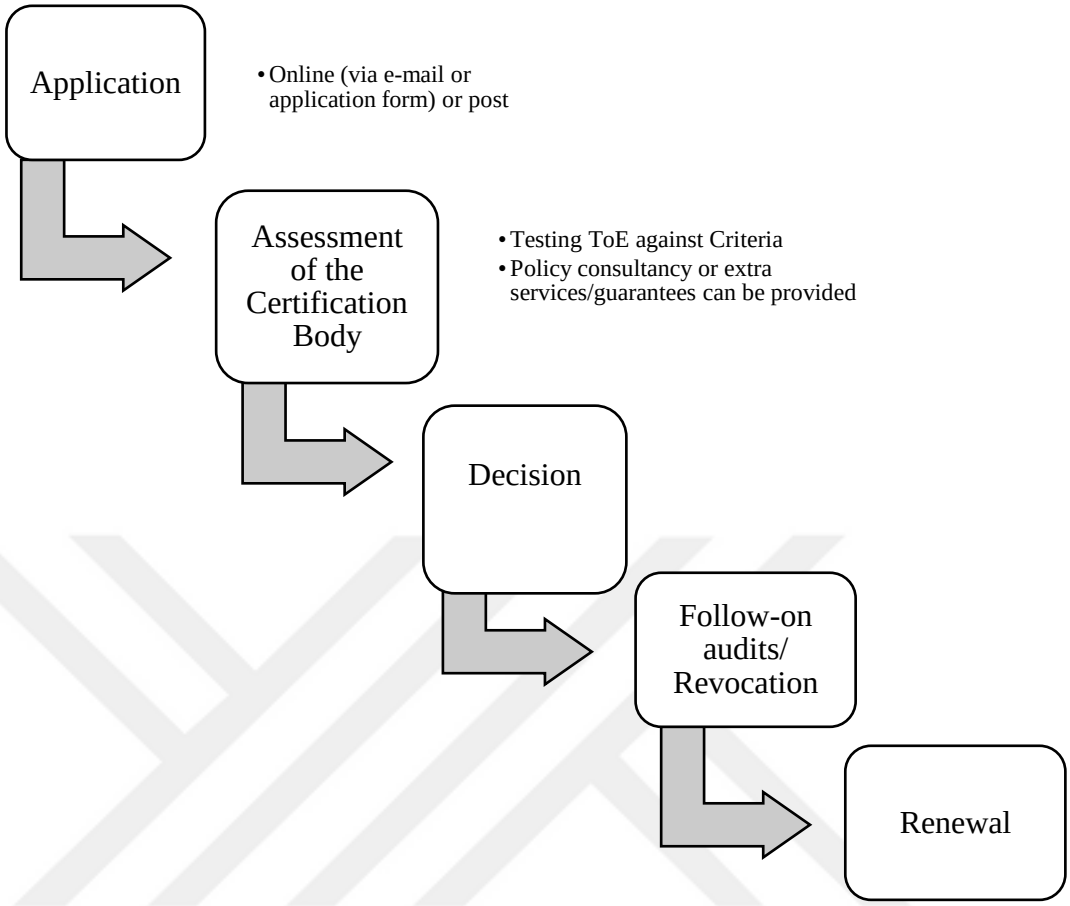

Figure 1: Stages of a typical certification process

Source: Rodrigues, et al., EU Privacy Seal Project," **Inventory and Analysis of Privacy Certification Schemes**, p. 44.

Despite being seen rare in practice, inconsistent implementation detected during follow-on audits of the criteria requires revocation of the certification, if the criteria are no longer met by the ToE previously certified. [119] Nevertheless, revocation can also occur automatically when the validity of the certification ends.

[119] Rowena Rodrigues et al. ,"The Future of Privacy Certification in Europe: an Exploration of Options under Article 42 of the GDPR", **International Review of Law**, **Computers & Technology**, Vol.30, No.3, 248-270, DOI: **10.1080/13600869.2016.1189737** , 2016, p.3.

The technical standard of the ISO/IEC 17065, which is generally used in certification processes, is also adopted by the GDPR.[120] Therefore, the process will be very similar to a typical certification process.

Figure 4: Stages of the Certification Process under the GDPR

Source: Irene Kamara and Paul de Hert, p.16.

5. THE OBJECTIVES AND IMPORTANCE OF DATA PROTECTION CERTIFICATIONS

Certifications are substantial data protection tools recognized by several stakeholders in the field.[121] This section examines the envisioned functions of the DCPs. The significance of the subject can be best examined under 3 aspects: from the perspectives of industry, the EU legal order, and the data subjects. Additionally, in this section, other relevant aspects of the DCPs will be examined.

5.1. The Importance of the DPCs for the Industry

[120] Kamara and Paul de Hert, p.16.

[121] Rowena Rodrigues et al., *EU Privacy Seal Project,"* ***Inventory and Analysis of Privacy Certification Schemes***, p.12.

Data protection certifications expectedly enable data controllers to demonstrate their full compliance with the requirements under the certification scheme they abide by. A controller or processor which is able to prove that it had already been audited in respect to its personal data processing activities would be prosperous in the eyes of both its customers and of the authorities.

Although there are no direct legal consequences stem from the compliance with a certification mechanism, data protection certifications offer practical effects for the brands which process personal data of their customers. European Data Protection Supervisor states that the controllers who are able to demonstrate their compliance via certifications are likely to gain a competitive advantage over other data controllers that do not obtain a DPC.[122] In other words, the brands economically benefit from certifications that promotes the remarkable features of their products. It is because of the fact an organization demonstrating its compliance through a compliance indicator, approved by an independent body, would be considered much reliable than one that demonstrates its compliance through its own means such as privacy notices. The annual feedbacks from the certification recipients of CNIL demonstrates that the impact of obtaining the certification, has been substantially affirmative and that the certifications usually increase the profit of the qualified entities. For instance, the recipients of the CNIL label are inclined to win the tender bids.[123]

It should also be mentioned here that the DPCs are likely to increase the preferability of processors, which have been certified their compliance, by the data controllers. Furthermore, data protection certifications appear to build trust with the partner companies as well as it enhances the trade circle of the companies.

Online shopping, unlike the traditional shopping, does not enable the buyers to assess the products on sale from many aspects, since the only information available to the

[122] "Data controllers - or even products or services - enjoying the benefit of a certification label are likely to gain a competitive advantage over others" Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions**,** OJ C 181/01, 22.06.2011, p.24.

[123] Carvais-Palut, p.55.

buyer is the pictures of the product provided by the seller itself on a website or on a smartphone application. For this reason, the majority of the online shopping platforms, also provide reviews of the previous buyers of the same products; however, in practice, the buyers only choose to shop on the platforms that are proven to be reliable. Thus, another salient role of the certification mechanisms is to promote customer trust[124] since users, usually, cannot by oneself comprehend the level of data protection that the controllers provide.[125] According to the European Commission, "*empowered and confident consumers can drive forward the European economy*".[126] Indeed, data protection certifications may empower customers, as they provide easily accessible information regarding the level of data protection to the data subjects which reduce the level of "*information asymmetry*" between the controller and data subjects.[127] The DPCs' importance in reducing the asymmetry of information between the data controllers and the data subjects will be further examined with respect to its impact on the data subjects.

5.2. The Importance of the DPCs for the EU Legal Order

The DCPs are recognized data protection tools by the governments, mainly because they have potential in reducing the regulatory and enforcement burden of the states.[128] Hence, when implemented properly they provide cost-effective solutions to data protection efforts of the Member States.

The primary reason for that, as also stated in the Opinion of Art 29WP on the principle of accountability, is that the DCPs can potentially play role in promoting

[124] Rowena Rodrigues and David Wright, "Developing a Privacy Seal Scheme (that works)", **International Data Privacy Law**, Vol. 3, No. 2 , 2013, p.101.

[125] Rowena Rodrigues et al., *EU Privacy Seal Project,"* ***Inventory and Analysis of Privacy Certification Schemes***, p.2.

[126] European Commission, Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee of the Regions, A European Consumer Agenda - Boosting confidence and growth SWD 132 final Brussels, 22.5.2012.

[127] Lachaud, "*Why the Certification Process Defined in the General Data Protection Regulation cannot be Successful*", p.7.

[128] Rowena Rodrigues et al., *EU Privacy Seal Project,"* ***Inventory and Analysis of Privacy Certification Schemes***, p.12.

accountability in data protection.[129] Accountability can be considered as "*an obligation or willingness to accept responsibility or to account for one's actions*".[130] The principle creates a burden upon data controllers and processors to take necessary measures ensuring the requirements under the data protection law.[131] It, basically, aims all the stakeholders to be held accountable where they are in violation of the laws. The concept has many dimensions, and is still evolving.

The relation between certifications and *"accountability"* can be clearly seen when considering that the certifications are the most compact ways of demonstrating compliance with legislation. The principle of accountability does not only require controllers and processors to comply with the laws, but it also requires them to demonstrate this compliance to data subjects, to society and to the public authorities. Moreover, accountability should not be regarded only as an obligation to accept responsibility, it also includes the willingness to accept responsibility. At the same time, responsiveness is a very critical aspect of accountability as it enables the public to contest the *"account"*.[132]

Bovens defines accountability as a relationship in which an actor can be held accountable by a forum that asks questions and passes judgments, including sanctions.[133] In the relationship demonstrated in Figure 2, certifications clearly play part in "*reporting, explaining and justifying*",[134] if the certification body is proved to be trusted. Therefore, the DPCs are highly relevant to the principle of accountability, since they can report that– if implemented correctly- the processing has been carried out in conformity with the certification criteria.

---

[129] Art 29 WP, WP 173, 2010 Opinion 3/2010 on the principle of accountability (24 August 2018), p.4.

[130] **https://www.merriam-webster.com/dictionary/accountability**, 10 September 2018.

[131] Paul De Hert, "*Accountability and System Responsibility: New Concepts in Data Protection Law and Human Rights Law*", Guagnin Daniel and Hempel Leon (Ed), in **Managing Privacy through Accountability** (193-232)**,** London: Palgrave Macmillan, 2012, p.201.

[132] Daniel Guagnin, Leon Hempel and Carla Ilten, *Bridging the Gap: We Need to Get Together*, Guagnin Daniel and Hempel Leon (Ed), in **Managing Privacy through Accountability** (102-124)**,** London: Palgrave Macmillan, 2012, p.119.

[133] Mark Bovens, "Two Concepts of Accountability: Accountability as a Virtue and as a Mechanism", **West European Politics**, Vol. 33, No. 5, 946–967, September 2010, p. 951.

[134] *Ibid.*, p.951.

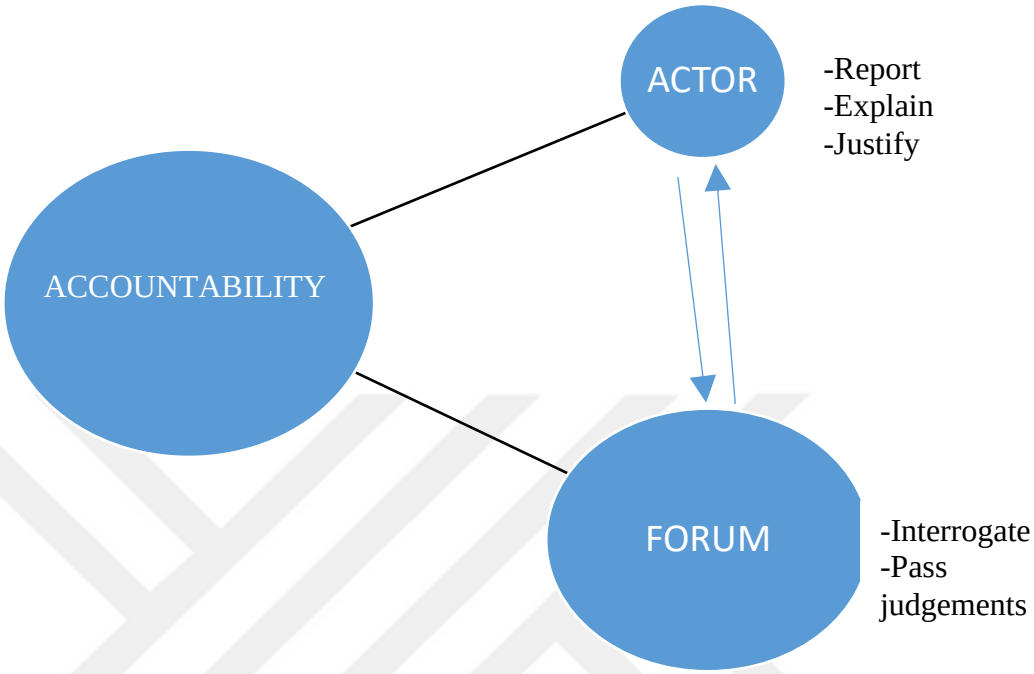

Figure 2: Accountability explained in forum-actor relationship

Source: Mark Bovens, "Two Concepts of Accountability: Accountability as a Virtue and as a Mechanism", **West European Politics**, Vol. 33, No. 5, 946–967, September 2010, p. 951.

Secondly, being regarded as transparency enhancing technologies (TETs),[135] certification mechanisms have long been used in order to enhance transparency in businesses and digital transactions.[136] In that vein, one of the envisaged functions of the certification endorsement, as provided in Recital 100 of the GDPR, is *"to enhance transparency… allowing data subjects to quickly assess the level of data protection of relevant products and services"*.[137]

[135] Christian Zimmermann, **A Categorization of Transparency-Enhancing Technologies**, https://arxiv.org/pdf/1507.04914.pdf, 1 October 2018.
[136] Kamara and De Hert, p.8.
[137] Recital 100 GDPR.

In a broad way, the concept means "*the conduct of business in a fashion that makes decisions, rules and other information visible from outside*".[138] Transparency requires proactive dissemination, which means the information made public by the authorities.[139] As supported by the majority in the literature, the principles of accountability and transparency overlap, however, they do not necessarily generate each other.[140] The relationship between the concepts will further be explained in the next Chapter.

The third function of the DPCs for the EU legal order can be seen as the harmonization of the data protection laws across the EU. However, this highly depends on the level of the accountability ensured by the mechanism in question.

5.3. The Importance of the DPCs for the Data Subjects

The DCPs are considered beneficial in facilitating the exercise of data subjects' rights. In general, people feel confident when they know that their rights are being protected. That is why data subjects who have been assured that their personal data would be safe will be more likely to share their personal data confidently with the certified data controllers.

Wojtjowicz states:

"*the statement made in data protection certificates, in combination with privacy policies, provide an excellent means for improving the transparency of data processing for data subjects and supporting them in asserting their rights*".[141]

---

[138] Christopher Hood, "*Accountability and transparency: Siamese twins, matching parts, awkward couple?*.", **West European Politics**, Vol.33, No.5, 989-1009, 2010, p. 989.

[139] Jonathan Fox, "*The uncertain relationship between transparency and accountability*." **Development in practice**, Vol.17., No. 4-5, 663-671, 2007, p. 668.

[140] Hood, p.989; Fox, p. 669.

[141] Wojtjowicz, p.2.

DPCs can play role in increasing transparency, and thus reducing the asymmetry of information between the data controller and the data subjects. Improved transparency enables the data subjects to be informed with regard to the use of their personal data, and practically, only an informed data subject can actually exercise control over his/her own personal data.[142] Plus, effective DPCs signify an official commitment to answer to data subjects' demand for information that otherwise would not be reachable.[143]

5.4. Other Relevant Aspects

One cannot consider DPCs properly without considering its impact on emerging technologies. Currently, almost all technologies facilitating humans' lives collect personal data through the devices that we can wear, carry or install in our houses. Therefore, data protection directly relates the Internet of Things (IoT) which means the network of the things, connected to the internet and to each other.

Effective DPCs that the IoTs have can show how reliable these devices are with respect to data protection. Furthermore, since the IoT are actual physical objects, the DPC can mean that they are accountable under the data protection rules of the jurisdiction in where they are located.[144] For instance, it assures the tenant of a smart house that the personal data collected by the house are not being misused. [145]

Second, DPCs have importance in cloud computing which is commonly used in the field of data protection. Having a very complex structure, cloud computing creates many issues with regard to personal data protection. The issues are mainly originated from the complex structure of the cloud that brings many privacy risks along. Thus, effective DPCs can reduce the privacy risks in cloud computing.

---

[142] Paul Voigt and Axel Von dem Bussche, **The EU General Data Protection Regulation (GDPR) A Practical Guide,** 1st Edition. Cham: Springer, 2017. p.141.

[143] Fox, p.668.

[144] Davis Barnard-Wills, "The Potential for Privacy Seals in Emerging Technologies", Rowena Rodrigues and Vagelis Papakonstantinou (Ed.), in **Privacy and Data Protection Seals**, The Hague: TMC Asser Press, (113-132), 2018, p.119.

[145] *Ibid.*, p.121.

6. RECURRING PROBLEMS IN THE FIELD

Ironically, the DPCs, in general, cannot perform their envisioned functions. Rather than enhancing transparency and accountability, they have been causing many problems endangering the protection of personal data.

In practice, it has been observed that the data certification mechanisms and seals have been used to create "*illusion of privacy protection*" .[146] According to the studies, the issuers are not considered reliable by the public, since they demonstrate biased behaviors towards their clients.[147] This is an indicator of that the desire for making profit prevails the willingness of the certification bodies to be compliant and accountable. It has been pointed out that the websites owning the TRUSTe certification are more than twice as likely to contain malware as those not certified.[148] Thus, the most salient problem in the market can be identified as the existing certification schemes not being independent and reliable. Such problems can be seen not only in the EU-based schemes, but also in the US where privacy or data protection certifications have vastly been increased in number. For example, BBB Accredited Business Seal has been criticized for being in too close relationship with scheme members, being biased towards accredited business members, and disregarding complaints. Those biased behaviors obviously damage the public trust to data protection certifications. Moreover, the counterfeit DPCs that had been proliferated in the market have reduced the reliability to the certification schemes by the public.

Self-regulation, which allows industries to operate without state involvement in their procedures, has vastly been used for long enabling DPCs to choose their criteria and procedures freely. This can be seen as the main reason why data protection certification schemes have been proliferated. Apart from that, the proliferation without state

[146] Privacy International, "Response to the European Commission's Consultation on Privacy", 2011, p.9, https://privacyinternational.org/sites/default/files/2017-12/Privacy_International_Commission_Consultation_on_Privacy_final.pdf, accessed 4 august 2018.

[147] Rowena Rodrigues et al., *EU Privacy Seal Project,"* ***Inventory and Analysis of Privacy Certification Schemes***, p.29.

[148] **Ben Edelman,** Certifications and Site Trustworthiness, http://www.benedelman.org/news-092506/**, (10 September 2018)**

involvement has brought many other problematic issues along.[149] There are plenty of overlapping frameworks trying to have an influence on the market, although most of them lack reliability. Only in Germany, there are more than 40 self-regulated data protection certification schemes which lack transparency, comparability, and common acceptance.[150] Apart from those, it has been stated in the studies that the environment in which the certifications operating is prone to be misused by the dominant actors in the market.[151]

Furthermore, it has been observed that the existing schemes offer weak guarantees that often do not correspond to what should be protected under an effective data protection certification scheme. [152] The criteria existing in the market for obtaining a certificate vary considerably. For example, SafeBuy UK does not even require any specific steps but the payment, before awarding the seal.[153] Whilst explicit guarantees to data subjects are rarely seen in schemes, the studies have shown that many DPCs offer "*abstract or poorly detailed data protection elements*" in their criteria.[154] On the other hand, some schemes openly affirming that they do not promise any legal guarantee[155] shows that the sector is highly fragmented into many different segments assuring different levels of protection.

Disabilities or difficulties in accessing the relevant information about the DPCs appear to be other problematic issues occurring in the market. It has been reported that any other private schemes provide insufficiently available information about their policies.[156] The EU Privacy Seals Project demonstrates that the information on policies

[149] Rodrigues, Barnard-Wills and Wright, *The Future of Privacy Certification in Europe: an Exploration of Options under Article 42 of the GDPR*, p.52.
[150] ENISA, p.23.
[151] The House of Lords EU Committee, **Report on Online Platforms and the Digital Single Market**, Select Committee on European Union, 2016, p.102.
[152] Rowena Rodrigues et al., *EU Privacy Seal Project,"* ***Inventory and Analysis of Privacy Certification Schemes***, p.52.
[153] Balboni and Dragan, p.102.
[154] Rowena Rodrigues et al., *EU Privacy Seal Project,"* ***Inventory and Analysis of Privacy Certification Schemes***, p.86.
[155] *Ibid.*, p.86.
[156] Rodrigues, Barnard-Wills and Wright, *The Future of Privacy Certification in Europe: An Exploration of Options under Article 42 of the GDPR*, p.53.

was either not easily accessible or not available at all in many cases.[157] Reportedly, constant name changes of the schemes, not available official web-sites along with the lack of multilingual data,[158] seems to make impossible to reach the necessary information regarding the data protection elements they claim to guarantee. It has been stated in the studies that, in some cases, the certification bodies did not response to the request for information of the research team, and in some other cases, even a contact information was not provided on their official websites.[159] Moreover, some of the schemes do not publish their criteria publicly. It is impossible for a data subject to understand what is protected under that scheme when general information concerning the DCP and/or its certification criteria are not accessible. Hence, the DCP in question would be nonfunctional, since it can neither enhance transparency nor accountability.

The studies also show that the certification bodies do not have sufficient organizational resources enabling proper conformity assessments of the target of evaluation and post-certification monitoring of the compliance of their applicants with the certification criteria.[160] As a result, they fail to detect the risks and security flaws that might impact the data subjects' rights. This can also be seen as one of the causes of the illusion of privacy originated from the lack of transparency in the field. As simply put, when there is no transparency ensured in certification processes, certification bodies may tend to act in accordance with their own interests. In case of conflicts of interests of the persons in charge of the certification processes, transparency would be at stake, which leads that the envisioned accountability to be jeopardized.

Another problem is that the DPCs do not deliver functioning complaint and enforcement mechanisms.[161] There are either no complaint mechanisms at all, or there is no information regarding the process. It has been observed that in many cases, complaint

[157] The aim of the project was to reveal the weaknesses of the existing privacy and data protection certifications so that the ones being developed can guarantee that the same mistakes would be avoided in the future.
[158] Balboni and Dragan, p.93.
[159] Rowena Rodrigues et al., *EU Privacy Seal Project,"* ***Inventory and Analysis of Privacy Certification Schemes***, p.29.
[160] Rodrigues, **Privacy and Data Protection Seals**, p.150.
[161] *Ibid.*, p.150.

and dispute mechanisms the schemes offer operate entirely internal, not allowing the involvement of independent bodies into the process.[162] Consequently, the data subjects either cannot complain about the implementations of the schemes or the complaint mechanism do not produce fair results.

The problems in the field can be further exemplified as the lack of competition between private stakeholders on data protection standards.[163] The lack of competition appears to stem from the fact that there have been no incentives for the DPCs to be compliant with the data protection laws. As mentioned, under such circumstances, it is not possible for the public to trust the certification schemes unless the environment they operate is changed in a positive manner.

7. CONCLUSION

There are many functions attributed to the DPCs. With respect to the private sector, the DPCs can potentially increase the customer trust and therefore they can increase the profit of the respective organizations. In the EU legal order and beyond, the DPCs are expected to become accountability tools in data protection.

Another implication that can be inferred is that the data protection certifications have the potential of enhancing transparency, whereas the principle of transparency itself is a necessary element to be ensured in a data protection certification scheme for ensuring the principle of accountability and improving the data subject's rights.

The visual demonstration of compliance via DPCs reduces the asymmetry of information and thus enables quick access to the data protection level of the respective products and services.

---

[162] Rowena Rodrigues et al., *EU Privacy Seal Project,"* ***Inventory and Analysis of Privacy Certification Schemes***, p.89.

[163] The House of Lords EU Committee, **Report on Online Platforms and the Digital Single Market**, Select Committee on European Union, 2016, p.102.

Since the DPCs can reduce the asymmetry of information between data controllers and data subjects, they have the potential for enhancing transparency in data protection. In relation to the data subjects, they present an official commitment which demonstrates that their personal data are being handled lawfully. Finally, the DPCs can be useful tools of accountability in the fields of cloud computing and the IoTs.

The problems in the sector vary. First of all, despite being easily accessible, the information signified by the data protection certification may not reflect the reality when the issuers' commercial focus is in question. Second, due to the self-regulated approach to certifications, there are many DPCs de facto operating in the EU by offering weak guarantees with respect to the protection of personal data. This fragmentation in the market causes that the data controllers and processors to apply for the frameworks requiring easier criteria. Although there are plenty of schemes allegedly guaranteeing transparency and accountability in data protection, it seems that they cause problems instead of solving them.

Such shortcomings enable the data controllers to make a profit without ensuring the compliance with the standards they promise for their users. In a sense, data protection certifications can be used for shielding the violations of data protection rights pledged under that certification scheme.[164] In such cases, data subjects may provide much more information relating to their personal data to the controller, only because they trust the certification mark claiming the data controller ensures the appropriate data protection.[165] As transparency is needed for the sake of data subjects' rights, it cannot be expected from the data subjects to easily invoke their rights in such an unclear environment. Besides, those facts demonstrate the necessity to a regulatory system that regulates trusted third parties as certification bodies.

Similar to the existing ones, the GDPR certification, has also been introduced as a tool aimed to enhance transparency and accountability in the field. Since there has yet

[164] Rodrigues, Wright and Wadhwa, *Developing a Privacy Seal Scheme (that works)*, p.106.

[165] Natalie L. Regoli, "Indecent Exposures in an Electronic Regime," **Federal Communications Law Journal,** Vol. 54, No.,2, 2002, cited in Rodrigues Wright and Wadhwa, *Developing a Privacy Seal Scheme (that works)*, p.107.

been no scheme approved under Article 43 of the GDPR, it is still unknown whether the mechanism would be successful in realizing its objectives which are enhanced transparency and accountability in data protection. Designing and implementing an effective DPC framework require a detailed analysis presenting the empirical findings on how to build an effective DPC.

When observed carefully, one can notice that all the objectives can be achieved if the accountability is ensured by the GDPR certification. The effectiveness of a DPC can be measured by the extent of the 'account' it can give to the data subjects. Therefore, it can be said that the effectiveness of the mechanism principally depends on whether it will ensure the envisaged accountability or not. Another issue to consider is that transparency is a prerequisite for accountability and that an effective mechanism cannot be established without transparency. Therefore, accountability can be deemed as both the solution and the objective within the EU and beyond. However, introducing such a principle cannot be sufficient without enclosing it into a solid system with concrete measures to be carried out by the data controllers and processors.[166] The next Chapter of the thesis will discuss how to ensure accountability in the field of DPCs and what components should be taken into account in order to ensure the envisioned accountability.

[166]De Hert, "*Accountability and System Responsibility: New Concepts in Data Protection Law and Human Rights Law*", p.201.

CHAPTER 3: SUGGESTED SOLUTION: EFFECTIVE ACCOUNTABILITY IN DATA PROTECTION CERTIFICATIONS

As previously stated, data protection certifications play a role in potentiating the principle of accountability, which is, in fact, an overarching principle that renders the other data protection principles more effective.[167] However, as explained, many problems still remaining in the field of data protection certifications, including lack of transparency and customer trust, meaning that the data protection certifications in the market are not sufficient to ensure accountability.

The potential effectiveness of a DPC closely depends on its ability to solve the problems hampering from a DPC to function as intended. This means that if an effective certification scheme is created, the recurring problems in the market could be eliminated. Having said that, how to exactly create an ideal DCP appears to be a conundrum since such DCP is expected to solve many problematic issues arising from the DCPs themselves. That is why it is crucial to address how to provide accountability regarded as the desired outcome of a DPC and the prerequisites which are considered necessary for ensuring accountability via an ideal DPC.

This Chapter unpacks the concept of accountability within the context of data protection certifications. To do that, the questions of why transparency must be regarded as a pre-condition for accountability, what is the best legislative environment for data protection certifications, why the certification criteria are significant for effective accountability, what is the importance of enforcement mechanisms with regard to DPCs and accountability will be addressed.

[167] Daniel Rucker and Tobias Kugler, **New European General Data Protection Regulation A Practitioner's Guide Ensuring Compliant Corporate Practice**, 1st Edition, Munich: C.H. Beck, Nomos, Hart Publishing, 2018, p.73.

Section 2 conceptually discusses transparency and its prerequisites which are regarded as *sine non-qua* in the context of data protection certifications. Transparency under this Chapter should not be confused with the previously mentioned "transparency" that is one of the envisaged functions of data protection certifications. It will be addressed as the main prerequisite for achieving the principle of accountability within the scope of data protection certifications.

Section 3 tries to reveal the most appropriate approaches to eliminate the problems arising out of the proliferation in the market. The question of whether or to what extent private stakeholders should involve in the certification process will be discussed. Also, the importance of enforcement mechanisms in relation to DPCs impact on accountability will be touched upon.

In Section 4, the important legal aspects that should be incorporated in every GDPR criteria and how to adapt them into criteria will be discussed. First of all, the general principles of personal data processing will be explained. Second, the legal grounds for processing and data subjects' rights will be touched upon. In Section 5, the risk-based measures in the GDPR that must be embedded in DPC criteria and how the certification bodies should legally assess the risks will be analyzed. It must be noted that developing criteria would not be sufficient to ensure accountability unless the assessment of such criteria is conducted properly. Therefore, how the certification bodies should evaluate those criteria in conformity with the GDPR provisions will simultaneously be elucidated.

This Chapter also sums up the useful points of the successful schemes that potentiate accountability. To understand whether the GDPR certification could promote accountability, the main qualifications required for an effective DPC will be discussed in this Chapter.

1. EFFECTIVE ACCOUNTABILITY UNPACKED

Previously, accountability has been mentioned with regard to its connection with the DPCs. An effective DPC scheme must be able to improve accountability in data protection. As stated, the concept has gradually become a goal in itself, although it used to be regarded as a tool to enhance the effectiveness of public governance.[168] It is today considered as an umbrella term that makes authorities or powerful institutions approachable and responsive to certain communities.[169] Accountability, as an umbrella term, requires several elements to be ensured to function as intended. If the term is scrutinized in terms of its preconditions, then the potential solutions to the problems in the market can be more accurately discussed.

Raab states that the controller is accountable both for the ethical quality of the processing, and for the story it tells you about its performance.[170] That is to say, the controller must be accountable for the transparency of the processing operations. With respect to the subject of this thesis, not only the processing by the controllers but also the certification criteria, conformity assessment and the accreditation procedures must be transparent. Since hoping for help from accountability without guaranteeing transparency resembles fishing in blurry water, the first building block of accountability, in data protection, must be "*trust in data controllers to treat personal information responsibly, and trust that the rules will be effectively enforced.*"[171] Therefore, it functions hand in hand with the principle of transparency, since transparency demonstrates who is really accountable and what are they accountable for. If the accountability of the responsible parties is ensured, community trust can be revived as well. Therefore, the first and the most important prerequisite for accountability can be considered as increased transparency which could eliminate most of the problems in the DPC market. The next section will address how to ensure transparency in DPCs, and which problems can be eliminated by improving the transparency.

---

[168] Bovens, "*Analysing and assessing accountability: a conceptual framework*", p.449.

[169] *Ibid.* p.449.

[170] Charles Raab, Information Privacy: Ethics and Accountability, 2016, at *SSRN: https://ssrn.com/abstract=3057469 or http://dx.doi.org/10.2139/ssrn.3057469*, p.344.

[171] Giovanni Butarelli, "The EU as a Clarion Call for a New Global Digital Standard", **International Data Privacy Law,** Vol.6, No.2, 2016, p.77.

As mentioned in the previous Chapter, one of the most noticeable problems in the market was the self-regulatory approach to DPCs. In order to provide accountability, the DPC must be embedded in the most appropriate environment in which they can show their best performance. Certification mechanisms that are developed under legislative frameworks, as seen in the examples of Schleswig-Holstein and CNIL certifications, contribute accountability, mainly because they are endorsed by legislators in binding legislative instruments.[172] However, the legislative frameworks regulating the DPCs should have the right approach for ensuring the accountability in data protection. The third section will discuss what regulatory qualities are needed in order for the DPCs to enhance accountability.

Enforcement and remedies in case of violations are equally important to ensure accountability in the data protection field.[173] Member States should protect the rights of the citizens, create respect for the law and remedy the damages stemming from the violations.[174] Hence, it is important not only to set guidelines but also to enforce such guidelines properly.[175] Also, the sanctions must be deterrent whereas some apparent advantages should be attributed to the certification recipients so that the certification mechanism would be incentivized.

Certification criteria are the third element that should be scrutinized because it is important against what the certification bodies will assess the ToE. For DPCs to function effectively, certification criteria must be developed in a way that is compatible with the principle of accountability. That is why the third prerequisite for the effective schemes promoting accountability should be considered as strong and comprehensive criteria. Although the criteria of the EU-based schemes seem generally adhere to the EU protection laws,[176] they needed to be organized under an umbrella framework such as the

[172] Carvais-Palut , p. 54-55.
[173] De Hert, *The Accountability Principle in Data Protection Regulation: Origin, Development and Future Directions* p.194.
[174] *Ibid*., p. 194.
[175] *Ibid.*, p. 216.
[176] Rodrigues, **Privacy and Data Protection Seals**, p.90.

one under the GDPR. In this regard, Article 42 can eliminate the fragmentation problem in the market.

It seems very difficult to ensure legal certainty since some schemes do not even provide a legal guarantee. However, an effective DPC should signify that the data protection risks have been minimized.[177] As a model, data protection accountability requires controllers and processors to carry out a set of activities, mostly risk-based ones, such as conducting a DPIA, appointing a DPO, and publicizing their data protection practices, or by means of TETs.[178]

Repeatedly, strong criteria would not be sufficient, if the certification mechanism itself is not regulated under a legislative framework. A legislative framework including certification schemes is both necessary for activating and ensuring the accountability of the stakeholders.

As we have unpacked accountability, which is the ultimate goal of the certification mechanism introduced under Article 42, we can better examine how to increase the efficiency of a DPC.

1.1. Increased Transparency

According to the European Union Agency for Network and Information Security (ENISA), "*openness and transparency are among the most important signs of quality of a certification mechanism*". CNIL, SH and EuroPriSe certifications all prioritize transparency as their core principle.[179]

The importance of transparency can be explained in three aspects. Without ensuring full transparency, the data protection legislations cannot serve to the right to

[177] *Ibid*., p.153.
[178] Yoel Raban, "Privacy Accountability Model and Policy for Security Organizations." **IBusiness,** Vol.4., No.2, 2012 p.168.
[179] Hansen, p. 44; Carvais-Palut, p.54.

protection of personal data. Secondly, it plays a certain role in increasing the principle of accountability. As these two principles overlap and promote each other, data protection certifications contribute to both principles. Thirdly and repeatedly, transparency improves customer trust. Since the customer trust is another envisaged function of the data protection certifications, transparency can be deemed as a precondition to realizing customer trust, specifically in online environment. Increased transparency in both personal data processing and the in the organization of the DCPs can eliminate the problems of the illusion of privacy, function creep and asymmetry of information.

The expected contribution of certifications to transparency can be realized only if the certification mechanism itself is transparent as well. In order for the scheme to be transparent, first of all, trustworthy and clear communication between the data controller and the data subjects must be ensured. Therefore, transparent processing is the core prerequisite for transparent DPC mechanisms. Second, transparent certification procedures must be ensured. An effective certification mechanism should primarily include transparent procedures, publicly accessible criteria along with summary reports on granted certifications.[180] Third, a transparent certification mechanism depends upon transparent requirements and methods for the conformity assessment. This means that all the technical and legal requirements necessary for the certification must be revealed in a transparent manner. Fourth, post-certification surveillance and on-spot audits in company with documentation in due form are the other mechanisms required for ensuring the transparency during the certification process. Last but not least, transparent complaints mechanism is deemed crucial for the data subjects to exercise their data protection rights.

As mentioned previously, the accuracy of the story that is told about the performance is of importance.[181] The story, here, should be in form of transparent reporting. For this reason, it is important that the schemes under Article 42 ensure transparent documentation of the entire process. German ULD and EuroPriSe, for instance, publish a short version of the final decision which clearly promotes the

[180] ENISA, p.28.

[181] Charles Raab, Information Privacy: Ethics and Accountability, p.344.

transparency of the procedure.[182] After the evaluation of the SH certification is completed, the chosen experts prepare a report on the technical and legal aspects of the IT product in question required for the certification. According to this report, if found certifiable, the certification body grants the SH data protection certification which has a validity period of two years, and it also publishes a short version of the decision.[183] Just like the SH certification, EuroPriSe also publishes a short version of the decision and carries out follow-on audits at 8 and 16 months.[184] This approach must be adopted by the GDPR certification as well to ensure the transparency of the mechanism.

The principle of transparency also requires the controller to inform the data subject in respect of the "*risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing*". [185] Regarding this particular requirement, risk-based approach to data protection will be touched upon in the subsequent sections.

Transparency between the controller and data subjects must be aimed at all the stages of the data processing. Personal data processing activities and transactions must be recorded by the controllers in order to provide the transparency. The main reason to that is to confirm that the processing of the personal data belonging to data subject has been done in accordance with the consent of the data subject or the other legitimate bases provided under the GDPR. [186] Only after ensuring the transparency of the processing, a certification mechanism would function as a demonstration of the ensured transparency in personal data protection. As a matter of fact, transparency must be provided even before the processing operations are commenced by the data controller in the context of receiving the consent allowing the processing. Data subjects should be able to reach every detail of the processing regarding their personal data in a transparent way in order to understand for what purposes their personal data will be processed. Hence, in the context

[182] Hansen, p.38-39.

[183] *Ibid.*, p.38-39.

[184] Rodrigues, et al., EU Privacy Seal Project," **Inventory and Analysis of Privacy Certification Schemes**, p.40.

[185] Recital 39 GDPR.

[186] Bonatti et al., "Transparent personal data processing: The road ahead", **International Conference on Computer Safety, Reliability, and Security**, (337-349), Cham: Springer, 2017, p.1.

of data protection certifications, first of all, the processing must be transparent, and the criteria should be developed in a transparent manner. Furthermore, accreditation and certification processes must be transparent as well.

Consequently, there are several elements that must be fulfilled in order to ensure the transparency in a certification scheme. They can be listed as:

(i) transparent processing;

(ii) transparent procedures:

- publicly accessible criteria and summary reports on each assessment;

-clear evaluation procedures supported by proper documentation;

-on-spot audits and regular post-certification surveillance and;

-transparent complaint mechanism.

The capacity of the GDPR certification on these matters will be discussed in Section 1 of Chapter 4.

1.2. Unpacking the Ideal Approach for DPCs

One can simply interpret that regulating data protection certifications under statutory codes will promote the trustworthiness of such certifications if such statutory codes are accompanied with right elements to enhance transparency. Schleswig-Holstein and CNIL examples show that where the certification mechanisms are regulated under legislative frameworks, the effectiveness of certification schemes increases. Also, in both certification schemes data protection authorities of the Member States operate as certification bodies. It can, therefore, easily be interpreted that certification mechanisms must be encouraged by the public authorities to be successful. The intervention of public authorities in processes as certification bodies or accreditation bodies are seen as an

indication of the trustworthiness of scheme by the public. Thus, it improves reliability and transparency of the schemes.

An inclusive legislative framework that encourages the controllers and processors to have their processing activities certified can be the solution for the proliferation issue in the area. However, building and endorsing such overarching certification scheme requires a complex set of evaluations demonstrating the best fitting qualifications necessary for an effective DCP. In this section, what qualities of regulation are considered the best in improving the accountability in a DPC scheme will be discussed.

1.2.1. Hard or Soft Law Approach?

Debates on soft law and its implications concerning accountability has long been on the agenda of the EU scholars. Unlike hard law, soft law approaches do not produce direct legal consequences, but they are intended to produce indirect legal effects and some practical effects,[187] such as accountability which is the most important practical effect of data protection certifications. The data protection certification mechanisms, although regulated under legislative frameworks, are usually voluntary. In accordance with the soft law approach, there is no binding force for the data controllers or processors to apply to those schemes.

However, among scholars, the soft law discourse did not receive uniform support.[188] According to some, the approach is regarded only as a tactic to enlarge the EU's legislative hard law powers and it circumvents usual systems of accountability. Thus, it weakens the effectiveness of a system, since it originates anticipations although it cannot generate any change.[189] On the other hand, hard law approach provides clear

[187] Senden proposes that the soft law should be defined as "Rules of conduct that are laid down in instruments which have not been attributed legally binding force as such, but nevertheless may have certain -indirect- legal effects, and that are aimed at and may produce practical effects" Senden, Linda. "Soft Law, Self-regulation and Co-regulation in European law: Where Do They Meet?" **Electronic Journal of Comparative Law**, vol. 9.1 (January 2005), p.23.

[188] David M. Trubek, and M. Patrick Cottrell, and Mark Nance, 'Soft Law,' 'Hard Law,' and European Integration: Toward a Theory of Hybridity, U of Wisconsin Legal Studies Research Paper No. 1002. **https://papers.ssrn.com/sol3/papers.cfm?abstract_id=855447**, (November 2005), p.2.

[189] *Ibid.,* p.2.

guidance, uniform treatment, sanctions and justiciability which are all of the significance with regard to accountability.[190] At this juncture, it seems appropriate to analyze this issue in relation to data protection certifications in order to answer the main research question of the thesis. The question of what sort of approach would be the most effective in regulating the DPCs should be addressed, by taking the contra and pro-soft law arguments into consideration.

Some authors think that a data protection certification, in any case, should be regulated under the soft law approach, thus, should have a voluntary character.[191] Voluntariness is the most fitting for the DPCs since certifications might not be required in many circumstances, for example, in the case of organizations processing personal data on a small scale. In addition to that, the costs required for the certification might be excessive for many small-scale companies. Hence, the approach is cost-effective for both the industry and for the Member States.

Another point is that soft law is found more effective in involving and encouraging the relevant parties. It encourages competition between the non-state actors, and therefore, can eliminate the problem regarding lack of competition. As a result, it potentiates DPCs ability to promote accountability given that the controllers and processors would be willing to demonstrate their compliance through the DPCs. Also, in my opinion, compulsory DPCs could not serve as proper accountability tools, since the willingness to demonstrate compliance -one of the necessary elements of accountability- would be neglected.

Moreover, soft laws should not be seen as stabilized legislations that will maintain their current status forever: they can signify the first stage on the way to legally binding hard laws. According to the constructivist approach, soft laws can be regarded as projects under construction rather than being a completed design. [192]

[190] *Ibid*, p.3.
[191] Kamara and de Hert, p.25
[192] Trubek et al., p.12.

Fast changing and technology-driven fields require legal instruments that can be easily modified as circumstances change.[193] This voluntary nature of certification schemes encourages and supports the compliance with the data protection legislation and provides the schemes for the necessary flexibility to cope with the technological developments.[194]

Raban thinks that the best policy in data protection would be the combination of both hard law and soft law to concretize principle of accountability.[195] this approach also appears to be the best fitting solution for the DPCs, particularly since voluntariness increases their efficiency. However, they should be regulated under legally binding legislative frameworks to promote accountability. For example, implementing sanctions to those who do not comply with the certification criteria would generate hard law-like results in a soft law framework. Also, certification agreements, which grant the right to use of certifications, and withdrawal of certification when requirements no longer met can be considered as further legal effects. Therefore, a legislative framework that embeds soft law instruments approach into hard law would be the most effective with respect to the GDPR certification because such approach has the capacity to increase accountability and eliminate the problems originating from the lack of competition in the market. I prefer naming this complex approach as voluntary binding approach; although it is voluntary to participate, the stakeholders are bound with the hard laws.

1.2.2. Co-regulatory Approach: Should Private Stakeholders be Included in The Certification Process?

As discussed, the self-regulated DPC market has been causing many problems that indicate that state intervention was needed. Contrary to what is expected, the full regulatory approach is not advised either in certification mechanisms. That is because, first of all, this approach requires higher costs for the regulating states. Second, building such a system entails a considerable amount of staff resources and capacity that is hard

[193] *Ibid.*, p.12.
[194] Rodrigues et al., The Future of Privacy Certification In Europe: An Exploration Of Options Under Article 42 Of The GDPR, p.9.
[195] Raban, *Privacy Accountability Model and Policy for Security Organizations*, p.170.

to achieve without the collaboration of the private sector. Also, in this approach, it is possible that the private actors tend to hide their real practices, and without the full support of the private sector, data protection can be endangered due to the lack of transparency. Lastly, the full-regulatory approach is found to be more intractable in handling the new technological developments than the self-regulatory approach. [196]

The co-regulatory approach requires that the "*regulations are specified, administered and enforced by a combination of the state and the regulated organizations*".[197] This can be provided by the regulatory frameworks involving both private and public bodies in the process, under the supervision of public authorities. The EU is familiar to the approach, as it has been tried in many sectors, such as food safety, consumer and environmental protection.[198] Since it has been seen that the self-regulatory approach to the data protection certifications fails in many ways because of its lack of reliability, [199] in order to ensure transparency in the process, the co-regulatory approach in certification is advised to be adopted.[200]

According to Bartle and Vass, there are five types of co-regulation:

Co-operative: Public authorities co-operate with the industry on matters concerning regulations. This co-operation can be either during the interviews of the new legislation, or during the implementation phase of the legislation;

Delegated: Public authority delegates some of its statutory tasks to the relevant private sector, while monitoring the compliance of the latter;

Devolved: Public authority devolves its statutory tasks to self-regulatory schemes;

Facilitating: Public authorities encourage, approve and monitor the schemes established by the private sector, without statutory backing;

---

[196] Rodrigues, Wright and Wadhwa, *Developing a Privacy Seal Scheme (that works)*, p.109-110.

[197] Ian Bartle and Peter Vass, Self-Regulation and the Regulatory State-A Survey of Policy and Practice" Research Report 17, Centre for Study of Regulated Industries, University of Bath, 2005, p.19.

[198] Marian Garcia Martinez, Paul Verbruggen, Andrew Fearne, "Risk-based approaches to food safety regulation: what role for co-regulation?" **Journal of Risk Research**, Vol.16, No.9., 2013, p.1101-1121.

[199] Lachaud, *Why the Certification Process Defined in the General Data Protection Regulation cannot be Successful*, p.6.

[200] Rodrigues, Wright and Wadhwa, *Developing a Privacy Seal Scheme (that works)*, p.110.

Tacit: This type is very similar to the self-regulation with a minor task for the public authorities. [201]

Co-regulation is not a formula, it can be designed in many different ways; different types of co-regulation can be determined either under these 5 types or separately as a mixture of some of these types.[202] However, it is crucial to find the best framework, regarding the individual features for each specific field.

There are several benefits of the approach. First of all, it is more practical for all stakeholders. It can be seen as task sharing, between public and private actors, in which the public authorities allocate some of their duties to the private actors that are able to demonstrate their expertise in the field. Secondly, if correctly constructed and implemented, this approach can reduce the financial burden on the governments and industries and offers inducements for private stakeholders to partake in the process.[203] Therefore the design of the co-regulation extremely matters. Third, the approach has the potential to increase transparency, provided that it is designed and implemented properly. Co-operation in accrediting and reviewing potentiates independency and reduces biased practices.[204] The relation between the co-regulatory arrangements and transparency stems from the fact that legislation, involving private actors into the process, envisage constant exchange information between the private and public actors. [205] Accordingly, if the structure has been solidly built, and if the transparency has been ensured, the accountability increases as well.

This would alone have many implications on eliminating the many issues in the market. First, the proliferation of the DPCs originated from the self-regulated market would be diminished. Second, public trust can be regenerated owing to the certification issuers co-operating with public authorities. Third, the problem regarding the

201 Bartle and Vass, p. 55-71.

202 Rodrigues, Wright and Wadhwa, *Developing a Privacy Seal Scheme (that works)*, p.113.

[203] Rodrigues, Wright and Wadhwa, p.111.

[204] Rodrigues, Wright and Wadhwa, p.114.

[205] Martinez, Verbruggen, Fearne, p.1100.

insufficiency of organizational resources would be eliminated, since only the private stakeholders that have sufficient capacity to participate in the process. Finally, the approach would promote fair competition and thus it would prevent the possible abuses of the market by the dominant actors.

Albeit its observed benefits, there are some issues to be considered in order for a co-regulatory approach to be effective. In co-regulatory frameworks, some flexibility must be provided to private participants, so that the private companies operate in their own familiar environment and have a certain extent of autonomy. Because organizational features and capacities differ among sectors, regulations should provide flexibility allowing the organizations to have the best suitable environment in accordance with their individual needs.[206] Flexibility in co-regulation potentiates creativity which is needed for developing effective technology-based solutions. It is also important that regulators observe what the best practices are in the field. However, if not delimited the flexibility may endanger the transparency of the process.[207] Besides, private participants must have sufficient capacity and expertise so that they accomplish the goals of the legislation. [208]

The certification should not be regarded as an accountability tool that can only be used by the private data controllers; it should also be regarded as a tool confirming the compliance of the public authorities with the GDPR. As accountability requires governments to give accounts to their citizens, certification schemes can be used in a way to demonstrate that the governments are compliant and liable too. At this point, it is important to question how far a DCP can ensure the accountability of the governments regarding their personal data processing activities. A co-regulatory approach can make the private DPCs bridge government and society. While increasing transparent communication between data subjects and governments, it also balances the power irregularities between the stakeholders. It simply gives the competence of auditing government practices to the private sector, and through the private sector to the public.

[206] Edward J. Balleisen and Marc Eisner "The Promise and Pitfalls of Co-regulation: How Governments can Draw on Private Governance for Public Purpose" in **New Perspectives on Regulation** (127-150), David Moss and John Cisternino (Ed.), 1st Edition, Cambridge: The Tobin Project, 2009, p.133.
[207] Balleisen and Eisner, p.134.
[208] *Ibid.* p.134.

Consequently, a properly implemented co-regulatory approach can eliminate many problems in the market, promotes accountability and increases the effectiveness of the DPCs.

1.2.3. Enforcement Mechanisms Supporting Accountability

Responsiveness of the responsible actors is an indispensable quality of accountability.[209] As stated in Chapter 2, data protection accountability requires the controller to provide explanations for its actions to the data subjects and authorities. Responsiveness of the controller can only be ensured in an environment where enforcement and sanction mechanisms run as it should be. In order to achieve effectiveness in a DPC, it is important to ensure that the certification bodies to be accountable so that they avoid biased practices. Moreover, governments also have to give accounts regarding their data protection practices. This Section will discuss the role of the DPCs in data protection enforcement and how to increase accountability in the field via DPCs.

In addition to the transparency and strong underlying criteria, it is crucial that the DPCs offer enforceable guarantees both to the data subjects and to their customers. The DPCs' ability to perform as credible indications of data protection adherence can be only as effective as their monitoring and enforcement.[210] In an ideal framework, the need for enforcement and sanctions against a certified controller could be minimized by means of other aspects of accountability such as transparency and proper evaluation based on strong criteria. Thus, the enforcement mechanism should be considered as a last resort to hold the controllers to account. After all, it should be the last resort, since in an ideal DPC framework -if other aspects of accountability are ensured- the need for enforcement would be lessened as much as possible.

[209] Daniel Guagnin, Leon Hempel and Carla Ilten, *Bridging the Gap: We Need to Get Together*, Guagnin Daniel and Hempel Leon (Ed), in **Managing Privacy through Accountability** (102-124)**,** London: Palgrave Macmillan, 2012, p.119.

[210] Rodrigues, **Privacy and Data Protection Seals**, p.151.

As stated in the last section of Chapter 2, DPCs generally do not have a complaint and enforcement mechanisms. The ones that provide such mechanisms have entirely internal processes, not allowing the impartial parties involvement. Consequently, data subjects cannot complain, or the mechanisms do not produce unbiased decisions. DPCs should not free recipients from their legal responsibilities towards data subjects. Complaint mechanisms make both controllers and certification bodies (stakeholders) aware of the problems concerning the certification procedure, if the complaints received are transparently reviewed and acted upon. The awareness concerning the existing problems would increase accountability because once identifying the causes, the stakeholders can question how to solve them. Therefore, it is suggested that the DPCs to an have effective complaint handling processes. This would indicate that the schemes protect the data subjects' rights, and therefore the credibility of the schemes may increase.

Another important issue regarding responsiveness is that the follow-on audits, subsequent to the grant, are commonly not conducted.[211] However, they are necessary for the consistent implementation of the certification criteria, and for timely enforcement. The scheme can only provide accountability provided that there are regular and random on-spot audits during the certification period. CNIL, SH and EuroPriSe all carry out follow-on audits which facilitates the authorities to take ex officio actions. These audits make the stakeholders to be on watch regarding their responsibilities. Also, in this way violations can be compensated before any harm is caused.

Another necessity for a scheme that promotes accountability is the revocation of the certification when the criteria are no longer met. Once receiving the CNIL Label, the recipient must be exceptionally compliant with the standards, including the appointment of a DPO and ensuring audit mechanisms for the obligations of the controller/ processor.[212] Otherwise, the label, which is normally valid for three years, may be revoked on the grounds that the compliance is no longer maintained by the recipient.[213] Revocation

[211] Rodrigues, et al., *EU Privacy Seal Project,* ***Inventory and Analysis of Privacy Certification Schemes***, p.45.
[212] Carvais-Palut, p.55.
[213] Rodrigues, et al., EU Privacy Seal Project," **Inventory and Analysis of Privacy Certification Schemes**, p.132-137.

of certification is a legal effect of breaching the certification agreement between the certification bodies and the recipient. One of the components of accountability should be regarded as accepting sanctions[214] and revocation refers that the recipient accepts the revocation in case of violating the contractual responsibility towards the certification bodies.

Although revocation of the certification is necessary, it can be seen as a soft measure and it does not sufficiently promote accountability if no other sanctions are laid down in the legislation. Accountability requires more than just legal settlements subsequent to violations; there must be a well-defined set of rules (*ex-ante* lawmaking) and implementation of these rules enshrined in legislations (*ex-ante* and *ex-post* enforcement).[215] In this regard, establishing high fines in case of violations is considered effective in increasing the commitments of the private stakeholders.[216]

Another important *ex-post* aspect of accountability is easily accessible remedies when violations have occurred.[217] Thus, for the DPCs to promote accountability in data protection, they must be able to provide information to data subjects on easily reachable remedies or remedial actions. DPCs should be the indication that the data controller respects the right to the protection of personal data and is ready to redress the damages in case of eventual harm.

It must be ensured that the certification bodies and the other authorities are held accountable in case they breach the laws. In this way, the trust of the data subjects can be increased to the DPCs. Accountability should not be seen only as a regulatory responsibility towards governments, but also as a tool that balances the power asymmetries between the weak and powerful parties.[218] As stated previously, the co-

[214] De Hert, *Accountability and System Responsibility: New Concepts in Data Protection Law and Human Rights Law*, p.195.
[215] *Ibid.*, p.195
[216] Balleisen and Eisner, p.131.
[217] De Hert, *Accountability and System Responsibility: New Concepts in Data Protection Law and Human Rights Law*, p.194.
[218] *Ibid.*, p.194.

regulatory approach to DPCs can be useful in ensuring the data protection compliance of the public authorities. In this context, DPCs can function as independent watchdogs to hold civil servants accountable to the public.[219] This means that DPCs can also certify the processing operations of public authorities and enforcement proceedings against public authorities in relation to their personal data processing activities can be launched *ex officio* by the DPCs, or upon a complaint from data subjects. In such an environment, the accountability of the government institutions can be achieved as data subjects would be brought into institutional decision-making.[220]

1.3. Certification Criteria

As stated in Section 6 of Chapter 2, there remain many problems due to diversified criteria co-existing in the fragmented DPC market. The most problematic issue is that the DPCs offer weak guarantees to their customers, thus to the data subjects. This has obviously been reducing the trustworthiness of the schemes and damaging accountability.

Studies have shown that the strength of the data protection certifications depend on the strength of their criteria, as the criteria are "*the backbone of the evaluation process*".[221] As Rodrigues points out "*a seal is only as good as the criteria and requirements it signifies are being met*".[222] Therefore, the content of the criteria is of significance as regards the extent of accountability it could provide. Concordantly, the other prerequisites for effective accountability that have been explained in Section 2 of the Chapter can be also affected by the quality of the criteria.

In this section, I briefly analyze the requirements that must be incorporated in every DPC criteria and make recommendations on how to refine the articles of the GDPR into certification criteria.

---

[219] *Ibid.*, p.195.
[220] *Ibid.*, p.195.
[221] Kamara and De Hert, p.22.
[222] Rodrigues, **Privacy and Data Protection Seals**, p.151.

1.3.1. How to develop approvable criteria that promote accountability?

As established previously, accountability complements current data protection policies with a view to render the entities more effectively responsible for their processing activities.[223] Demonstration of compliance forms an indispensable part of accountability. In order for data protection certifications to be able to demonstrate full compliance with data protection legislation, data subjects' rights, the general principles of processing, requirements for receiving consent and other legitimate bases must be ensured under the certification criteria.

EuroPriSe, which is an effective certification scheme promoting accountability, had derived its criteria from the European rules on privacy and data protection rules, especially from the Data Protection Directive and e-Privacy Directive (2002/58/EC), before the GDPR came into force. It guarantees that processing has been operated in conformity with the EU legislation; it promises data subjects' rights that the legal bases for processing have been in place, technical-organizational measures in line with the legislation have been completed. [224] EuroPriSe has published its criteria updated based on the GDPR requirements, to be submitted to the competent supervisory authority. However, there have been no criteria approved as of the date of the thesis.

The criteria of the SH certification, which have been derived from the EU legislation, include the legal bases and the general principles of processing, along with comprehensive data subject rights.[225] The evaluation is conducted on the basis of published criteria, which have been developed by the ULD, and founded on four aspects: (i) fundamental design aspects of the product (data minimization and transparency), (ii) lawfulness of data processing (consent or other legitimate bases), (iii) technical and

[223] De Hert, p.193.
[224] Cavokian and Chibba, p.70
[225]Hansen, p.40-44.

organizational measures preventing the risks of data breaches, and (iv) data subjects' rights. [226]

Criteria must be relevant to the current data protection legislation: the GDPR. The GDPR certification must guarantee that processing has been operated in conformity with the EU legislation, promise transparency, ensuring data subjects that the legal bases for processing are checked, technical-organizational measures in line with the legislation are completed, their data subjects' rights are being protected.[227]

One can simply assume that in order for the criteria to be strong, the source of the criteria which is the GDPR itself, shall be strong as well, not leaving room for relative interpretations.[228] On the other hand, the criteria should provide flexibility enabling the authorities to evaluate different ToE, since criteria may change depending on the ToE, the sensitivity of the personal data in question or the intended usage and purposes of the IT product subject to the evaluation. The type of the processing and the scope in which the processing operations are taking place may change the extent to which these aspects are reflected in the criteria.[229] Therefore, while developing criteria, a one-size-fits-all approach must be avoided, considering the specific characteristics of the different processes. In my opinion, generic catalog criteria that are not covering any specific ToE must be avoided. To ensure such flexibility there might be structured templates to be applied to a specific group of ToE.[230]

Above all, the criteria promoting accountability must include the right questions to test the relevant ToEs. For refining the legal, technical and organizational principles from the source to criteria, the methodology requires importance. .[231]

[226] *Ibid.,* p.40.
[227] Cavokian and Chibba, p.70
[228] Kamara and De Hert, p.22-23.
[229] EDPB, p.11.
[230] Hansen, p.4.
[231] Kamara and De Hert, p.22.

DPC criteria and conformity assessment that promote accountability must ask the right questions to evaluate the potential risks that might originate from the processing operations or are existing in the system of the controllers or processors. This can also be provided by a detailed checklist. However, in the sake of legal certainty, open-ended questions must be avoided the parameters must be as measurable as possible.

Unlike the other sections in this Chapter, the suggestion regarding criteria will not be checked against the GDPR criteria, since there have not been any certification criteria approved by the supervisory authorities. Hence, this section should be considered as recommendations on what to include in the GDPR criteria and how the certification bodies should properly assess the compliance of the ToEs with the GDPR.

1.3.2. Principles that must be enshrined in criteria

GDPR certification must certify that the processing of personal data is carried out in accordance with the general principles enshrined in the GDPR.[232] There are 7 principles that are stipulated under Article 5 of the GDPR. The principle of transparency under the GDPR will be examined in detail in the next Chapter with reference to its significance as regards certification process.

Purpose limitation: Undefined purposes for processing are not compliant with the data protection law.[233] Identification of the purpose must be the first step to be followed by the controllers in order to comply with the GDPR and to have their processing operations certified under the GDPR certification mechanism. The principle is regarded as the most important data protection principle, [234] a prerequisite for other data protection requirements; and it contributes to the principles to "*transparency, legal certainty and predictability*".[235]

[232] Art. 5 GDPR.

[233] Council of Europe, **Handbook on European Data Protection Law**, Luxembourg: Publications Office of the European Union, 2014, p.68.

[234] Dienst, p.54, para 262.

[235] *Ibid*., para 263

When a practitioner analyses a case concerning personal data protection, the first data quality requirement to be checked must be the purpose limitation. [236] Likewise, when the experts test a ToE against the certification criteria, they should first check whether the purpose of the processing is specified, explicit and legitimate. This requirement is a focal safeguard of the rights of the data subject since it prevents the controller to use the personal data "*beyond the purposes for which they were initially collected*".[237]

It is also a very important concept with reference to the accountability of the controller, therefore the criteria that properly incorporate the principle in its provisions would increase its overall efficiency. Because the principle is the cornerstone of the data protection, its interpretation requires a profound analysis. For the same reason, the principle must be carefully included in the GDPR certification criteria and analyzed in detail during conformity assessments prior to certification.

How to include it into criteria and how to evaluate the principle in a service or a system, however, might seem complex. Because of the open-ended wording of the Articles (both in the directive and the GDPR) the purpose limitation was interpreted differently in different Member States, the results were not homogenous as initially intended by the principle.[238] For this reason, the Art. 29 WP issued an Opinion on Purpose Limitation in order to prevent the divergences in the understanding of the concept in the different Member States. The Opinion should be taken into consideration by the scheme owners since the way that scheme owners interpret the principle may affect the quality and the criteria's probability to be approved.

The principle is composed of two constituents, as mentioned hereinabove. First, it requires that personal data are collected for specified, explicit and legitimate purposes. It should be noted that if there are more than one purposes existing simultaneously from

[236] Art. 29 WP, WP 203, 2013, Opinion 03/2013 on purpose limitation (9 September 2018), p.12.
[237] *Ibid*., p.4.
[238] *Ibid*., p.5.

the beginning, the purposes must separately be specified explicitly and legitimately.[239] There is no definition of "specified purpose'" provided in the GDPR. The Opinion 03/2013 on purpose limitation provides that in order for the purpose of the processing to be specified, the purpose should be "*sufficiently defined to enable the implementation of any necessary data protection safeguards, and to delimit the scope of the processing operation*".[240] The description of the purpose also must be "*detailed enough to allow that compliance with the law can be assessed*".[241] For instance, vague or general descriptions such as "improving users' experience", "marketing purposes", "IT- security purposes", "future research" should be avoided.[242] The degree of detail that is required for the compliance depends on the context. The assessment of how much data personal data involved in processing must be observed by the experts when deciding the appropriate degree of details to be provided to the data subjects. Addition to the quantity of personal data involved, the complexity of the case should also be regarded in accordance with the risk-based approach to the data protection.

The purpose must be specified by the controller before, and in any event not later than, the collection of the personal data. Therefore, organizations must clarify their purposes of collection of the personal data prior to the initial operation of processing. [243]

According to the Art. 29 WP, "*the purpose must be sufficiently unambiguous and clearly expressed*".[244] The purpose of processing should not be hidden and "*be in some intelligible form*". [245] Furthermore, when it is expressed by the controller, it should be easy to understand and leave no doubt regarding its meaning.[246] In this regard, the requirement of the purpose being explicit clearly relates to the principle of transparency.

[239] *Ibid*., p.12.
[240] *Ibid*., p.12.
[241] *Ibid*., p.15.
[242] *Ibid*., p.16.
[243] *Ibid*., p.15.
[244] *Ibid*., p.12.
[245] *Ibid*., p.17.
[246] Dienst, p. 56, para 273.

The purpose must comply with the data protection law, employment law, contract law, consumer protection law, "*including all forms of written and common law, primary and secondary legislation, municipal decrees, judicial precedents, constitutional principles, fundamental rights and other legal principles*".[247]

Data minimization and storage limitation: Under the GDPR, the personal data shall be "*adequate, relevant and limited to what is necessary in relation to the purposes for which they are collected and/or further processed*".[248] The principle has three components, as provided in Article 5(1) (c): adequacy, relevancy and necessity which all must be cautiously assessed during the conformity assessments. Those components should be assessed in the light of the specified purposes for which the data have been processed since the principle is closely connected to the principle of purpose limitation.[249] It is significant for the experts to determine how long the data should be stored with respect to the purposes for which it has been processed. The period of the storage should be limited to a strict minimum.[250]

In cases that the excess data is processed, it should be deleted immediately. Article 5(1)(e) states that "*personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed*". Thus, the experts must check whether the applicants implement automated or regular erasure of the personal data that are no longer necessary for the specified purposes.

Accuracy: Approved criteria must include questions that are capable of assessing whether the personal data shall be accurate and be kept up to date. [251] In other words, the processed data relating to a natural person should reflect the reality.[252] For this purpose, it must be clear that inaccurate data that have been processed must be erased or rectified

[247] Art. 29 WP, WP 203. p.20.
[248] Art. 5(1)(c) GDPR.
[249]Dienst, p.65, para 315.
[250] Rec. 39 GDPR.
[251] Art. 5(1)(d) GDPR.
[252] Voigt and Von Dem Bussche, p.91.

without delay, having regard to the purposes for which they are processed. The principle of accuracy requires systematic and periodic reviews of the processed data, specifically when there is a risk of damage to the rights and freedoms to the data subjects.[253] Moreover, appropriate mathematical or statistical procedures should be applied by the controller for the purpose of profiling, and the controller should implement appropriate technical and organizational measures to minimize the risks of errors in order not to cause inaccuracies in personal data.[254] Thus, it must be checked by the certification bodies whether the product or service that process personal data have the features to erase or rectify the inaccurate personal data.

Integrity and Confidentiality: During the conformity assessment it must be checked whether the controller provides the personal data to a third party with any justification stated in the legislation. Data confidentiality must be guaranteed by design and default from collection to deletion. To understand this, what methods and technical measures are used to keep the personal data secure, and whether they are efficient compared to the sensitivity of the personal data, in accordance with the risk-based approach explained in Section 6, must be checked.

It should be reminded that the general principles in Article 5 should be considered within the context of the legitimate bases of the processing. There are certain legal bases for processing, which are specified under the GDPR, must be checked by the experts during the evaluation process.

1.3.3. Criteria for evaluating legitimate basis for processing during conformity assessments

Processing of personal data is subject to general prohibition [255] unless it is justified by one of the legitimate bases provided under the GDPR.[256] The GDPR certification

[253] Dienst, p. 68-69.
[254] Recital 60 of the GDPR.
[255] Voigt and Von dem Bussche, p.92.
[256] Dienst, p.75, para 358.

should demonstrate that the processing has been lawful, in so far as it has been carried out on the basis of legal justifications determined in the GDPR.

1.3.4. Consent

When compared to Directive 95/46, the GDPR has introduced stricter rules regulating the consent for the controllers to comply with. Article 6(1)(a) stipulates one of the justifications of the personal data processing as the consent of the data subject. According to Article 6, "*processing shall be lawful only if… the data subject has given consent to the processing of his or her personal data for one or more specific purposes*". Therefore, all the GDPR criteria must have qualities enabling the evaluators to assess whether the consents of the data subjects are being received in accordance with the requirements under the GDPR or not.

What should be assessed regarding the consent of data subjects during the conformity assessment? Pursuant to Recital 32 GDPR, "*consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication*". Therefore, the criteria should evaluate if consent practices of the controller or processor comply with the following requirements:

-It must be freely given. The consent for the processing of its personal data must be the genuine and free choice of the data subject. The data subject should be able to refuse the request for consent. Any external pressure which can harm the free will of the data subject may make the consent invalid. According to the Art 29 WP, free consent exists *"if the data subject is able to exercise a real choice and there is no risk of deception, intimidation, coercion or significant negative consequences if he/she does not consent".* [257]

-The consent must be specific. The controller shall present the request for consent to the data subject concerned in a manner that is clearly distinguishable from the other matters regarding their relationship e.g. other provisions of the agreement between

[257] Art 29 WP, WP 259, 2018, Guidelines on Consent under Regulation 2016/679, p.7.

them. In order to realize this requirement, the word "consent" can be written in bold letters or be highlighted.[258]

-The data subject should be informed regarding the nature of the processing, the identity of the controller and the purposes of the processing.[259] While assessing the compliance of the consent against the criteria, the evaluator should ask whether the data processing on the basis of consent is limited to what is necessary.[260]

-The consent must be given by a clear affirmative act establishing an unambiguous indication of the data subject's agreement to the processing. Silence, pre-ticked boxes or inactivity do not constitute the consent of the data subject. The GDPR specifies three different situations in which the consent is deemed to be a clear affirmative act, and thus it is legally obtained.[261] The following can be considered as clear affirmative acts of the data subjects:

- ✓ ticking a box indicating a statement clearly meaning that the data subject gives consent for the processing when visiting an internet web site;
- ✓ choosing technical settings that enables sharing of the personal data (allowing for the use of cookies on an internet browser);[262]
- ✓ Any other statement or conduct that clearly indicates acceptance of the data subject.

Volker und others[263] is important on the matters of the consent being unambiguous, specific and freely given. In this case, the applicants, who were both operating farming business, applied for agricultural subsidies. Federal Agency for Agriculture and Nutrition published the applicants' personal data containing the

[258] Voigt and Von dem Bussche, p.94
[259] Rec. 42 GDPR.
[260] Dienst, p.90.
[261] Rec. 32 GDPR.
[262] Voigt and Von Dem Bussche, p.94.
[263] Judgment of the Court (Grand Chamber) of 9 November 2010, *Schecke*, Joined cases C-92/09 and C-93/09, EU:C:2010:662.

applicants' name, municipality of residence, and the amounts awarded to them on its website. The applicants objected the publication of the personal data. First of all, the consents of the applicants were not freely given, since data subjects were not sufficiently informed concerning the consent. Although, on the application form the phrases that "*the publication of information on the beneficiaries*" and "*the amounts received per beneficiary*" were mentioned, the application form did not contain a specific request for the consent. Moreover, the wording on the application form did not make it "*unambiguously clear that an applicant is consenting to publication*" of his name, municipality of residence and the amounts awarded to him. Thus, the consent allegedly given to the Agency was not ambiguously clear.[264] The applicants did not have an alternative choice but signing the form due to their economic needs. Therefore, there was an economic duress, rendering the consent non-voluntary, over the applicants. As a consequent, the consent was not also freely given.[265] The Court decided that processing of personal data was not carried out based on the consent of the applicants.[266]

That is why it is important for the certification bodies to review the usual practices on receiving consent from data subjects of controllers and processors. Moreover, they must assess whether the conditions for consent are met before processing operations start.

Demonstrating that the consent is obtained in an online environment can be achieved by using a double opt-in procedure. According to this procedure, the first step is to obtain the declaration of consent via online mask asking the data subject's email address. After the user enters its email address, the data subject receives a verification email that contains a personalized hyperlink. By clicking this link, the consent for processing would be obtained by the data controller.[267] Furthermore, in order to ensure whether the data subject wishes to share their personal data with the controller, the

[264] Opinion of Ms. Sharpston, Joined Cases C-92/09 And C-93/09 Opinion of Advocate General Sharpston delivered on 17 June 2010, EU:C:2010:353, para. 78.
[265] Opinion of Ms. Sharpston, para. 82.
[266] *Schecke Case*, para. 54.
[267] Voigt and Von dem Bussche, p. 93.

controller needs to create a ledger of all data transactions. [268] Keeping all the records of transactions would help certification bodies and supervisory authorities to assess the lawfulness of the consent received.

Pursuant to Article 7 Section 3, the data subject has the right to withdraw his/her consent at any time and as easily as giving it.

According to the last requirement in Article 7, according to the last requirement in Article 7, the controller shall not ask for consent from the data subject, in cases where the consent is related to the personal data which is not necessary for the performance of the contractual relationship.

The GDPR criteria can test the lawfulness of the consent by asking the following:

- Is consent given by a clear affirmative act?
- Is consent freely given, specific, informed and ambiguous?
- Is consent for processing, which is not necessary for the performance of a contract, conditioned for the performance of a contract?
- In case the processing is carried out for multiple purposes, is consent obtained for all those purposes separately and specifically?
- Can data subjects withdraw their consent any time?

1.3.5. Other Legitimate Basis for Processing

[268] Bonatti Piero *et al.*, "Transparent Personal Data Processing: The Road Ahead.", **International Conference on Computer Safety, Reliability, and Security,** Cham**:** Springer, 12 September 2017, (337-349), **https://www.specialprivacy.eu/images/documents/TELERISE17.pdf, 10 June 2018.**

In cases where there is no possibility of processing based on the data subject's consent, the data processing shall be based on other legitimate basis provided in the GDPR. Dienst analyses such legal basis under two categories:[269]

-legitimization *ipso iure (contract, compliance with a legal obligation, vital interests of the data subject, public interest);*

-legitimization subject to a balancing of interests (Art 6(1)(f)).[270]

In practice, the following cases as legal grounds should be applied in addition to the consent requirement.

1.3.5.1 Contractual necessity

There are two scenarios provided for the contractual necessity to be deemed as a legitimate basis in the sub-paragraph b:

-performance of a contract to which the data subject is a party;[271]

-in order to take steps at the request of the data subject before entering into a contract.

In the first scenario, the processing activity must be genuinely necessary for the contract, meaning that contractual requirements cannot be fulfilled without the processing activity takes place. For instance, processing the buyers' address to deliver the purchased goods to his address or credit card information so that the payment can be transferred to the seller's bank account can be seen necessary in order to perform the contractual requirements.[272] However, if the buyer will pay cash-on-delivery, the controller will not

[269] Dienst, p.76.

[270] According to Article 6(1)(f) processing shall be lawful if "*processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child"*.

303

[272] Art. 29 WP, WP 217, p.16.

need the credit card information.[273] Another example to contractual necessity could be processing bank account details of an employee for the purpose of paying his salary.[274] Even though the necessity should be assessed depending on the concrete case, there are certain cases in employment relationships clearly go beyond what is necessary for the employment contract. Monitoring employee's online activities or telephone use and video surveillance of the employees are deemed beyond necessary.[275] It is important to note that some processing activities which go beyond contractual necessity can still be legitimized and certified under other legal grounds provided in Article 6(1). Hence, the experts must test whether the processing activity carried-out in the scope of a contract that is genuinely necessary to fulfill the contractual requirements.

The paragraph, secondly, covers pre-contractual relationships upon the request of the data subject. To exemplify, processing of the address details will be covered under this legal ground, if product or service information is requested by the data subjects.[276] If there is a pre-contractual processing that is necessary for the future services of the controller, such processing must be justified backed by reasonable arguments to both supervisory authorities and certification bodies.

1.3.5.2 Legal Obligation

If processing of personal data is "*necessary for compliance with a legal obligation to which the controller is subject*", then the processing activity can be legitimized under the subparagraph c. For this to happen, first of all, the obligation must be derived from the law of the EU or a Member State.[277] Secondly, there must be no alternative for the controller instead of that obligation. Third of all, the legal obligation in question must be sufficiently clear about the processing concerned.[278] Anti-money-

[273] Voigt and Von Dem Bussche, p. 102.
[274] Art. 29 WP, WP 217, P.16.
[275] *Ibid.*, p.17.
[276] *Ibid.*, p.18.
[277] *Ibid.*, p.19.
[278] *Ibid.*, p.20.

laundering laws obliging companies or tax authorities to inform the authorities regarding suspicious transactions can be an example to the legal obligation.[279]

Criteria can include the following questions about this particular legal basis:

- Is there a legal obligation for processing derived from the EU law or a Member State law?
- Is there any alternative to this legal obligation? If so, what are the justifications for not choosing that alternative?
- Is the legal obligation in question sufficiently clear?

1.3.5.3 Public interest or exercise of official authority vested in the controller

This legal ground may be used by both private sector and public institutions, depending on the Member State law. The Member States, however, are not required to adopt specific laws for each processing activities in isolation, such laws might include several processing activities.[280] In such cases, official authority or a public interest task may be vested in the controller. For instance, a bar association may process personal data of its members to carry out disciplinary measures against them.[281] In terms of the private sector, it is often seen that, particularly in the transport and health sector, official authorities outsource tasks of processing personal data.[282] This legal ground differs from the legal obligation since there is no legal requirement for the controller to act in the sake of public interest.[283]

1.3.5.4 Legitimate interests pursued by the controller or by a third party

[279] Dienst, p. 79.
[280] Rec. 45 GDPR.
[281] Art. 29 WP, WP 217, p.21.
[282] *Ibid.*, p.22.
[283] Dienst, p. 81, para 388.

Article 6(1)(f) provides that processing of personal data may be legitimized in cases where the legitimate interests pursued by the controller or by a third party, unless these interests are overridden by the interests or fundamental rights and freedoms of the data subject. The burden of proof will be vested on the controller for its legitimate interest. [284] Pursuant to this, a balancing test, which will be analyzed in detail, is required to find out whether or not the fundamental rights or freedoms of the data subject override so-called legitimate interests of the controller. As explained in Section 4, this legal ground can be very complex to evaluate.

1.3.6. Data Subjects' Rights That Must Be Enshrined in Criteria

The rights that are granted to the data subjects under the GDPR can be examined under three elements depending on their purposes:

Transparency	Accuracy	Limitation
Information duties (Art 13-14)	Right to rectification (Art 16)	Right to object (Art 21)
Right of access (Art 15)	Right to erasure- right to be forgotten (Art 17)	Right not to be subject to a decision based on automated processing, including profiling (Art 22)
	Right to restriction of processing (Art 18)	
	Right to data portability (Art 20)	

Table 1: The rights that are granted to the data subjects under the GDPR
Source: Schrey, p.127, para. 602

[284] Voigt and Von Dem Bussche**,** p. 103.

Generally, the criteria must include the following questions:

- Are all the processing activities and transactions recorded and ready to be immediately submitted to supervisory authorities upon request?
- Is the controller or processor efficiently inform the data subjects regarding their rights that can be invoked under the GDPR?

Moreover, the information duties of the controller in Article 13-14 also oblige controllers to provide transparency regarding the processing operations. As a result, the GDPR criteria must be comprehensive as to include all the above-mentioned rights in order to verify full transparency and therefore accountability. To ask the following questions is necessary for a complete evaluation of these rights and requirements:

- What is/are the purpose(s) of the processing operation(s)?
- What methods are used to inform the data subjects? Are they efficient, transparent and reachable?

As recommended by the Art 29 WP, the controllers should use the "layered notice" method. By using this method, the controllers may provide laconic key information to the data subjects regarding the purpose of the processing, while also providing additional information which includes a more detailed description of their purpose of processing.[285] In this method, the essential information concerning the purpose of processing should be provided with "*on-the-spot*" notices. For example, companies using video surveillance (closed-circuit television systems) in public places can use the layered notice method combining the immediate "*on-the-spot*" notices with detailed policy published on their websites.[286]

On the websites which allow the users to share their personal data publicly or with their friends, there must be enough and understandable information, such as short

[285] Art 29 WP, WP 203, p.16.

[286] *Ibid*. p. 52, Annex 3, example 9.

notices supported with icons concisely explaining the purposes of the processing, allowing the users to choose with whom they will share their personal data. Besides, the controller should provide links directing the users to more detailed information on the next layer, about the purpose of the processing. It is also important that the language of the notice is adapted to the target audience.[287]

Furthermore, a purpose can be segmented into a number of "*sub-purposes*". For example, a job application of an individual can be processed by a company for checking the eligibility or educational records of him or her, storing the data for the potential future vacations. In such cases, using the concept of an overall purpose can be useful. An overall purpose can be provided on the first layer, just like in the method of "*layered notices and further information can be provided on the next layer*".[288]

- Does privacy notice sufficiently include all the necessary elements under Articles 13-14-15?
- In what ways the data subjects may request information regarding the processing? (web form, e-mail, phone)
- How long does it take, under normal circumstances, for the controller to inform the data subjects?

The duties of the controllers towards data subjects constitute a significant part of their compliance with the GDPR and should be incorporated into the criteria of the GDPR certification. Particularly, information duties of the controller have been enhanced, in comparison with Directive 95/46. It is crucial how fast the controller can react to the potential demands of the data subjects.

Paragraph 3 of Article 12 states that:

[287] *Ibid*., p.52-53, Annex 3, example 10.
[288] *Ibid*., p.53, Annex 3, example 11.

"*the controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request*".

This period might be extended by two further months if necessary. The information to be provided to the data subjects must be free of charge,[289] concise, transparent, intelligible, easily accessible, written in a clear and plain language, [290] and in the mother tongue of the data subject.[291] Although as a general rule, information shall be provided in writing, oral information also can be provided if the data subject whose identity has been proven by other means, requests so.[292]

The following questions must be posed during the evaluation of the ToE:

- How do the applicants evaluate the requests received from the data subjects?
- What specific measures are taken in order to comply with the general deadline requirement?

The right to be forgotten was derived from the Directive 95/46 in 2014, in *Google Spain* Case, and it has been recognized under Article 17 of the GDPR together with the right to erasure. The court, by stating that the data subject has right to request the removal of its personal data which is inaccurate, inadequate, irrelevant or excessive, confirms a more comprehensive reading of the right to be forgotten.[293] According to the respective decision of the Court:

"*the operator of a search engine is obliged to remove from the list of results displayed following a search made on the basis of a person's name links to web pages, published by third parties and containing information relating to that person*".[294]

[289] Art 12 (5) GDPR.
[290] Art. 12(1) GDPR.
[291] Schrey, p.128, para 606.
[292] Art. 12(1) GDPR.
[293] *Google Spain*, para. 92.
[294] *Ibid.*, para. 88.

Article 17 regulates both the right to erasure and right to be forgotten. The relationship between those two rights stems from their related legal consequences since the right to be forgotten is a legal consequence of the right to erasure.[295] Article 17 can only be invoked by the data subjects, provided that the personal data are no longer necessary in relation to the process, the data subject withdraws consent or objects to the processing activity, the personal data have been unlawfully processed, the personal data have to be erased for compliance with a legal obligation in Union or Member State law or the data subjects are under 16 years old.[296] In all those cases, the processing has been carried out unlawfully from the beginning or the legal grounds for processing no longer exist. Article 17(2) introduces a complex obligation for the controllers:

"*Where the controller has made the personal data public and is obliges pursuant to paragraph 1 to erase the personal data, the controller, taking into account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of those personal data."*

Consequently, it must be assessed whether the data subjects can request from data controllers a complete deletion of their personal data which have been disclosed to third parties or made public by the controller.[297] The GDPR certification would play an important role in ensuring that the controller would take reasonable technical measures and any other steps conditioned in the provision.

Another explicitly enhanced right is the right to object set out in Art. 21 GDPR. Under certain conditions, the subjects have the right to object at any time to processing. For example, an absolute right has been enshrined under Article 21(2) for data subject to object the processing carried out for direct marketing purposes, which is recognized as a

[295] Voigt and Von dem Bussche, p.161.
[296] Art. 17 (1)(a)-(f).
[297] Schrey, p.141, para 653.

legitimate interest of the controller for processing activities.[298] Since generally, and also with regard to this specific right, the burden of proof rests on the controller, the controllers should pay particular attention to the legal grounds necessary for the exercise of the rights together with the exemptions under the Regulation. Although the GDPR has been well-heard across the EU and beyond, most websites still require personal data of the visitors for direct marketing purposes without providing any option to object such processing. Such processing operations without enabling data subjects to object shall not be certified under Article 42.

Another right that has been derived from the German Data Protection Law is "*the right not to be subject to a decision based solely on automated processing, including profiling*", which produces legal effects concerning him or her or similarly affects him or her. [299] As seen often in practice, personal aspects of natural persons can be evaluated based on automated processing, and those decisions may have legal effects concerning those natural persons. The GDPR prohibits automated decision-making that may produce legal or significant effects concerning the data subjects merely as a result of automated decision-making processes.

By the way of automated decision-making, costumers of companies can be tracked and targeted with advertisements that offer different prices only to certain customers. Such targeted advertisement must also be prohibited under Article 22, since in such cases a significant effect may occur on the data subjects.[300] Automatic refusal of an online credit application or e-recruiting practices without any human intervention is exemplified in Recital 71. The prohibition also includes profiling such as predicting aspects relating to "*the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behavior, location or movements ".*[301]

[298] *Ibid.* p.147, para 684.
[299] Art. 22(1) GDPR.
[300] Schrey, p. 150, para 694.
[301] Rec. 71 GDPR.

The following questions can be useful when assessing the compliance of the applicants with the criteria:

- Is there any automated decision which may affect the rights of the data subjects?
- Is the algorithm being used fair? How does the controller prevent any possibility of unfair or biased automated decisions?

1.4. Risk-based approach embedded in DPC criteria

The GDPR adopts a risk-based approach to data protection, which means that entities processing personal data must clarify the level of risk of their data processing activities with respect to the potential damage risk to the rights and freedoms of individuals, prior to the processing operations.[302] Depending of the level of risk, the measures that must be taken by the entities may vary. Therefore, the approach is founded on the principle that detecting potential risks before they occur helps controller and processors to calibrate their practices in proportion to those potential risks.

Similarly, the "criteria" against which the ToE will be tested, must be developed considering the level of risk of the processing activities. For example, in the case of "high-risk" processing activities, the entities shall conduct a data protection impact assessment (DPIA), and they are required to consult with a supervisory authority prior to processing. Correspondingly, those requirements must also be covered in the criteria.

The risk-based approach is important for the scheme owners since the criteria must be equipped with the sufficient elements, efficiently able to test the ToE, with regard to the potential risks that may emerge as a result of the processing operations. For instance, the French CNIL recommends controllers to first clarify the potential damage

[302] Gabriel Maldoff, "The Risk-Based Approach in the GDPR: Interpretation and Implications", **https://iapp.org/resources/article/the-risk-based-approach-in-the-gdpr-interpretation-and-implications/**, 10 July 2018, p.6.

related to a specific processing activity. Second, controllers are recommended to assess the gravity damage that may emerge. To do that, for example, controllers should ask themselves what if they neglect the consent requirement, what would be the worst scenario with respect to data protection. Eventually, they should evaluate the possibility of the damage that could result due to the vulnerabilities of their systems and operations.[303] The risk-based approach will be analyzed in terms of the principle of proportionality, in the light of the case law and the guidelines and opinions of the Article 29 WP. However, calculating the entire risks, especially of the processing operations on large scales can be extremely difficult.

In this section, the concept of the legitimate interest of the controller will be elaborated in order to demonstrate how to accurately calculate the risks that may emerge from the processing of personal data. The principle of proportionality, which is the foundation of the risk assessment, requiring that the processing operations to be proportionate to the legitimate interests of the controller will be analyzed in the light of case law. The fundamental risk-based measures in the GDPR will be summarized to exhibit when and under what circumstances they are necessary to conduct, and thus to be included in the certification criteria.

1.4.1. The Foundations of Risk Assessment

As stated in Section 2 of Chapter 1, the right to the protection of personal data is not an absolute right; it should be balanced against other fundamental rights. In some cases, it is possible that legitimate interests of the controller might conflict with the right to protection of personal data. Such interests can belong to third persons and also stem from other fundamental rights as well. If such conflict is inevitable, in order to mitigate potential risks and not to harm to the fundamental rights and freedoms of individuals, the principle of proportionality must be applied to the relevant cases by the experts. In terms of risk-based approach, the principle of proportionality can be considered as the most relevant principle, since the Court has used this principle to balance the conflicting nature

[303]Maldoff, p.6.

of right to privacy with other freedoms, legitimate interests and with statutory obligations that may have potential to limit the right to privacy and the protection of personal data.

The principle requires that:

-the measures taken shall not "exceed the limits of what is appropriate and necessary in order to attain the objectives legitimately pursued by the legislation in question";

- if "there is a choice between several appropriate measures" "the least onerous" one shall be chosen;

- the harm caused "must not be disproportionate to the aims pursued" by the legislation.[304]

In the context of data protection, the principle of proportionality was first mentioned in 2003 in *Östrerreichischer Rundfuk* case where the Court found that the interest of the Austrian State must be balanced with the right to privacy of the persons in question.[305]

Östrerreichischer Rundfuk was a public broadcasting organization obligated by the State to inform the Court of Audit regarding the salaries and pensions which are in excess of a certain limit paid by it to their current and retired employees, including the names of the recipients. The purpose of State was to demonstrate the payments in an annual report in order to ensure the best use of the public funds. The Court asked the national court to find out whether the public disclosure of the information related to natural persons' salaries and pensions by Östrerreichischer Rundfuk is proportionate to the legitimate aim pursued,[306] considering the natural persons in question would suffer from the negative effects stemming from this disclosure.[307]

---

[304] Judgment of the Court (Fifth Chamber) of 5 October 1994 *Crispoltoni and Others/ Fattoria Autonoma Tabacchi and others*, Joined Cases C-133, C-300 and C-362/93 ECLI:EU:C:1994:364, para.41

[305] Judgment of the Court of 20 May 2003, *Östrreichischer Rundfunk* Joined Cases C-465/00, C-138/01, EU:C:2003:294, para. 84.

[306] *Ibid.*, para.86.

[307] *Ibid*., para.89.

The principle plays an important role particularly in balancing the right to the protection of personal data and freedom of expression, since those two may seem to conflict in many cases.[308] In order to determine how to balance these two fundamental rights, the Court suggested applying a necessity test which had been previously left to the discretion of the national courts. The approach was obviously not compatible with the objectives of the harmonization of the data protection rules throughout the EU.[309] Article 9, titled as processing of personal data and freedom of expression, of the Directive provides the exemptions or derogations that can be applied by the Member States for the certain chapters of the Directive, on the condition that the processing is carried out merely for the journalistic purposes or for artistic or literary expression and that "*only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression*". In *Satamedia* case, the Court, interpreting Article 9, held that the exemptions of the right to privacy should only apply if they are strictly necessary.[310] The same approach is maintained under the GDPR, as Recital 153 states that the Member States may have legislations constituting exemptions and derogations only if they are necessary for the purpose of balancing the right to protection of personal data and the freedom of expression.

In the light of the case law, the Member States developed their own criteria for the assessment of the legitimate interests of the controller or a third party.[311] In the *Google*

[308] *Östrreichischer Rundfunk;* Judgment of the Court of 6 November 2003**,** *Bodil Lindqvist*, Case C-101/01, EU:C:2003:596

[309] Tranberg, p.242.

[310] Judgment of the Court (Grand Chamber) of 16 December 2008, *Satakunnan Markkinapörssi and Satamedia* Case C-73/07, EU:C:2008:727, para 56.

[311] European Commission, Commission Staff Working Paper, Impact Assessment, Brussels, 25.1.2012 SEC (2012) 72 Final, Annex 2, p.27; "The implementation of the "balance of interest" criterion (Article 7(f)) differs substantially between Member States. In the UK it is largely left to controllers to conduct the assessment and to determine whether they can process personal data on this basis. In the Netherlands, the explanatory memorandum to the data protection law sets out guidance on what issues should be taken into account when applying this criterion. Given its vagueness, several Member States (including Belgium, Ireland and UK) have envisaged issuing further rules for the application of this criterion but have not yet adopted such rules. DPAs have provided guidance in their opinions interpreting the law. In some countries, it is explicitly indicated that the balance test applies only to the private sector (e.g. Germany) or in cases specified by the Data Protection Authority (Italy) or on the basis of the permission of the national data protection supervisory authority in a specific case (Finland). Other countries (including Greece and Spain) impose stricter requirements on processing on the basis of this criterion.

Spain case, with regard to the principle of proportionality, the Court held that "*a fair balance*" between parties' interest should be sought. The legitimate interests of internet users, who have the right to enjoy the access to the information listed in the search results, were found overridden by data subject's fundamental rights. This balance, however, may depend on the nature of the information listed by the search engine.[312]

Finally, in 2014 the Article 29 WP provided guidelines for the test in its opinion on the notion of legitimate interests. Pursuant to the interpretation of the Article 29 WP, before applying the balancing test, both legitimate interests of the controller and its impact on the interests and rights of the data subject should be pictured on a spectrum.[313]

Legitimate interests can range between:

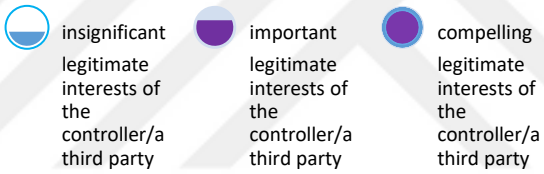

Figure 6: The Level of Legitimate Interests

The impact of the legitimate interests on the interests & fundamental rights of the data subject can range between:

[312] *Google Spain* Case, para 81.

[313] Art 29 WP, WP 217, 2014, **Opinion 06/2014 on the "Notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC"**(last access 22 August 2018), p.30.

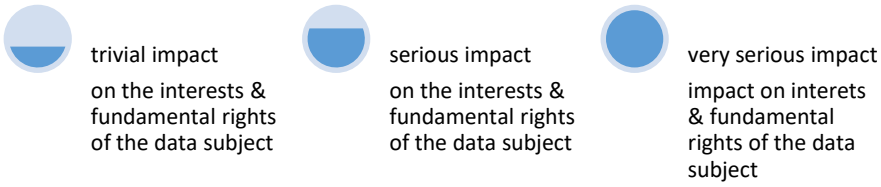

Figure 7: The Level of Impacts on the Interests & Fundamental Rights of the Data Subject

During the evaluations, the experts should assess the specific processing situation on the case-by-case basis. [314] Once the weight of both sides is determined, it must be assessed whether the legitimate interests of the controller or a third person override the interests and rights of the data subject. It is significant to determine whether the nature and the scope of the legitimate interests of the controller are necessary and proportionate.[315]According to this preliminary assessment, a "provisional balance" can be established.[316] However, in many cases, the result of the provisional balance test will still likely be unclear.[317] When the first result of the balancing test comes out as unclear, the legal experts should check whether there are additional safeguards applied in order to ensure that the rights of the data subjects are protected.

[314] Voigt and Von Dem Bussche, p.105.

[315] Art 29 WP, WP 217, p.34.

[316] Art 29 WP, WP 217, p.34.

[317] Sebastian Dienst, "Lawful Processing of Personal Data in Companies", Daniel Rucker and Tobias Kugler (Ed.), in **New European General Data Protection Regulation A Practitioner's Guide Ensuring Compliant Corporate Practice** (49-105), Munich: C.H. Beck, Nomos, Hart Publishing, 2018, p.86, para 411.

Figure 8: Balance Test

Additional safeguards play an important role in changing the balance in favor of the controller.[318] However, Article 29 Working Party does not mention any safeguards beyond the compulsory rules already provided under the GDPR such as transparency, technical and organizational measures to ensure that the data cannot be used to make decisions or other actions with respect to individuals, the use of anonymization techniques, privacy by design, DPIA and data portability. Providing a general and unconditional right that enables data subjects to opt-out has been suggested by the WP. This suggested right goes beyond the right to object in Article 21, since data subjects, in order to exercise the right, should provide their grounds for their particular situation to object. This ambiguity should be resolved by the Court or by the EDPB in the sake of legal certainty. Since approved certification criteria can play an important role in guiding other controllers that are subject to the same criteria, the additional safeguards can be

[318] Art 29 WP, WP 217, p.42.

clarified in approved criteria as well. Otherwise, the GDPR criteria cannot properly assess the potential risks and therefore cannot ensure accountability in data protection.

1.4.2. Explicit risk-based measures

Although the principle of proportionality and the balance test seem helpful to identify the risks, nevertheless in practice risk assessments require more tangible measures that can facilitate the demonstration of compliance. Particularly, this is very important for the certification bodies when assessing the compliance of the applicants against the GDPR criteria. The GDPR consists of several explicit risk-based measures to facilitate the risk assessment for all stakeholders. The purpose of that is to improve accountability by obliging the responsible persons to demonstrate their risks. The measures written hereinbelow must be reflected in every DPC criteria in detail in order for the certification to verify genuine data protection.

1.4.3. Data Security

The first step of the risk-based actions is to take measures to keep the personal data subject to processing secure. Under Article 32, controllers and processors are required to execute appropriate technical and organizational measures, such as pseudonymization, encryption of personal data or adherence to an approved certification mechanism referred under Article 42, to ensure a level of security appropriate to the risk.

The GDPR does not apply to data that are not identifiable.[319] Therefore, anonymized personal data do not fall within the scope of the GDPR. Anonymization basically means modification of personal data that can be achieved by randomization or generalization techniques.[320] The technique is beneficial for companies since it prevents

[319] Rec 26 GDPR. Randomization alters the accuracy of personal data by removing the connection between the personal data and the individual whose personal data has been subject to the processing activity. This method prevents the data to identify a specific person. Generalization blurs the details of the personal data by enhancing the respective scale. For example, personal data containing the information regarding an individual's address can be generalized to his/her city or country depending on the context.

[320] Voigt and von dem Bussche, p.13.

the applicability of the GDPR, it saves time, money and staff sources.[321] For example, in scientific research, the controller should modify the personal data of the participants by using their countries, age, and sex instead of their name.

As another appropriate measure for data protection is pseudonymization. Pseudonymized personal data can only be identified with the use of additional information which should be kept separately. In this technique, specific personal data can be replaced by a certain indicator such as numbers, or nicknames. After pseudonymizing the data remains easily re-identifiable; the processing remains within the scope of the GDPR.

The GDPR criteria, therefore, must include questions such as:

- Does the controller implement appropriate technical and organizational measures addressing the potential vulnerabilities in the system?
- What measures are implemented and how?
- Are the measures sufficient when considering the specific features of the personal data to be processed?

1.4.4. Data Breach Notifications

The GDPR criteria must enable the evaluators to check whether there are measures fulfilled in order to implement data breach notification obligation of controllers.[322] "Personal data breach" is defined as a "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed*". This particular obligation imposes the data controller to be aware of the actualized breaches and to immediately take the necessary measures to prevent further damage. Furthermore, this obligation means that

[321] *Ibid*., p.14.

[322] Article 34 GDPR states that *"when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay."* Moreover, Article 33 stipulates that in case of any kind of data breach, the controller or processor shall without undue delay, if possible, not later than 72 hours after noticing such data breach, to the competent supervisory authority.

the controller or processor must be transparent as well when it comes to its own non-compliance. In order to fulfill the obligation, the controllers are advised to have prepared notification forms to be filled in case of a data breach.[323] Following questions can be asked in this regard:

- How does the applicant comply with the requirement under Articles 33-34 of the GDPR? How does it calculate the potential high risks to the rights and freedoms of natural persons?
- What are the ways used by the applicant in order to detect personal data breaches?
- How does the applicant notify the data subjects under Article 34? What are the communication methods chosen by the applicant?
- How does the applicant notify the competent supervisory authority regarding the personal data breach?
- What are the measures taken in order to comply with the deadline of the requirement? How does the applicant make sure to notify the data subjects and supervisory authority without undue delay?

1.4.5. Data Protection Impact Assessment linked certification

DPIA is a new obligation, although it is not a new concept. The GDPR combines certification schemes with DPIAs. DPIAs facilitates entities to clarify, tackle and control data protection matters and risks effectively. Data controllers, before applying to certification schemes, must self-assess their compliance and document their possible impact on the freedoms and rights of the data subjects. Since the method reveals the risks

[323] Joachim Schrey, "Data Privacy in Private Companies", Daniel Rucker and Tobias Kugler (Ed.), in **New European General Data Protection Regulation A Practitioner's Guide Ensuring Compliant Corporate Practice** (105-193), Munich: C.H. Beck, Nomos, Hart Publishing, 2018, p.154, para 709.

that might emerge from the processing operations, it raises public awareness. Besides, the DPIAs allow the controllers to satisfy the data protection rules and principles such as accountability.[324] In order to enhance accountability, public authorities should review the compliance and whether the DPIA reflects the truth.

To carry out a DPIA is not generally compulsory. A DPIA shall be required in cases where:

-a systematic and extensive evaluation of personal aspects relating to natural persons which are based on automated processing, including profiling;

-in case of decisions that produce legal effects concerning the natural person or that similarly significantly affect the natural person;

-processing on a large scale of special categories of data, or of personal data relating to criminal convictions and offenses;

-systematic monitoring of a publicly accessible area on a large scale.[325]

After the self-assessment and fulfilling all the requirements in the GDPR, corresponding the level of risk of their processing activities, the entities may apply for the GDPR certification to the competent supervisory authority or to the accredited certification bodies.[326]

The following must be included in the GDPR criteria and evaluated by the experts:

- Is the data flow mapping comprehensive and accurate? Does it reflect the real practices of the controller?

[324] Rodrigues, Wright and Wadhwa, *Developing a Privacy Seal Scheme (that works)*, p.113-114.
[325] Article 35(3)GDPR.
[326] Article 42(5) GDPR.

- Have all the risks that may emerge from the processing been identified appropriately in a framework demonstrating appropriate reasoning for each possibility?
- Have all the potential impacts on the individuals been identified and documented?
- What are the measures envisaged by the applicant to mitigate those risks and impacts? Are they sufficient?

In the light of the criteria, certification bodies should check the DPIA documents and compare them with the real practices of the controller during on-spot audits. DPIA documentation provides certification bodies and supervisory authorities with a comparable base to build their subsequent audits on while helping controllers in accomplishing their accountability requirement.

1.4.6. Data Protection Officer

Designation of a data protection officer (DPO) is one of the new requirements for the controllers and processors under the new legal framework. Although in some Member States, such as Poland, France, and Sweden, the designation of a DPO was optionally provided, [327] the majority of the Member States did not have such possibility under their national laws. Only the German Data Protection Law has successfully provided the mandatory appointment of the DPO over 30 years before the GDPR.[328]

Under the GDPR, with the exception of the courts acting in their judicial capacity, any public authority, which processes personal data, shall designate a DPO. [329] Also, similar to the conditions envisaged for DPIA, a DPO shall be appointed in cases where the controller or the processor is a private entity whose core activities consisting

[327] Paul Voigt and Axel Von dem Bussche, p.53.
[328] *Ibid*, p.53.
[329] Article 37(1)(a) GDPR.

of regular and systematic monitoring of the data subjects on a large scale or whose core processing activities consist of special categories of data on a large scale.

At this point, the question of what this requirement has to do with accountability may come to mind. DPOs have been designated by the GDPR, as contact points for data subjects, with regard to all issues related to the processing of personal data.[330] It puts the controllers and processors in a state of constant accountability that requires them to share the quality of the data processing operations to the data subjects in a transparent manner. It also enables and guides data subjects to exercise their rights.

DPOs may be an employee of the controller or processor.[331] The GDPR stipulates that DPOs neither can be instructed concerning the performance of their tasks, nor can be dismissed or penalized by the controller or processor. Nevertheless, the fact that there is no mention or guarantee of the independence of DPOs in the GDPR is causing ambiguities in practice. The DPOs, who engage in an employment relationship with controllers and processors, might tend to hide the real practices of organizations in fear of losing their jobs. Consequently, this may endanger the transparency of the process and therefore accountability. Despite the fact that the controller or processor in question is also tasked with ensuring that the DPO's activities do not result in a conflict of interests,[332] it seems extremely hard to ensure averting such situations in the dynamics of an employment relationship, since the DPO may not be transparent with regard to the quality of data processing operations of the respective organizations, when cooperating with the supervisory authority.[333] In my view, DPOs must be impartial as much as possible, and this can only be ensured if their independence is guaranteed. DPO services should be provided by external, independent organizations. In practice, it is seen that the DPOs do not function any different than the data protection lawyers.

[330] Article 38(4) GDPR
[331] Article 37(6) GDPR.
[332] Article 38 (6) GDPR.
[333] Article 39 (1)(d) GDPR.

Apart from this, in general, DPOs are found useful in planning, awareness building and reflexivity in data protection.[334] Hence, even where organizations do not fall within the scope of Article 37, which obliges controllers or processor to designate a DPO under certain circumstances, they are recommended to appoint a DPO to ensure compliance of their processing activities with the GDPR.

1.4.7. Certification of Accountability and the Principle of Data Protection by Design and Default

The principle of data protection by design and default requires the controller to take appropriate technical and organizational measures not later than the purpose and means of the processing is determined.[335] Article 4 of the Data Protection Act of German land of Schleswig-Holstein demands that the priority in merchandising should be given to the IT products that are in conformity with the data protection principles proved by virtue of certification. This particular approach promotes the principle of privacy by design and default, since data controllers and the vendors of the IT products must ensure the compliance of their new products with the certification requirements in order to gain a competitive edge, specifically in public procurements.[336]

The GDPR also explicitly recommends controllers and processors to demonstrate their compliance with the principle via GDPR certification.[337] However, this recommendation does not indicate that the certification mechanism effectively proves

[334] Yoel Raban, "Privacy Accountability Model and Policy for Security Organizations." **IBusiness,** Vol.4., No.2, 2012 p.168.

[335] Article 23.1 states that "*Data protection by design shall have particular regard to the entire lifecycle management of personal data from collection to processing to deletion, systematically focusing on comprehensive procedural safeguards regarding the accuracy, confidentiality, integrity, physical security and deletion of personal data*." Article 23.2 states that "*The controller shall ensure implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained or disseminated beyond the minimum necessary for those purposes.*" Recital 61 states that "the principle of *data protection by default requires privacy settings on services and products which should by default comply with the general principles of data protection, such as data minimization and purpose limitation*".

[336] Hansen, p. 37-38.

[337] Art. 25 of the GDPR.

that the principle is ensured. It is important to establish how to increase accountability in the light of the principle.

According to the developer of the idea, Ann Cavoukian, data protection cannot be realized merely by complying with the legal framework, but also the concept itself must be a default *modus operandi* for the controllers.[338] She states that there should be seven principles which the controllers should take into account when implementing privacy by design: (i) the measures should be proactive and preventative in accordance with the risk-based approach to privacy; (ii) privacy must be the default setting in the business practice. That could be realized by designing the IT systems that can automatically protect the personal data; (iii) embedding the protective elements into the system taking the purpose of the processing into consideration; (iv) the design must have a win-win approach to the data protection which means that there should not be any trade-offs or pretenses undermining the protection of personal data; (v) the protection must be ensured during the full lifecycle of the data from start until the end; (vi) the process must be visible and transparent during the entire cycle; (vii) the design must be data subject friendly prioritizing the rights and interests of the data subjects.[339] Unless these elements are embedded in the certification criteria, accountability cannot be achieved by means of the GDPR certification.

2. CONCLUSION

Transparency must be regarded as the core prerequisite for accountability. To reduce information asymmetry, and thus the illusion of privacy via data protection certifications, transparency between relevant parties, including certification bodies, must be guaranteed. As stated, certifications can contribute transparency only under the right conditions. When even one of the oldest privacy certification TRUSTe has violated its privacy policy, envisaged objective of enhancing transparency via certification

[338] Ann Cavoukian, 2011 **https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf**, accessed on 7 August 2018
[339] *Ibid.*

mechanisms seems questionable.[340] Besides, in such an untrustworthy environment, the question of how the GDPR certification will provide full transparency comes to existence.

Data protection certifications, if granted by trusted third parties, have the potential to increase transparency. It is easy to notice that all the successful schemes have the intervention of public authorities to their processes to some extent. Public authorities are either in the position of certification bodies themselves, or the auditors, playing the roles of trusted third parties in certification processes. This renders the recipients to be more aware of their data protection responsibilities, and the data subjects to be informed directly by the trusted third parties with regard to the compliance of the recipients with the certification criteria. It, ultimately, leads to more accountable controllers and processors who might compete to comply with the data protection principles, in order to gain a competitive edge in the market.

The co-regulatory and the combination of soft and hard law approaches are regarded useful for ensuring the accountability as well as the transparency.[341] It seems right to name this approach as 'voluntary binding participation'. Where there is a co-operation of the public and private stakeholders in the process, transparency is improved mainly because concerned private parties operate together and share all the information with regard to their tasks and duties.

[340] Federal Trade Commission, *FTC v Toysmart.com, LLC, and Toysmart.com, Inc.*, District of Massachusetts, Civil Action No.00-11341- RGS, **https://www.ftc.gov/enforcement/cases-proceedings/x000075/toysmartcom-llc-toysmartcom-inc**, 10 July 2018.

[341] Rodrigues, Wright and Wadhwa, *Developing a Privacy Seal Scheme (that works)*, p.110.

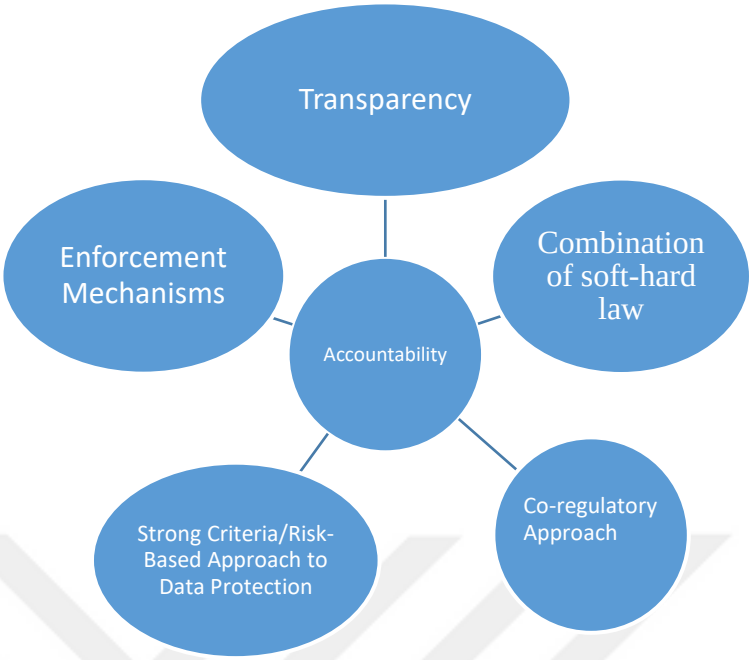

Figure 5: Essential Features of a Data Certification Scheme that Promotes Accountability

Proper enforcement mechanisms are critical for DPCs to promote accountability. Private stakeholders in this regard should function as watchdogs observing both other private stakeholders and public bodies' compliance. Accountability, therefore, must not be considered as a concept that is only necessary for private actors in the process. While public authorities carry out audits to reveal the real practices of the private actors or certificate their compliance, they must be held accountable as well as the other actors. Thus, in order for a certification mechanism to function in line with the principle of accountability, all the stakeholders should be willing to accept responsibility with regard to their respective actions. In addition to the controllers, processors and the supervisory authorities, it is important that the accredited certification bodies are also held accountable with regard to their activities.

All three effective DCPs derive their criteria from the EU legislation, thus all of them demonstrate that the certified processing operations have been carried out in conformity with the general principles such as transparency and accountability and that

the data disclosure to the controller has been protected and that the data subjects' rights have been enforceable. During conformity assessments, certification bodies should evaluate the substantive requirements of the GDPR,[342] such as lawfulness of the processing, the principles of the data processing, the obligation to notify data breaches, and the data subjects' rights.

Section 4 aimed to answer the question of which data protection matters should the GDPR criteria include and how to refine the Articles into the criteria. In my opinion, the criteria must not be only based on the GDPR, but it should pass beyond it. As seen in the example of CNIL certification, data protection certifications must signify the exemplary practices of the controllers and processors in order to fulfill their envisaged objectives.

Additionally, DPCs should mean that all the risks are calculated, and safeguards are implemented by the controllers and processors who obtain certifications. The risk-based approach to data protection requires all stakeholders to take necessary measures before processing personal data, in order to avoid potential risks to the rights and freedoms of natural persons. In other words, certification criteria must be developed in a way to assess the risks and also the preventive measures, in accordance with the risk-based approach. The principle of proportionality, which is crucial to understand what legitimate interest can be and how to balance it, is one of the core principles of risk management, and therefore the scheme owners must definitely include the principle into their criteria. An assessment promoting accountability of the mechanism should cover the principle of data protection by design and default, and it should check whether data protection impact assessment has been concluded along with the technical and organizational measures taken by the controller.[343] Moreover, the questions assessing the conformity of the processing operations must be comprehensive. The appropriate questions to test each requirement must be included in the criteria detailed enough to

[342] ENISA, p.10.
[343] EDPB Guidelines 1/2018, p.10.

reflect the wording of the GDPR. Furthermore, criteria must be understandable, objective and flexible enough to correspond the aspects of the ToE in question.

In light of the requirements established in this Chapter, Chapter 4 of the thesis examines whether the GDPR certification can promote accountability in data protection. In this regard, not only the organization of the certification mechanism but also the GDPR's provisions which potentiate accountability should be scrutinized as the certification aims to certify the GDPR compliance.

CHAPTER 4: THE GDPR CERTIFICATION

This Chapter seeks to answer the main research question of the thesis which is whether the GDPR certification complies with the general prerequisites for an effective

data protection certification mechanism that promotes accountability. As established, in order to complement the other purposes attributed to data protection certifications (see: Section 1 Chapter 3), a properly functioning mechanism is primarily expected to operate as an accountability tool. 3 main conditions for an effective DPC promoting accountability have been established in Chapter 3, as increased transparency, voluntary participation accompanied by effective enforcement, and strong certification criteria enabling proper conformity assessments.

In order to evaluate the effectiveness of the GDPR certification in promoting accountability, the wording of Article 42 and 43 of the GDPR, the guidelines published by the EDPB and other relevant provisions of the GDPR are examined. In this Chapter, however, the effectiveness of the mechanism cannot be assessed entirely, since there has been no GDPR certification been approved until now. This is why, this Chapter only will assess the proposed criteria framework in the light of the current provisions of the GDPR and of the guidelines of the EDPB. It should be reminded that the assessment of the effectiveness of the GDPR certification can be only made hypothetically since there are no feasible outcomes generated by the mechanism. The Chapter also revisits the suggestions made in Chapter 3 to promote accountability in DPCs.

1. TRANSPARENCY IN GDPR CERTIFICATION

In this section, it will be discussed whether the EU can eliminate the problems concerning the lack of transparency in the field of DPCs. How the GDPR certification will contribute to transparency of personal data processing will be discussed in detail. To achieve that, it is important to establish that how the GDPR approaches this very concept and the visible weaknesses of the envisaged mechanism with respect to transparency.

1.1. Is it Possible to Certify Transparent Processing

As stated in Chapter 3, for DPCs to ensure accountability, first of all, transparent personal data processing must be ensured both under the criteria and under the legislation.

Transparency must be the guiding principle of the regulatory frameworks:[344] it must be systematically enshrined in statutory frameworks.[345] If transparency requirement is not described clearly in provisions, it cannot be properly included in certification criteria, and thus it cannot be properly assessed. Also, the right elements potentiating the principle must be ensured under the legislation. Otherwise, even if the rest of the certification process assures transparency, the certification cannot function as a transparency tool, and thus accountability cannot be achieved.

It can be observed that the GDPR handles the transparency as a general principle to be protected. According to Article 5(1)(a), processing shall be lawful, fair and transparent. Directive 95/46 (Art 6) and the GDPR both include the concepts of lawfulness and fairness. However, the concept of transparency has newly been introduced by the GDPR. According to Recital 39, to ensure that personal data is processed in a transparent manner, any information and communication concerning the processing must be:

-easily accessible;
-easy to understand;
-using clear and plain language.[346]

Besides, the controller must also be able to provide clear information to the data subject on:

- the identity of the controller;
-purposes of the processing;
-any other information required to ensure the data subject that the processing is lawful, fair and transparent.[347]

[344] Bartle and Vass, p. 47
[345] ENISA, p.28.
[346] Recital 39, para.1 of GDPR.
[347] Recital 39, para 2 of GDPR.

More accurately, transparency constitutes the basis of the information requirements and enables data subjects to control their own data.[348] The GDPR, stipulating transparency as a general principle to be protected seems to ensure that the future DPCs are entitled to certify the processing operations that are only sufficiently transparent. However, transparency can be very difficult to ensure in complex processing operations, such as automated decision-making. In case of such decisions, it is very difficult to understand how the decision is made and prove the transparency of the processing because it requires data subjects to understand complex algorithms. The complexity of such processing can damage the communication between the data controller and data subjects, thus it prevents transparency. In this regard, the GDPR certification can play a big role in providing transparency to data subjects, if the scheme is reliable.

Furthermore, the GDPR rules that personal data must be processed fairly without including any definition of the concept of fairness. Recital 60 of the GDPR analyzes the principles of fair and transparent processing together, stating those principles require the data subject to be informed of the existence of the processing and its purposes. This approach can create many problems considering that the vast majority of processing operations today are being performed by Artificial Intelligence using specific algorithms to take decisions. Such algorithms can take biased decisions which can even threaten fundamental human rights of data subjects (e.g. racial, ideological or gender biases).[349] Although the GDPR provides a right to object to such decisions, the algorithms that are used by machine learning for making decisions on the processed data can be very deceptive, as they are not easily understandable for those who do not have expertise in the area. This is in fact where the GDPR certification can make difference since the fairness of the processing can be certified by the certification experts. However, the current ambiguity on the meaning of the 'fairness' may jeopardize envisioned accountability, if the certification criteria accept fairness as an information duty of the

[348] European Commission, Commission Staff Working Paper, Impact Assessment, Brussels, 25.1.2012 SEC (2012) 72 final, Annex 2, p.16.

[349] **https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazonscraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G**, accessed on 12 December 2018).

controller. Therefore, the concept of fairness must be differentiated from transparency and should be made clear both in general sense and with regard to the automated decision-making processes. Otherwise, the lawfulness of the processing cannot be ensured and verification of the compliance via certification would be misleading.

If this uncertainty remains, the problems of asymmetry of information and illusion of privacy cannot be eliminated in the market and in long term, the GDPR certification may lose its potential to provide accountability.

1.2. Transparent Procedure during Evaluation

As mentioned, in Chapter 3, the second requirement for transparency is a transparent procedure to be ensured from the beginning of the process until the very end. On this matter, Article 42 (3) indicates that the certification shall be "*available via a process that is transparent*". Although the Article remains silent how the transparency exactly will be realized in practice, the EDPB states that for the process to be carried out in a transparent manner: there must be documentation provided for each step of the evaluation.[350] Documentation must be of pivotal significance for both certification bodies and supervisory authorities, in order for the system to be successful. It can be interpreted that transparent documentation is constantly required under the GDPR from the beginning of the processing, during the evaluation and even after the attestation. Though no process has been realized yet under the new certification regime, this is a good indication that transparency is tried to be ensured during the whole process.

Expectedly, the GDPR provides that the EDPB shall collect all certifications in register and make them publicly available. Therefore, all of the approved criteria under the GDPR certification mechanism, are expected to be published online. In these terms, it appears that the GDPR certification has prepared the basis that could enable the comparability of certifications issued.

[350] EDPB Guidelines 2018, p.5.

As stated in Chapter 3, the conformity assessment should be clear and transparent, the methods and the methodology of the assessment must be identifiable. For example, how the certification bodies will collect the information necessary for the conformity assessment is significant. In relation to this, the requirement of Article 43(5) that the certification bodies shall provide the reasons for granting or withdrawing the certification to the competent supervisory authorities, clearly contributes the transparency function of the certification mechanism.

Some points that might endanger the transparency of the process can be mentioned here. The supervisory authorities are both tasked with approval of the criteria and assessing the conformity of the applicant controller and processors, at the same time they are entitled to audit the compliance of the same applicants which may cause function creep. In order to prevent this, it is important to ensure that the different impartial actors carry out different tasks in the certification process. In practice, the certification process of the EN-ISO/IEC 17065, in which the experts who evaluated the conformity are not involved in the decision stage, is commonly followed by certification schemes:[351] SH certification has two distinct phases during evaluation: the evaluation of the compliance and the validation of the evaluation. After this step, the certification body assesses the report conducted by the expert team and gives the final decision.[352] CNIL certification also consists of two distinct evaluation phases. If admissible, the application is respectively sent to the Privacy Seal Unit and the Seal Deliverance Committee. The GDPR certification is also inspired by the EN-ISO/IEC 17065 with respect to the certification process, and therefore it is expected to provide different impartial expert groups for each stage of the process. This organizational structure can prevent function creep while increasing the accuracy of the evaluations.

Another measure to prevent possible function creep is, once more, to ensure the transparency particularly via proper documenting of all stages of the certification process. In terms of the GDPR certification, documentation must be complete and comprehensive

[351] Kamara and De Hert, p,16.

[352] Rodrigues, et al., *EU Privacy Seal Project, **Inventory and Analysis of Privacy Certification Schemes***, p.39.

leaving no room for doubt. As stated in the Guidelines on certification of the EDPB, without proper documentation, a proper assessment cannot be achieved.[353]

1.3. Transparency after the Attestation of the Certification

Article 42(6) states that the controller or processor, which applies to the certification mechanism, should enable the competent supervisory authority (or the accredited certification body) to access all the information regarding its processing activities. As mentioned, in Chapter 3, a transparent certification mechanism requires regular surveillance to be provided in the post-certification process as well.

Certification under the GDPR can be issued for a maximum period of three years. Although there is no statement concerning on-spot audits in the Regulation, Article 42(7) provides that certification must be revoked by the certification bodies or by the supervisory authorities if the requirements for the certification are no longer met. according to Article 43(7), the same rule applies when the requirements for the accreditation are no longer met by a certification body. Likewise, Article 57(1)(n) specifying the tasks of supervisory authorities states that each authority shall on its own territory "*where applicable, carry out a periodic review of certifications issued in accordance with Article 42(7)*", and Article 58 referring powers to the supervisory authorities states that each authority shall have the power "*to carry out a review on certifications*". These Articles imply that the supervisory authorities do not have to carry out periodic reviews where the circumstances do not allow to do so. Also, it appears that only one review would be deemed enough by the legislator during the validity period of each certification. "Periodic review" is not explained in the GDPR either; it is not clear whether it means an on-spot audit or only a documentation review. To ensure transparency of the whole process these ambiguities should be elucidated in detail by the EDPB.

[353] Guidelines 1/2018, p.15.

As regards to transparent complaint mechanism, under Article 43(2)(d), certification bodies can only be accredited if they have established complaint mechanisms to handle complaints concerning the infringements of the certification. Yet again, all the procedures of these mechanisms must be transparent to data subjects and to the public. This provision constitutes an important driving factor for accountability as it will be explained in detail in Section 2.3.

Although, the regulation seems to ensure transparency after the attestation, there can be some points mentioned to improve transparency of the post-certification period. The feedbacks of the recipients improve the transparency of the post-certification periods. For example, in the first year of the grant of the CNIL certification, the entities of which the processing activities has been certified, are required to submit an activity report providing feedback to CNIL with regard to the conformity of the procedures and products in question with the standards.[354] To promote accountability, a similar type of arrangement is advised to be adopted by the GDPR certification.

2. THE REGULATORY FRAMEWORK GOVERNING THE GDPR CERTIFICATION

2.1. Voluntariness in GDPR Certification

As stated, Article 42 foresees a voluntary certification mechanism; however, the GDPR itself is binding in its entirety. In my opinion, GDPR certification combines both hard and soft law approaches; because, although the mechanism itself is voluntary, demonstration of the compliance, in any case, is obligatory under the GDPR. The introduction of this voluntary mechanism aims to provide a transition between the soft and hard law instruments in data protection.[355] Considering that the provisions of the

[354] *Ibid.*, p.55.

[355] Lachaud, *Why the certification process defined in the General Data Protection Regulation cannot be successful*, p. 8.

GDPR are binding, data controllers and processors would be held accountable under the GDPR regardless of their certification status. Some think that it is the best approach for promoting accountability in data protection[356] and in my opinion, it can alleviate some of the problems in the DPC market.

Here, the potential implications of this approach should be recalled in light of the suggestions in Chapter 3 of the thesis. First of all, while the voluntariness of the certification increases efficiency, the legally binding nature of the certification agreements, and of the GDPR would create a hard law impact which improves accountability. This hard law impact will be discussed in Section 2.3 in detail.

Second, Article 42 applies only to the data controllers who wish to demonstrate their compliance via certifications, in other words, only the ones that wish to prove their accountability would apply to the scheme. In the long run, this can foster the intended competition among data controllers.

Third, the approach provides the necessary flexibility required in data protection which is a technology-driven field that must be adapted to the new developments in the area.[357]

2.2. Private Participation in the GDPR Certification Process

As discussed in Chapter 3, in order to increase accountability, the private sector should engage in the certification processes. In this Section, to what extent the GDPR engages the private sector in the process will be discussed.

As some authors noted, the certification mechanism has been introduced by the EU legislator deliberately to create "*a regulatory continuum between self-regulation and*

[356] Raban, *Privacy Accountability Model and Policy for Security Organizations*, p.170.
[357] Trubek et al., p.12.

traditional regulation".[358] The GDPR certification is neither self-regulatory nor full-regulatory, but it is co-regulated, as there will be co-operation of different stakeholders during and post-certification process. In accordance with the approach, the GDPR requires all stakeholders including the Member States, supervisory authorities, EDPB, the Commission, accredited private and public certification bodies and private organizations to co-operate in the certification processes. [359]

Four main actors involve in the certification process under the GDPR:

-Data controller or processor (applicant);
-Accredited certification body;
-Competent supervisory authority;
-The European Data Protection Board.

Lachaud stated that the GDPR certification mechanism envisages a complicated range of processes, the pattern of the co-regulation is vague, and it prescribes "*complex matrix of responsibilities*".[360] Based on the classification made by Bartle and Vass,[361] the framework of the GDPR certification does not correspond to one specific category; it reflects an atypical sort of co-regulation; it possesses the characteristics of multiple types. Indeed, there are several duplicating tasks determined under this atypical framework. For example, both the competent supervisory authority and the certification bodies have the responsibility to grant certifications.[362] Additionally, they both have the power to review and, if necessary, withdraw the certifications. Until this point, the framework appears to bear the qualities of a co-operative co-regulation, because it requires private stakeholders to undertake the role of certifiers together with the supervisory authorities. However, it is worth noting that the certification bodies must inform the competent supervisory

[358] Eric Lachaud, The General Data Protection Regulation and the rise of certification as a regulatory instrument **Computer Law & Security Review**, The International Journal of Technology Law and Practice, September 2017, doi:10.1016/j.clsr.2017.09.002, 10 July 2018.
[359] Article 42-43 of the GDPR.
[360] Lachaud, *Why the Certification Process Defined in the General Data Protection Regulation cannot be Successful* p.7
[361] Bartle and Vass, p. 203.
[362] Article 42(5) of the GDPR

authority with regard to every step of their certification practices, including the reasons for issuing or revoking the certifications.[363] This fact shows us that there is a delegated co-regulation in the GDPR certification process. On the other hand, the approval of the criteria that will be developed by the private scheme owners, by the competent supervisory authorities reflects a characteristic of facilitating co-regulation. Thus, it also falls into the category of facilitating co-regulation since the certification is voluntary and the public authorities can encourage, accredit and monitor the DPCs.

It is likely that supervisory authorities without sufficient personnel and experience in the field, will not carry out the certification process themselves. They will instead accredit the efficient self-regulatory certification schemes in order for them to certify the processing activities of the applicants. Therefore, in practice, the framework might also represent the qualities of delegated co-regulation.

Accredited certification bodies that require "*an appropriate level of expertise in relation to data protection*" have been introduced by the GDPR. A competent supervisory authority or the national accreditation body are authorized to grant accreditations to the respective entities. Legal entities under private and public law can both apply for the accreditation, provided that they demonstrate their independence and their expertise regarding the target of evaluation of the certification to the satisfaction of the competent supervisory authority.[364] An accredited certification body or a competent supervisory authority are entitled to issue certifications as provided in Article 43 of the GDPR. Conditioning that the private parties, which have sufficient expertise in the field, may participate to the process as certification bodies, increases the effectiveness of the co-regulative frameworks since the mechanism would have the sufficient capacity to achieve the goals of the respective regulation; they would have the facilities to recognize the inefficacies and obstacles in the process of which they are responsible to carry out. [365] In practice, it is expected that only the large firms already experienced in the field would

[363] Article 43 (5) of GDPR.
[364] Article 43(2)(a) of the GDPR.
[365]Balleisen and Eisner, p.134.

participate in the process as certification bodies, owing to their capacity to afford costly practices.

As stated in Chapter 3, the co-regulatory approach requires some degree of flexibility in order to be effective.[366] Such flexibility can be seen in the GDPR certification, as it allows the scheme owners to develop their own criteria based on the principles and rules enshrined in the GDPR. Apart from that, they are also provided with sufficient procedural autonomy since they are allowed to create their own certification schemes, as well as their own procedures for monitoring, reviewing the processes and also withdrawing the certifications. [367]

Co-operation in accrediting and reviewing potentiates independency and reduces biased practices.[368] The GDPR certification mechanism envisages co-operation between supervisory authorities and National Accreditation Bodies (NABs) in accrediting the certification bodies. Article 43 provides that the Member States shall ensure that the out-sourced certification bodies are accredited by the competent supervisory authority or the national accreditation body in accordance with EN-ISO/IEC 17065/2012. Member States can only have one NAB and NABs are considered to exercise public authority, regardless of their legal status, to assess the technical competence of the certification bodies.[369] Thus, NABs, in some Member States can be private bodies to which public authority is delegated.

While the NABs and supervisory authorities together accredit and monitor the certification bodies, the accredited certification bodies and supervisory authorities certify the processing activities of the applicants, they review the compliance of the recipients, and further, they will revoke the certification if the requirements of the criteria are no longer met. Rodrigues writes that this model creates an "*independent, non-biased and*

[366] *Ibid.*, p.133.
[367] Guidelines 2018/1, p.8.
[368] Rodrigues, Wright and Wadhwa, p.114.

[369] Article 15 of Regulation 765/2008.

effective" stage for the stakeholders to express any matters concerning exploitation of certifications.[370]

The co-regulated approach is criticized because the certification mechanism may easily become a "*trojan horse*" that could highly undermine the personal data protection and accountability, instead of improving it.[371] Korff argues that accredited certification bodies that are not subject to directions from supervisory authorities might by-pass all European cooperation and consistency mechanism.

Although this criticism is notable, the success and trustworthiness of the GDPR certification highly depend on how the public authorities will involve in the certification process carried out by the private certification bodies. This is not only required for the accountability, but also for the transparency of the process. As previously stated, there are many tasks and powers allocated to the supervisory authorities in the process. The supervisory authorities do not only have the power to issue or withdraw the certifications,[372] but they also have power to approve the certification criteria after communicating with the EDPB regarding the criteria, carry out a periodic review of issued certifications, order the certification bodies to withdraw the certifications, and accredit certification bodies.[373] Regular audit of the private stakeholders involved in the certification process is obviously an indication that the EU legislator did not disregard the importance of the principle of accountability.

2.3. Linking Enforcement Mechanisms to DPCs

As discussed in Chapter 3, properly functioning enforcement mechanisms are significant for data subjects to enforce their rights enshrined under the laws and are also crucial to ensure the effectiveness of the GDPR certification. Because an effective certification should represent an accurate 'account', there should be sanctions in place in

[370] Rodrigues, Wright and Wadhwa, p.114.
[371] Douwe Korff, p.11.
[372] Article 58(3)(f) and 58(2)(h) GDPR.
[373] Article 57(1)(o); 58(2)(h); 58(3)(e); 64(1)(c) GDPR.

cases where the account is turned out to be not accurate. Where the certification does not represent the reality, not only of the data controller, but also the liability of the certification bodies (public or private) who certify the activities of the data controller should be in question. Also, the situations in which the data controller is the public authority must not be neglected.

First of all, we stated that DPCs should provide enforceable guarantees. Certification agreements can be enforced in this matter. But under the new framework, the GDPR Article 43(2)(d) provides that the accredited certification bodies shall have "*established procedures and structures to handle complaints about infringements of the certification or the manner in which the certification has been, or is being, implemented by the controller or processor…".* Such complaint mechanisms can be effective in ensuring that the guarantees stated in the criteria are enforceable. Considering that, as in the case of CNIL certification, certification criteria can go beyond the GDPR requirements, in terms of some certification, the enforceability can even go beyond the GDPR requirements.

However, the GDPR does not mention any external complaint mechanism to be ensured by the certification bodies. One of the problems regarding DPCs has been the fact that complaint mechanism being entirely internal. To eliminate the problem of biased decisions, impartial parties should involve in the complaint processes. The GDPR does not bring a solution to this very problem in its fullest sense, but it states that the accredited certification bodies must have "… *demonstrated, to the satisfaction of the competent supervisory authority, that their tasks and duties do not result in a conflict of interests."*[374] It can be inferred from that the departments which handle the complaints must be separated from the rest of the departments of the certification body (evaluation and decision bodies), although there is no clear explanation on how the competent supervisory authority should decide whether there is a conflict of interests. Also, as stated in Section 1 of this Chapter, the procedures and structures governing the complaint mechanisms

[374] Article 43(2)(e) of the GDPR.

shall be transparent to data subjects and to the public.[375] It appears that the Article enables the decisions of the internal or external complaint mechanism to be monitored by the public and mitigates the possibility of biased decisions which has been detected as a recurring issue in the DPC market.

Certification can be granted, no longer than 3 years with the possibility of renewals, to the companies that proved their compliance.[376] Expectedly, the certification bodies have the right to withdraw the GDPR certification in case the recipient concerned no longer meet the criteria during the post-certification period. The legal effect of a breach of a certification agreement is the revocation of the certification. The revocation clause stipulated in a certification agreement demonstrates that the certified entity would lose its advantage of using the certification in case of non-compliance with the agreement. The likelihood of revocation of the GDPR certification appears to be a successful incentive for the recipients to keep being compliant, hence it may improve accountability.

The existence of a DPC should not free the recipients from their legal responsibilities. Monitoring in form of follow-on audits can be conducted both by the accredited certification bodies and supervisory authorities and it makes timely enforcement possible. Article 57(1)(o) provides that supervisory authorities shall carry out a periodic review of certifications issued. This means that the GDPR certification does not free the recipient from its responsibility and increases the effectiveness of the scheme. Moreover, according to Article 58(1) of the GDPR, ex officio proceedings can be initiated upon suspicion by the competent supervisory authority against controllers and processors. Under this procedure, supervisory authorities have the right to access any possessions and establishment of the controller and processor. According to Article 58(1), supervisory authorities can order controller, processor, or their representatives to provide any relevant information necessary for fulfilling their investigation tasks, they shall carry out data protection audits and review of certifications. These audits can also be carried out without any prior notification.[377]

[375] Article 43(2)(d) of the GDPR.
[376] Article 42(7) of the GDPR.
[377] Voigt and Von dem Bussche, p.204.

As stated in Chapter 3, establishing high fines in case of violations is effective in increasing the commitments of the private stakeholders.[378] Depending on the importance of the Articles infringed, there are two categories of administrative fines to be imposed: the first is the maximum amount of 10 000 000 EUR, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher. The second category is up to 20 000 000 EUR, or 4 % of the total worldwide annual turnover of the preceding financial year, again, whichever is higher. Expectedly, the second category of administrative fines are to be imposed in cases of breaches of the data subject rights, general principles for processing and conditions for consent, and with regard to trans-border data flows.[379]

Although the sanctions under the GDPR are scarce yet, under the Directive, Facebook Ireland Ltd was fined by ICO for £ 500,000 on 24 October 2018, due to unfair and unlawful processing of personal data that had been occurred before the GDPR entered into force, affecting almost 90 million data subjects whose personal data had been processed by Facebook.[380] Also, recently French CNIL fined Google Inc. for EUR 5,000,000.00 due to non-compliance with transparency and consent requirements under the GDPR. [381]

Data subjects can also lodge complaints with supervisory authorities in the Member State of his or her habitual residence, place of work or place of the alleged infringement.[382] This, in essence, provides a great bundle of choices and convenience to data subjects in relation to where they would like to lodge their complaints. Data subjects

[378] Balleisen and Eisner, p.131.

[379] Art. 83(5) of the GDPR.

[380]Information Commissioner's Office (ICO), Monetary Penalty Notice, 24 October 2018, https://ico.org.uk/media/action-weve-taken/mpns/2260051/r-facebook-mpn-20181024.pdf, 1 November 2018, para.4.

[381]https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000038032552&fastReqId=2103387945&fastPos=1, accessed on 25 January 2019.

[382] Art. 77(1) of the GDPR.

either can launch proceedings directly against the controller or processor under Article 79(2) or they can commence proceedings before the national courts against the supervisory authorities that fail to act timely or reject their complaint. Hence, it is highly possible that a data subject can both invoke its rights under the GDPR and also challenge the certification status of the organizations. Furthermore, compensation can be claimed by anyone who suffered material or non-material damage due to an infringement of the GDPR.[383] According to Article 82(2), any controller engaged in processing operations shall be accountable for the harm done. This provision will increase the burden of the controllers because they might pay fines in addition to the compensations to the data subjects.

The GDPR certification can be used as a protective base that economically shielding the organizations against high administrative fines. Article 83 provides elements that should be regarded by the supervisory authorities when deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case. One of the elements which shall be taken into account by the supervisory authorities is given as "*approved certification mechanisms pursuant to Article 42*". Thus, the entities of which processing activities certified by an accredited certification body or supervisory authorities will be advantageous compared to the ones without certification. It should be noted repeatedly that obtaining certification does not mitigate the responsibility of the controller or processors. However, certified entities might face administrative fines in very limited cases.[384] This is mainly because, the GDPR certification is expected to demonstrate that the organization has already taken all the necessary technical and organizational measures such as data protection by design and default, the appointment of a DPO and conducting a DPIA. Nevertheless, in my opinion, the GDPR certification must certify more than the mere compliance with the Regulation. CNIL certification promotes "corporate social responsibility" based on transparency and accountability.[385] Once the applicants receive the certification, they do not only show their compliance with the laws, they show that their personal data processing activities are

[383] Art. 82 (1) of the GDPR.
[384] Voigt and von dem Bussche, p.79.
[385] Carvais – Palut, p.55.

praiseworthy in every aspect.[386] Even though at first glance, this opportunity seems to disregard the accountability of the recipients of certifications, it is a way of endorsing the certification mechanism and therefore the principle of accountability.

Under such a deterrent framework, one can claim that demonstration of compliance would become crucial for the controllers and processors, and they would try to find best fitting ways to do so in accordance with the individual structures of their organizations. Since it is the only way, to visibly demonstrate the GDPR compliance, the GDPR certification may become incredibly common amongst controllers and processors to compete with each other in terms of the GDPR compliance and to attract more customers. Therefore, whereas the mechanism can eliminate the issue of lack of competition in the market, the legislation can improve the effectiveness of the complaint and enforcement mechanisms. Finally, this framework would promote overall compliance with the GDPR, while encouraging controllers and processors to demonstrate their compliance via GDPR certifications.

3. THE GDPR CERTİFİCATİON CRİTERİA

It is not possible to test whether the GDPR criteria would be strong because no criteria under Article 42 has yet been approved. It is stated in the official website of EuroPriSe that the criteria catalog incorporating the GDPR requirements has not been approved and the entity has not been accredited as a certification body.[387] This is why it is not possible to make an assessment of the approved criteria at the time of the writing of the thesis. However, one can scrutinize the procedural requirements concerning the approval of the certification criteria and their potential implications for the intended accountability and harmonization. This would give us an insight into the extent of the potential effectiveness of the GDPR certification with regards to the promotion of accountability.

[386] *Ibid*, p.55.

[387] **https://www.european-privacy-seal.eu/eps-en/criteria**, 12.12.2018.

3.1. The Approval of Criteria

The GDPR only provides a framework that explains how the criteria will be approved by the authorities.[388] It has designated competent supervisory authorities as the bodies to approve the certification criteria. Even though it is not clear either in the GDPR, or in the Guidelines 1/2018 on certification and identifying certification criteria in accordance with Article 42 and 43 of the Regulation (Guidelines on Certification) how and by whom the criteria will be drafted, it is stated in the Guidelines on Certification that "*a scheme owner creates criteria and procedures*",[389] without clarifying the definition of a scheme owner. According to the ISO/IEC 17065 "*the scheme owner can be the certification body itself, a governmental authority, a trade association, a group of certification bodies or others*".[390]

As recognized under Article 6 (2), Member States may maintain or introduce further rules to specify a legal basis for data processing. Hence, Member States will presumably introduce different options allowing data controllers to process on a different legal basis which may create legal uncertainties in the future[391] with regard to certification criteria as well.

In cases where the Member States determine different legal bases for processing, supervisory authorities may approve different criteria, which would create multipolicy among the GDPR certifications. While one of the aims of the endorsement of the certification is to harmonize the data protection certification market, there can be *de facto* many different sets of certification criteria circulating within the EU.

This means that the GDPR allows various certification mechanisms, and criteria to exist in the market simultaneously. This also means that competent supervisory

[388] EDPB Guidelines 1/2018, p.10.
[389] *Ibid.,* p.8.
[390] https://www.iso.org/obp/ui/#iso:std:iso-iec:17065:ed-1:v1:en
[391] Voigt and Von Dem Bussche, p.100-101.

authorities may approve a specific set of certification criteria consisting of a specific type of activities. Bitkom warns that there might be numbers of different criteria existing under different certification schemes, since any certification body may create its own criteria and submit to the accreditation bodies for the approval. [392] It has been asserted by many authors that the flexibility that has been recognized concerning the approval of the criteria may harm the intended interoperability of the certifications and further the harmonization of the data protection standards at the EU level.

Nevertheless, there can be no single standard criteria for data protection certifications, since the context and the nature of data processing activities differ vastly. Also, the criteria cannot be monolithic, they must be adequately flexible so that they correspond the necessities of different processing activities wanted to be certified. That is why, it is inevitable that there will be many different criteria for different ToEs in the EU, but they will all be based on the standards set in the GDPR. The EDPB states that, in any case, criteria must reflect the requirements stipulated in the GDPR, and it must contribute the consistent application of the GDPR.[393] Hence, supervisory authorities of all Member States must cooperate closely in order not to approve conflicting criteria across the EU.

In the last analysis, this potential dichotomy would not cause serious fragmentations in the implementations in different Member States, because all the criteria will be approved in accordance with the compulsory GDPR standards and within the knowledge of the EDPB. The EDPB has explained the purposes of the certification criteria as reflecting the requirements and principles laid down in the GDPR and contributing to the consistent application of the GDPR.[394] In light of these circumstances, one can construe that the harmonization objective would be achieved within the standards of the GDPR.

---

[392] Bitkom views on EDPB Certification Guidelines under Regulation 2016/679 **https://www.bitkom.org/noindex/Publikationen/2018/Positionspapiere/Bitkom-views-on-EDPB-Certification-Guidelines-under-Regulation-2016679/20180711-Bitkom-Position-Paper-on-the-EDPB-Guidelines-on-Certification.pdf**, 10 July 2018.

[393] EDPB Guidelines 1/2018, p.9.

[394] EDPB Guidelines 1/2018, p.9.

3.2. Criteria or the Seal?

The EDPB states that the certification bodies may issue certifications under the seal.[395] Certification criteria that are approved by the EDPB may result in European Data Protection Seal which functions as a common certification.[396] In case certification criteria are approved by the EDBP pursuant to Article 42(5), accredited certification bodies may issue certification on the basis of these approved criteria on the EU level.[397]

In this context, if the EDBP approves criteria approved by a supervisory authority in a Member State, those criteria become a seal. At the same time, there might be other criteria in circulation, and they can be in use together with the seal. However, it is not clear which criteria the certification bodies should rely on when assessing the compliance of their applicants' processing activities. This dichotomy between the seal and the criteria may create confusion in practice, since the certification bodies can issue certifications, alternatively both according to the seal or to the criteria approved by the competent supervisory authority. Neither the wording of the GDPR nor the Guidelines by the EDPB give any clue on how the certification bodies should choose between the seal or the approved criteria. As a matter of course, it seems more logical to count on the criteria that will be approved by the EDBP (the seal or the EDPS).

In my humble opinion, there should be a step-by-step harmonization on the certification mechanism, starting with the national criteria, developing into a common criterion: "the seal". It may decrease the confusion emerged due to the proliferation of the schemes.[398] As long as no extreme costs are set for obtaining the seal, it would be likely that the data controllers and processors of the big companies would prefer applying for the seal instead of the criteria approved by their competent supervisory authority, in order to demonstrate their compliance across the EU.

[395] EDPB Guidelines 1/2018, p.10.
[396] Art. 42(5) GDPR.
[397] EDPB Guidelines 1/2018, p.10.
[398] Rodrigues, Wright and Wadhwa, p. 114.

4. CONCLUSİON

In this Chapter, the GDPR certification has been tested against the prerequisites for accountability established in Chapter 3, in order to find an answer to the main research question of the thesis. Transparency, the co-regulatory framework including enforcement, sanctions and remedies, and strong criteria were defined as the prerequisites of an effective DPC. In parallel with the main research question, the Chapter also sought to find an answer to the question of to what extent the GDPR certification can eliminate the problems occurring in the DPC market.

It is not clear in some respects whether the new mechanism can solve the problems regarding the lack of transparency. To eliminate asymmetry of information, it must be clarified how transparency and fairness of the processing should be ensured, particularly in the cases of automated decision-making processes. It must be detailed how the supervisory authorities will carry out periodic reviews of the granted certifications. Reviews definitely must be on-spot and these audits must be documented using identical templates. Most importantly, the results of the reviews also must be published publicly. It is important to mention again that the fate of the objectives other than the transparency is highly dependent on how and to what extent the transparency is achieved in the certification mechanism.

Although Article 42 reflects a soft law approach, the GDPR, being entirely binding, reflects the impacts of hard law such as clear guidance, uniform treatment, sanctions, and justiciability.[399] The GDPR seems to adopt an unordinary version of the co-regulatory approaches presented above. As stated in Article 43, an accredited certification body or competent supervisory authority can certify the processing activities of an entity, but all the steps taken by the certification bodies with regard to the certification process must be within the knowledge of the supervisory authorities. The

[399] Trubek, p.3.

structure has been designed for the actors to constantly communicate during the procedure and also for optimizing the limited sources which stem from the lacking knowledge and experienced staff in the field. This hybrid arrangement reflects the co-regulatory approach and the GDPR adopts it efficiently and uniquely with regard to the certification mechanism. I choose to name this approach as "*voluntary binding participatory*" approach. It is voluntary in conformity with the soft law approach. However, at the same time, it is binding since once the certification bodies have committed to participate in the scheme, they become accountable to the supervisory authorities as accredited certification bodies. Although the GDPR requirements are obligatory to fulfill, data controllers, after having signed the certification agreement, become accountable also to the certification bodies. Lastly, it is participatory: it embraces all the stakeholders in the market (data controllers and private certification bodies).

The GDPR introduces "*the European Data Protection Seal*" with a view to establishing a pan-European certification mechanism. To prevent complications, supervisory authorities should not be given the choice of issuing certifications on the basis of either criteria or the seal.

CHAPTER 5: GDPR CERTIFICATION AND TRANS-BORDER DATA FLOWS

The digital world has no borders. In accordance with the state of art of the technology, hardware has become only a small part of our devices in use today. People, every day, upload an enormous amount of their personal data to a network that can record, document, transfer personal data and even predict the basic human behaviors. Once it is

uploaded to the internet, the data can easily be sent from one continent to another without being subject to any restriction.

Unfortunately, early regulations in Europe did not attempt to introduce the rules concerning trans-border data flows, since trans-border data flows had been regarded as the exception rather than the rule.[400] The conflicts between the legal orders are inevitable[401] ; the GDPR rules will conflict with data protection rules of other countries, if international legal instruments do not offer better effective solutions.

Because there are no globally recognized data protection standards, in the context of cross-border data transfers, the following risks emerge:[402]

- Non-compliance with the EU data protection law
- Unlawful emancipation of personal data
- Failure to provide access rights to data subjects (lack of transparency)
- The lack of co-operation with the EU authorities in case of complaints
- Inadequate level of protection of personal data
- Conflicts between the EU and the third country laws
- Access to and misuse of personal data by the foreign governments
- Third state's court decisions demanding the revelation of personal data
- Difficulties regarding the recovery or secure disposal of personal data
- Mistrust of individuals due to the misuse of personal data

One can simply notice that those problems mostly stem from conceptual and political differences, and they particularly gather around enforceability issues. Especially, the differences between the data protection rules of the EU and the US have been problematic. Furthermore, in the light of the principle of accountability, redress

[400] Christopher Kuner, "Extraterritoriality and Regulation of international data transfers in EU data protection law". **International Data Privacy Law**, Vol.5, No.4, 235-245, 2015, p.14.
[401] *Ibid.*, p.241-242.
[402] Christopher Kuner, "Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present, and Future", https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1689483, p.31.

availabilities in third countries, for data subjects, are indispensable in order to guarantee a comparable level of data protection ensured in the EU. Although the acceptance of global data protection standards seems to be the solution at first sight, first of all, it is not easy to assess the level of data protection of each country in its entirety. Secondly, this issue is highly relevant to the democracy and human rights' standards and the level of the arbitrariness of each state.

As the GDPR certification mechanism is a means of demonstrating the presence of appropriate safeguards provided by the controllers or processors, even if they are not located in a third country providing an adequate level of personal data protection, it may offer a solution to the issues aforementioned. But, how many of these problems can be solved by the GDPR certification mechanism? The previous chapters have demonstrated that the GDPR certification may eliminate the mistrust of individuals, ensure transparency and therefore, may prevent unlawful emancipation of personal data within the EU if it employs the prerequisites determined for the effective certification schemes.

However, it is unclear in what manner the GDPR certification will ensure the protection of personal data in the trans-border data flows. In this chapter, it will be discussed whether the GDPR certification is an appropriate tool to be relied on in trans-border data flows, and under what circumstances it should be preferred by the organizations in third countries. It should be noted that the trans-border flow of personal data is an issue that is also related to questions of applicable law and jurisdiction.[403] Hence, the main question to ask should be whether the GDPR certification would be capable of ensuring the data subjects rights. A couple of questions must accompany this main question: how will the certification bodies carry out on-spot audits in third countries? Who will certify the processing operations of third country data importers? Can the GDPR certification pave the way to effective investigations in third countries or is it just a perfunctory mechanism which will play a role until better solutions are figured out? Has it been designed only to be an alternative to the existing options or in some cases is it the

[403] Kuner, *Extraterritoriality and Regulation of international data transfers in EU data protection law*; Rolf H. Weber, Transborder data transfers: concepts, regulatory approaches and new legislative initiatives. **International Data Privacy Law,** Vol.*3, No.*2, (117-130), 2013.

only reliable option? In order to answer those questions, one must also consider alternative safeguards recognized under the GDPR on the same matter. This is needed to comprehend why the legislator has introduced such a mechanism to be relied on as an appropriate safeguard.

1. EXTRA-TERRITORIAL SCOPE OF THE GDPR

The GDPR has an extra-territorial scope, since it applies to the processing of personal data of the individuals in the EU, even in cases where the controller or processor are not established in the EU.

Pursuant to Article 3, the GDPR applies to 3 territorial cases. First, in cases where the controller or processor process personal data in the context of the activities of an establishment in the EU. In *Google Spain* Case, the Court found that Google Inc. "*orientates its activities towards the inhabitants*" of Spain, by envisaging "*to promote and sell advertising space*" by its branch established in Spain; the Court found that the processing was carried out in the context of the activities of an establishment of the controller within the EU.[404] Thus, the GDPR applies to the cases where a controller or processor is not established in the EU but processes personal data of the data subjects in the Union with the purpose of offering them goods or services or monitoring their behaviors.[405] Finally, it applies to the cases where a controller is not established in the EU but processes personal data in a place where Member State law is applicable by virtue of public international law.[406] In all of these cases, respective controllers are obliged to demonstrate that they ensure at least one of the appropriate safeguards envisaged in the GDPR, such as the GPDR certification.

Kuner notes that when assessing the scope of extraterritoriality, the extent of the secondary sources such as adequacy decisions and SCC decisions by the Commission

[404] *Google Spain* Case, para 60.
[405] Art. 3 GDPR.
[406] Art. 3 GDPR.

should be considered.[407] We should, therefore, consider DPCs when determining extraterritoriality since they mean, within the scope of the GDPR, adequate safeguards as well as the SCCs and the adequacy decisions.

Certification mechanism can be preferred by foreign organizations in 2 situations:

- If they fall within the territorial scope of the GDPR according to Article 3;
- They receive personal data of the natural persons located in the EU.

These two points are interconnected. The transfer of the personal data means processing of the personal data because according to Article 4(3), any operations on personal data means processing. When personal data of the individuals in the Union are transferred to controllers or processors that does not fall within the scope of the GDPR, the recipients of the data enter into the scope since they actually process the data received. Hence, it is possible to claim that the EU legislator aims to provide a magnified protection to the data subjects in the Union.

However, in many situations a GDPR certification might not be necessary for third country controllers or processors. To understand the importance and the function of this specific tool in trans-border data transfers, it should be examined in consideration with the other means of lawful transferring of personal data to third country recipients.

2. THE ADEQUATE LEVEL OF PROTECTION

Article 44 of the GDPR regulates the general principle for third country transfers of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organization. The scope of the Article covers the personal data already processed in the EU and intended to be transferred to a

[407] Kuner, *Extraterritoriality and Regulation of international data transfers in EU data protection law*, p. 240.

third country or to an international organization. Similar to the rules for lawful processing, the transfer of the personal data outside the EU is prohibited unless the conditions laid down in Chapter V of the GDPR are complied with by the controller or processor. This general principle applies, unlike under the Directive, to the onward transfers of personal data from the third country or an international organization as well.

2.1. Adequacy Decisions: The First Safeguard to Check Before Trans-Border Data Transfers

Pursuant to Article 45(1) of the GDPR, the Commission decides whether a third country or an international organization ensures an adequate level of protection, adopting implementing acts so-called adequacy decisions, based on Article 291 TFEU. Accordingly, transfers to a third country or to an international organization may take place on the basis of these adequacy decisions and such transfers do not require any specific authorization.[408]

The adequate level of protection is assessed by the Commission with respect to the rule of law, the level of protection of human rights and fundamental freedoms in that country, comprehensiveness of data protection rules and their implementation, case-law, the ability of public authorities to reach personal data, the rules governing the trans-border data flows, effectiveness and enforceability of data subject rights and the possibility of the judicial remedies in that country for the data subjects whose personal to be transferred. Additionally, the Commission when deciding on adequacy decisions also takes into account whether the third country effectively deploys independent supervisory authorities.

The Commission also regards the international commitments the third country or the international organization has entered into, or other obligations arising from legally binding conventions or instruments, as well as from its participation in multilateral or regional systems in relation to the personal data.

[408] Art. 45(1) GDPR.

The Commission adopts implementing acts after the assessment of the adequacy level of protection of a third country or an international organization. This implementing act should provide a mechanism for a periodic review of the adequacy level at least every four years.[409] Furthermore, the Commission shall monitor the developments in third countries and organizations,[410] and if the level of protection envisaged does no longer exist, it shall repeal, amend or suspend the adequacy decision without retro-active effect.[411] Eventually, the Commission publishes the list of the third countries and international organizations that ensure or do not ensure the adequacy level of protection in the Official Journal of the European Union.

In cases the Commission published an adequacy decision concerning a country, there is no need to apply additional safeguards, such as the certification mechanism, for the data transfers from EU to that country or international organization.[412]

2.2. Appropriate Safeguards

In case there is no adequacy decision regarding the level of protection of a third country or an international organization, a controller or processor may still transfer the personal data, if appropriate safeguards, enforceable data subject rights and effective remedies are available.[413] Article 46(1), foresees three conditions under which the controller or processor can make personal data transfers even when there is no adequacy decision adopted by the Commission:

- The controller or processor shall provide appropriate safeguards

[409] Article 45(3) GDPR.

[410] Article 45(4) GDPR.

[411] Article 45(5) GDPR.

[412] "The European Commission has so far recognized **Andorra**, **Argentina**, **Canada** (commercial organisations), **Faroe Islands**, **Guernsey**, **Israel**, **Isle of Man**, **Jersey**, **New Zealand**, **Switzerland**, **Uruguay** and the **United States of America** (limited to the **Privacy Shield framework**) as providing adequate protection." **https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en**, accessed on 8 September 2018.

[413] Article 46 (1) GDPR.

- There must be enforceable data subject rights in the third country
- There must be effective remedies available for the data subjects in the third country

These three conditions must be met together. Paragraph 2 of the Article explains how the appropriate safeguards may be provided. Pursuant to this, the appropriate safeguards may, first of all, be provided by a legally binding and enforceable instruments, such as international agreements, between public authorities and bodies.

Second, binding corporate rules adopted by the Commission, [414] standard data protection clauses adopted by the Commission or by a supervisory authority and approved by the Commission, an approved code of conduct and an approved certification mechanism are enlisted as another means of providing the appropriate safeguards. These listed actions do not require any specific authorization from a supervisory authority. [415]

The appropriate safeguards can also be deemed provided if there are "*contractual clauses between the controller and processor or the recipient of the personal data in the third country or international organization*"; or if there are "*provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights*" which have been authorized by the competent supervisory authority.[416]

Certification mechanism is also mentioned in Article 42, as a demonstration of the appropriate safeguards in the context of trans-border data flows. Before discussing under what conditions, the certification mechanism must be preferred as a means of

[414] Binding corporate rules as defined in Article 4(20) GDPR, means "*personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engages in a joint economic activity*". The competent supervisory authorities are entitled to approve the binding corporate rules on a condition that they are legally binding. BCRs shall apply to every member of the group of undertakings concerned. They can be enforced by every member concerned of the group of undertakings. BCRs also apply to the employees of those undertakings, as well as they can be enforced by them. It should be reminded that the main concern of the EU data protection law is to protect the rights of the data subjects, and therefore the second function of the BCRs is clarified as they 'expressly confer enforceable rights on data subjects' concerning the processing of their personal data.

[415] Article 46 (2) GDPR.

[416] Article 46 (3) GDPR.

appropriate safeguards, the credibility of the adequacy decisions adopted by the Commission must be examined.

3. ARE ADEQUACY DECISIONS REALLY ADEQUATE? SPECIAL TRANS-BORDER DATA FLOW CASE: EU-US

From the EU standpoint, personal data protection regulations in the United States were offering an inadequate level of data protection, mainly because of the self-regulated sectoral structure in the US, existed at both federal and state level.[417] For example, in the US the data processing is permitted if no harm was caused, whereas in the EU, as a general rule, data processing is not allowed unless there is a legal basis justifying the processing .[418] Consequently, data protection laws in the EU have been way more comprehensive than the ones in the US. When this is the case, the US authorities and the Commission started to discuss to discover the most fitting solutions that would answer the disparities between data protection policies of the two legal systems.

The solution, although temporary, was Safe Harbor Principles which was also an adequacy decision (Decision 2000/520/EC) adopted by the Commission upon the negotiations with the US authorities and with the assistance of the Article 29 Working Party. Lasting 15 years, the Safe Harbor allowed both legal systems to employ their own data protection norms and jurisdictions while enabling the transfers of personal data between them. However, the Court in its *Schrems* Judgment declared the Decision 2000/520/EC invalid.

The recent history of the adequacy decisions illustrates that the arrangements for securing international data transfers are unstable. The invalidated Safe Harbor Decision is a proper example to demonstrate the potential inadequacy of the adequacy decisions adopted by the Commission. Since it is an embryonic field, businesses might also be

[417] Art. 29 WP, WP 15, p.2.

[418] Paul M Schwartz, and Daniel J. Solove. "Reconciling Personal Information in the United States and European Union." **California Law Review**, Vol.4, No.102, 2014, p. 881.

affected by these volatile arrangements between the states, regarding trans-border data transfers. In order to avoid the probable vulnerability of the personal data that are subject to trans-border transfers in such cases, respective organizations must be able to immediately respond to the challenges that may emerge due to the invalidation of such decisions; e.g. backing-up their preferred means of appropriate safeguards. The GDPR certification, for instance, can provide a back-up protection in such cases.

3.1. Schrems Case

Shrems case constitutes a demonstration of how the adequacy decisions taken with respect to a third country to which personal data being transferred may not guarantee an adequate level of personal data protection in that third country. [419]

Mr. Shrems, who had been a user of the Facebook since 2008, applied to the Irish Data Protection Commissioner in 2013, for the prohibition of the transfer of his personal data by Facebook Ireland to the Facebook's parent company, Facebook Inc. located in the US. He claimed that the US did not ensure an adequate level of protection of personal data, on the grounds that the US public authorities have been carrying out surveillance activities which were revealed by Edward Snowden with respect to the activities of the National Security Agency.

Since Facebook was self-certified under the Safe Harbor, the Commissioner decided that the Decision 2000/520 (Safe Harbor Decision) was sufficient to ensure the level of protection provided by the US authorities.

Mr. Shrems, thereupon, appealed the Commissioner's decision to the Irish High Court which later referred two questions to the ECJ within the context of the preliminary ruling procedure. The Irish court asked how to interpret Article 25(6)[420] of the Directive,

[419] Judgment of the Court (Grand Chamber) of 6 October 2015, *Maximillian Schrems v Data Protection Commissioner*, Case C-362/14, ECLI:EU:C:2015:650.

[420] Article 25 of Directive regulates the principles of the third country transfer of personal data. According to the 6th paragraph of the Article, "*the Commission may find, that a third country ensures an adequate level of protection… by*

in the light of Article 7, 8 and 47 of the Charter,[421] and whether the supervisory authority (Commissioner) in question should investigate the claim that the level of personal data protection provided in a third country was not adequate, although there is an adequacy decision on the level of protection provided in that country.

It has been found by the Court that the adequacy decisions should not prevent a supervisory authority of a Member State from investigating a claim that an EU citizen's personal data was not adequately protected when transferred to a third country on which the adequacy decision was taken. The Court, in its judgment, besides interpreting the meaning of Article 25(6) of Directive 95/46, also examined the validity of the Safe Harbor Decision adopted by the Commission.

The court noted that the Safe Harbor Principles were "*intended for use solely by US organizations receiving personal data from the European Union for those purpose of qualifying the Safe Harbor and the presumption of adequacy it creates*".[422] Therefore, the Safe Harbor Principles were not binding the US public authorities, as they were only applicable to self-certified US organizations. Besides, Safe Harbor principles might have been limited on the grounds that national security, public interest or law enforcement measures are required to be taken.[423] According to the Part B of Annex IV to the Decision, when a conflicting obligation was imposed by the US law, the organization in the US had to comply with this obligation, regardless of their self-certification status under Safe Harbor.[424]

Furthermore, in case of an occurrence of such interference with fundamental rights, there were no effective remedies envisaged in the Decision, and no other rules were mentioned that could limit such interference.[425]

---

reason of its domestic law or of the international commitments it has entered into,.. for the protection of the private lives and basic freedoms and rights of individuals".

[421] Charter of Fundamental Rights of the European Union.

[422] Annex I to Decision 2000/520, para.2; *Maximillian Schrems v Data Protection Commissioner*, Case C-362/14, ECLI:EU:C:2015:650, para. 82.

[423] *Maximillian Schrems v Data Protection Commissioner*, para. 84.

[424] *Ibid.*, para.85.

[425] *Ibid.*, para. 88-89.

Pursuant to the Commission's two Communications on the issue, it is found that the US authorities were able to access and process the personal data transferred from the EU to the US in a way that "*incompatible… with the purposes for which it was* transferred, *beyond what was strictly necessary and proportionate to the protection of national security*". Apart from that, the data subjects were deprived of any administrative or judicial remedies which would enable them to exercise their data protection rights.[426]

Safe Harbor, similar to its successor, was a self-certification mechanism. Different than the GDPR certification, though voluntary, it was not a means of demonstration of compliance with the EU data protection law. As stated by the Article 29 WP, the choice of pursuing such frameworks are totally left to the discretion of individual organizations, and therefore the problem of those organizations that do not wish to adhere to the principles continues, whereas no data protection legislation providing adequate level of protection exists in the US.[427]

3.2. Privacy Shield

Another well-known example of self-certification mechanism is the controversial EU-US Privacy Shield, which has been in operation since 2016. Similar to its predecessor, the framework has been founded on 7 principles: notice, choice, accountability for onward transfer, security, data integrity and purpose limitation, access, and recourse, enforcement and liability.[428] Clearly, the framework does not reflect the comprehensive nature of the GDPR; it is not a GDPR compliance mechanism.[429] Even though this new framework has improved the protection of the personal data compared to the protection provided under the Safe Harbor, such improvement is not considered sufficient.[430]

---

[426] *Ibid.*, para.90.

[427] Art. 29 WP, WP 15, p.2.

[428] **https://www.privacyshield.gov/EU-US-Framework**, date accessed 10 October 2018.

[429] **https://www.privacyshield.gov/article?id=General-FAQs**, date accessed 10 October 2018.

[430] Voigt and Von Dem Bussche, p.124.

Further, although the Privacy Shield ensures much more protection and enforceability than the invalidated Safe Harbor, its enforcement procedures have been found too complex and inconsistent by the Article 29 WP, being carried out by various independent dispute resolution bodies.[431]

In 2016, Digital Rights Ireland Ltd contested the Privacy Shield before the CJEU. The Court has found the application inadmissible, since the applicant did not have any interest to bring the proceedings before the Court. [432] Privacy Shield might, nevertheless, be contested again in the future due to its lack of adequate level of protection.

4. GDPR CERTİFİCATİON AS AN APPROPRİATE SAFEGUARD

International data transfers are one of the most relevant fields in which the newly introduced certification mechanism play a role,[433] because if encouraged effectively, the GDPR certification may create safe passages enabling compliant transfers of personal data between various legal frameworks.

Pursuant to Article 42(2):

"*data protection certification mechanisms, seals or marks… may be established for the purpose of demonstrating the existence of appropriate safeguards provided by controllers or processors that are not subject to this Regulation…within the framework of personal data transfers to third countries or international organizations… Such controllers and processors shall make binding and enforceable commitments, via*

[431] Art. 29 WP, WP 238, 2016, Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision (10 July 2018), p.3-4.
[432] *Digital Rights Ireland*, para. 43.

contractual or other legally binding instruments to apply those appropriate safeguards, including with regard to the rights of data subjects".

Thus, certification is a tool that ensures legal certainty when personal data is transferred outside the EU if coupled with binding and enforceable commitments of the controller or processor in the third country to implement the appropriate safeguards.

To rely on the certification mechanisms for trans-border data flows additionally requires the controller or the processor in the third country to make binding and enforceable commitments to apply the appropriate safeguards, including data subjects' rights.[434] Hence, it can be understood that the GDPR certification provides only a general legal basis for the trans-border data transfers.

Yet the GDPR certification is not the only instrument that can be used for lawful transfer of the personal data to third countries. As discussed in the previous sections, adequacy decisions adopted by the Commission, binding corporate rules, standard data protection clauses adopted by the Commission or supervisory authority and approved code of conducts coupled with binding and enforceable commitments are appropriate safeguards.

CIPL states that it is important to ensure interoperability, avoiding conflicting frameworks in the field of international frameworks.[435] In third country transfers, to rely on approved certification mechanisms might seem more preferable for some organizations established in the EU; except for the codes of conduct, there are no other appropriate safeguards that allow third country organizations to import personal data on a frequent basis from various controllers or processors in the EU. The function of codes of conduct has been changed by the GDPR with a view to facilitating trans-border data flows, however, it does not offer a visible sign demonstrating the GDPR compliance as

[434] Art 46(2)(f) GDPR.

[435] Centre for Information Policy Leadership GDPR Implementation Project (CIPL), "Certifications, Seals and Marks under the GDPR and their Roles as Accountability Tools and Cross-Border Data Transfer Mechanisms", Discussion Paper,https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_certifications_discussion_paper_12_april_2017.pdf12, 8 July 2018, p.12.

in the case of the GDPR certification. Moreover, it is not clear in the GPDR, how the third country controllers and processors will apply to such schemes, as Article 40(5) clearly states that 'the competent supervisory authorities can approve code of conducts submitted to them.

In fact, binding corporate rules can be considered as *de facto* forms of certifications,[436] except the fact that they are inherently binding. Yet they are not preferable in cases where a controller outside the EU receives personal data from various controllers and processors within the EU.[437]

Other means of appropriate safeguards that are inherently binding, such as standard data protection clauses, may be preferable in specific data transfers, meaning that the parties have to conduct a new set of standard data protection clauses for each specific type of data transfers from the EU. If a controller or processor in a third country receives data from many different data exporters within the EU, standard data protection clauses are not practical, since the standard data protection clauses are limited in their scope of application. [438]

Hence, certification mechanism in trans-border data transfers seems beneficial in the situations where there are several data exporting points in the EU.

4.1. Who will Certify the Processing Activities of Third Country Data Importers?

The GDPR emphasizes the word "*competent*" to signify that each supervisory authority has competence on the territory of its own Member State.[439] According to Article 43(1)(a) and 57(1)(q), supervisory authorities can only accredit the certification bodies in

[436] *Ibid*. p.12

[438] Tobias Kugler, p.211, para 904

[439] Article 55 (1) of GDPR

their own territory where they have competence. Similarly, each supervisory authority shall conduct a periodic review of certifications issued in its own territory where it has competence.[440] It means that the competence of supervisory authority of a Member State regarding the accreditation of certification bodies and reviewing the certifications on a periodical basis is restricted with the territorial jurisdiction of that Member State. This helps supervisory authorities to exert control over the issuers in their own territories, in order to prevent possible irregularities in the certification process.

Although it can be interpreted that the supervisory authority where the representative is located would be deemed as the competent supervisory authority, the obligation to designate a representative under Article 27 GDPR only covers the controllers and processors falling within the scope of the GDPR, under Article 3(2).[441] There is no mention in Article 27, regarding a representative to be designated by the third country controller in trans-border data transfers. Yet, it should be noted that all the personal data transfers fall within the scope of Article 3(2) because transfer of the personal data, too, means processing; the personal data becomes processed by the third country data importer, when it has been transferred. Therefore, the competent supervisory authority of the third country controllers is supposed to be the supervisory authority in the Member State where the representative is located.

The accredited certification bodies, nonetheless, seem to have the authority to issue certifications for the third country controllers and processors. This can be interpreted when reading paragraphs 2 and 5 of Article 42 together. It can even mean that the accredited certification bodies can carry out reviews on the issued certifications in third states. Though investigations in third countries are not common, a certified third state entity is supposed to adhere to the GDPR requirements as well as the principle of accountability.

4.2. Investigations Based on Certifications in Third Countries

[440] Article 57 (1)(o) of the GDPR
[441] Article 27(1) of the GDPR.

Even where they fall within the scope of the GDPR, the third country controllers and processors cannot be habitually investigated or fined by the EU authorities. Therefore, as a general rule, the controllers and processors in the EU bear the risk and they shall ensure that their data transfers have complied with the GDPR. In other words, they must also evaluate the level of the risks which might stem from the processing activities of the controller/processor in the third country, before transferring the personal data.

However, certifications can be reviewed by the supervisory authorities within the context of their investigative powers.[442] Although not common, there had been a couple of examples of these kinds of audits conducted by the EU data protection authorities in third countries: e.g. in 1996, Berlin Data Protection Commissioner conducted an on-site audit in Citibank USA upon consent by the Citibank. Spanish Data Protection Authority (DPA), also conducted an audit of a processor in Colombia based on standard contractual clauses. Apart from these, the Italian DPA has carried out an audit on Google's premises in California after receiving the consent of Google Inc.[443]

Article 58, which specifies the investigative powers of supervisory authorities, neither stipulates such powers to be used only in the territory of the Member States, nor uses the term "*competent*". This more flexible wording seems to pave the way for supervisory authorities to conduct their investigations in third countries as well. Paragraph (c) of the first section of the Article expresses that one of the investigation powers of each supervisory authorities is to "*carry out a review on certifications issued pursuant to Article 42(7)*" which states that certifications can be issued by the accredited certification bodies or by the competent supervisory authorities. Therefore, regardless of the location, supervisory authorities can review the certifications issued by the accredited certification bodies for the third country controllers. The Article, moreover, confers the capacity of withdrawing a certification, or of requiring the accredited certification body

[442] Article 85(1)(c) of the GDPR.

[443] Kuner, *Extraterritoriality and regulation of international data transfers in EU data protection law*, p.240.

to withdraw a certification or of ordering the suspension of personal data transfers to a recipient in a third country.[444]

The GDPR confers investigation powers to supervisory authorities in cases that the certification mechanism is preferred by the third country data recipients that are not in the scope of the GDPR. As stated, transfer of the personal data of the individuals in the EU to such data recipients actually makes them subject to the GDPR, even though the transfer occurs only once. The certification of the processing operations of the third country controllers and processors will be carried out by the accredited certification bodies, unless the EDPB or the Commission states otherwise in the future. Consequently, it is possible that the GPDR certifications would enable trans-border audits of certified entities in third states.

4.3. How to ensure enforceability?

Although there are many legal bases introduced by the GDPR, for personal data transfers, enforceability remains as the main concern in the field of trans-border data transfers, due to lack of harmonization in the field of data protection standards.

In general, the GDPR certification does not by itself provide enforceable rights to the data subjects, since it does not have direct legal effects. Therefore, certifications only serve as a legal basis for cross-border data transfers. Binding and enforceable commitments must be made by the third country controller or processor, in order to give the power of enforceability to the certification.

The GDPR does not explain what the "*other legally binding instruments*" are. Until the Court or the EDPB explains the meaning of the phrase used in the Article, it would be sensible to use the guidance of the Art. 29 WP on how to render BCRs binding within an organization. According to the Article 29 WP on binding corporate rules, to bind an organization with enforceable commitments, the individual architecture of that

[444] Article 58 (2)(h) and (j) of the GDPR.

organization must be regarded, in the light of the relevant laws of the Member State in which the data exporter is located.[445] In the case of certifications, the commitments can be incorporated into the general principles of an organization assisted by appropriate policies, audits, and sanctions.[446]

With regard to the US, differing from the Safe Harbor, the Privacy Shield framework introduced a binding arbitration mechanism that can be invoked, provided that all of the other complaint mechanisms have been exhausted. Although found complicated by the Art 29 WP, it is clearly more enhanced compared to the Safe Harbor Certification. Thus, US organizations that receive personal data from the EU controllers or processors are advised to self-certify their processing operations under the Privacy Shield framework, since it provides many options for the parties and for the individuals to exercise their data protection rights. Despite being costly, more inclusive option for the US organizations receiving personal data of the individuals in the EU would be a double certification under both Privacy Shield and the GDPR certification, so that they can demonstrate their compliance with the GDPR while providing enforcement and redress options for the data subjects.

The GDPR acknowledges the difficulties that may hamper the capability of individuals to exercise their data protection rights and of the supervisory authorities to pursue complaints when personal data pass beyond the borders of the EU. In this regard, close cooperation among supervisory authorities and the Commission is needed. Furthermore, Recital 116 states that the supervisory authorities shall exchange information and carry out investigations with their international counterparts based on reciprocity.[447] It seems unfeasible since there are many countries in the world which do not have specific data protection laws or data protection authorities.[448] In such cases, the Commission and supervisory authorities must take appropriate measures to develop

[445] Art. 29 WP, WP 108, 2005, **Working Document Establishing a Model Checklist Application for Approval of Binding Corporate Rules**, (11 September 2018), p.5.
[446] Kugler, p.210, para 900.
[447] Rec. 116 GDPR.
[448] Data Protection around the World, **https://www.cnil.fr/en/data-protection-around-the-world**, 10 October 2018.

international mutual assistance to enable the effective enforcement of data protection rights, engaging respective stakeholders in the discussion, pursuant to Article 50 of the GDPR. However, the fact that the data transferred to the organizations in third countries without adequate data protection, even if the appropriate safeguards are used, cannot be easily tracked remains unless the state authorities cooperate with the EU supervisory authorities.

Regardless of the certification status of the third country controller or processor, enforceability can be provided of the rights of both parties and data subjects that are affected by the transfer, through the representatives.[449] Pursuant to Article 27 GDPR, third country controllers and processors have to appoint a representative, which is a natural or legal person established in the Union. Although the appointment of a representative does not affect the responsibility of the controller or the processor under the GDPR, the appointed representative can be subject to enforcement proceedings in case of non-compliance by the third country controller or processor. Hence, accountability of the third country controllers and processors can be realized through the representatives; as they can be forced to redress the damages and to pay the fines. This also concerns the certified third state entities, since certification will also mean that they have a representative appointed in writing in the EU. Within the binding commitments made by third country controller or processor, it is also possible to embed an arbitration mechanism for dispute resolution into the agreement between the parties. Furthermore, within the powers of supervisory authorities, data flows to the recipient can be suspended in case of breach, though it is unclear how to do so.[450]

However, in cases that the controller or processor do not process personal data on a large scale, or do not to process sensitive data, there is no obligation of the designation of a representative. In such cases, transfers are still supposed to be subject to the safeguards; the question of who to hold accountable still remains since the third countries can be immune to be held accountable if they do not provide adequate protection

[449] Art. 27 of the GDPR.
[450] Art. 58(2)(j) of the GDPR

or if they reject to cooperate, although the third country data recipient is certified under the GDPR. In such cases, the withdrawal of the certification can be a way of demonstrating that the controller in breach is no longer trustable.

5. CONCLUSION

The GDPR certification is accepted by the EU legislator as a means of appropriate safeguards, provided that it is accompanied with binding and enforceable commitments. In the light of the facts mentioned hereinabove, the GDPR certification is advised where the third country data importer receives personal data from various sources from the EU. It is obvious that there will be no common acceptance of only one single means of appropriate safeguards, since each organization is expected to find the best suitable tool to count on when transferring personal data outside the EU, corresponding its individual needs.

Even though Privacy Shield, offering easier criteria, seems even more preferable for the organizations in the US, the GDPR certification might still be used as an interoperable tool with the other transfer mechanisms such as the Privacy Shield certification in the US. Still, the Court may invalidate the Privacy Shield any time after the GDPR certification becomes commonly recognized in the market.

As seen in the previous Chapters of the thesis, to ensure accountability, we need sanctions and redress mechanisms. In respect to trans-border data flows, the GDPR certification cannot function as an accountability tool, since it only provides an indication regarding the GDPR compliance of the certified third country controllers. It can only provide guarantees to the data subjects if it is coupled with binding enforceable instruments.

The GDPR certifications can pave the way for investigations in the certified third country controllers. However, the main problem remains here with the non-certified ones who do not want to comply with the GDPR standards.

The EDBP mentions that other guidelines will be published on the criteria to approve certification mechanisms as transfer tools to third countries. Hopefully, many questions that have been raised here would be addressed by those guidelines soon. Also, the decisions of supervisory authorities and certification bodies on the issue will clarify the level of efficiency of the GDPR certification mechanism in trans-border data flows.

CONCLUSION

Data protection certifications are one of the recognized accountability tools in personal data protection. Despite being highly recognized in the field, according to the studies, they do not function as intended, on the contrary, they have generated many problems threatening the personal data protection. As indicated in Chapter 2, the problems consist of asymmetry of information, weak guarantees, the lack of organizational resources, non-functional complaint, and enforcement mechanisms, and the lack of competition between controllers in becoming compliant.

The introduction of the GDPR certification is seen revolutionary, since for the first time in the EU history, that certifications have been fully regulated under a legally binding framework. Although this development appears to be considered positive, the effectiveness of the mechanism, particularly with regard to its ability to promote accountability, should be questioned in multiple aspects. Since accountability refers to an umbrella term encompassing other intended objectives of the GDPR certification, the effectiveness of the mechanism can be measured by the extent to which accountability is provided. Therefore, the thesis seeks to answer whether and to what extent the GDPR certification mechanism can promote the intended accountability in personal data protection.

Chapter 3 unpacks the concept of accountability within the context of data protection certifications and concludes that a data certification scheme can function as an

accountability promoter only if it meets certain conditions. The first condition has been identified as transparency that is needed for assessing the account given. Subsequently, three important aspects that improve the accountability in DPCs have been established as the co-regulatory approach, the combination of soft and hard law (voluntary binding participation) and enforcement mechanisms. Third, it has been stated that the criteria of the DPC must be strong as much as to enable proper evaluation.

Transparent processing requires that any information concerning the personal data processed shall be easily accessible and understandable by data subjects.[451] It appears to be a good indicator of accountability that transparency is regulated as the guiding principle of the GDPR. However, the meaning of fair processing is not explained in the Regulation. In complex personal data processes that are automatedly evaluating personal aspects of individuals and making decisions, which may produce legal effects on individuals, fairness might be very difficult to evaluate. Considering that many decisions concerning personal data are currently taken by automated systems, there might be many biased decisions made by the algorithms. In fact, biased AI decisions are already problematic. To prevent biased decisions taken by automated systems, the algorithms governing them should be transparently explained to the public. Unless the algorithms of automated personal data processing systems are evaluated by the experts, it seems impossible for many individuals to comprehend the level of fairness of automated-decisions. When they cannot understand the decision-making process, the processing is not deemed transparent either. The GDPR certification can be the assurance of the fairness of the processing since the conformity assessment will be conducted by the experts. If these ambiguities remain, transparency would become neglected from the beginning and the rest of the certification process cannot ensure transparency and therefore accountability. In that case, the illusion of privacy and the asymmetry of information in the DPC market cannot be eliminated.

The fact that the GDPR and the EDPB emphasize the significance of transparent procedures supported with proper documentation signals that the transparency of the

[451] Recital 39 GDPR.

process will be of utmost importance. However, regarding surveillance of certification, the same outcome may not be expected as there is no mention of on-spot audits of the certified entities. This can directly impact the effectiveness of the mechanism since the information received out of the audits conducted merely on the documentation might not accurately reveal the real practices of the organizations. The possibility of function creep seems to be another issue to be tackled. To prevent this possibility, evaluation and decision phases must be entirely separated into two distinct stages to be conducted by two different expert groups. Last but not least, as regards transparency that has been established as the first prerequisite for accountability, it should be appreciated that the GDPR conditions the certification bodies to have transparent complaint mechanisms.

The voluntary binding approach in data protection is seen as the most effective approach to promote data protection accountability.[452] In Chapter 3, I applied this view to the DPCs and decided that the best environment for the DPCs to operate is, too, the combination of the approaches because of its proven benefits that might eliminate the problems in the market. The accreditation in Article 43 reflects an atypical co-regulated arrangement accompanied by a soft law approach, embedded in a Regulation directly applicable in all of the Member States. Therefore, the GDPR seems to have the appropriate approach for the certification mechanism to become effective as an accountability tool since while it creates hard law impact, it also provides the flexibility required in data protection law. Laying down the sufficient expertise in relation to the ToE of the certification of accredited certification bodies as a condition is perceived as a positive development for a co-regulatory approach to be effective.[453] Moreover, co-operation in accreditation and reviewing is welcomed as it increases independent and unbiased practices in certification.[454] I strongly believe that the approach can, in long run, foster the intended competition between the data controllers.

[452] Raban, *Privacy Accountability Model and Policy for Security Organizations*, p.170.
[453] Article 43(2)(a) of the GDPR.
[454] R Rodrigues, Wright and Wadhwa, p.114.

The GDPR has linked the enforcement mechanisms to DPCs, and remedies accompanied by high fines in case of breaches. Follow-on audits and complaint mechanisms constitute the first step of proper enforcement. Under these circumstances, a breach of a certification agreement can also mean a breach of the GDPR and many sanctions, in addition to revocation of the certification, can be implemented at the same time. Under the GDPR, not only investigative powers of supervisory authorities have been expanded, but also the sanctions have been noticeably increased up to EUR 20,000,000.00 or 4% of the total annual worldwide turnover. Considering that the certified entities will enjoy mitigated fines under Article 83(j), it can be estimated that the large companies are likely to obtain a GDPR certification to demonstrate their compliance. Furthermore, the data subjects, who have been granted many options under the GDPR, can also challenge the certification status of the entities by lodging complaints.

The GDPR criteria should be very comprehensive; it should cover the general principles of personal data processing (Article 5), legal grounds for processing (Article 6) and the data subjects rights. The risk-assessment is the most complicated part of the data protection both for the controllers and for the experts during conformity assessments. It is very important that the DPIA is conducted considering the principle of proportionality and the balance test. When balancing the legitimate interest of the controller and the impact of the processing on the fundamental rights and freedoms of the data subject, additional safeguards should be applied. Additional safeguards are not clearly identified, and this can make problems in relation to accountability since it is not clear how to incorporate them in certification criteria. Apart from the risk-based approach, some other points with regard to criteria can be revisited here. First, as stated hereinabove, the ambiguities regarding the concepts of transparency and fairness in automated decisions may create issues in conformity assessments. Second, an approved certification mechanism, according to Article 25 of the GDPR, is acknowledged as an element demonstrating compliance with the requirement of data protection by design and by default. Perceptibly, the requirement, which means that controllers or processors must be aware of their accountability, even before designing a system intending to process personal data, constitutes an overarching obligation for data controllers. However, this recommendation does not give any clue on the effectiveness of the certification

mechanism, since how the principle was reflected in the criteria and how accurate is the conformity assessment may affect the envisioned accountability.

The GDPR recognizes a step-by-step approach to the harmonization with regard to the certification criteria. The last step of the harmonization is envisaged as *"the seal"*. The completion of a harmonizing may eliminate the reasonable concerns, of the authors, regarding the potential multivocality of the several criteria existing simultaneously in the market.

In the context of third country transfers, the GDPR certifications alone cannot ensure the enforcement of the rights and claims, since it does not inherently provide direct legal effects. However, the legislator conditioning the adherence of enforceable instruments in trans-border data flows offers a variety of options in order to hold third country controllers and processors accountable. Although having a certification does not produce any direct legal effects, non-compliance to certification schemes may bring serious results such as revocation of the certification and the termination of certification agreements. Plus, certification agreements may facilitate the future investigations in third countries.

Consequently, there is no one answer to the main research question: there are plenty of possibilities dependent on to what extent the prerequisites, established in Chapter 3, would be met by the certification mechanism.

BIBLIOGRAPHY

BOOKS

Alhadeff, Joseph; Van Alsenoy Brendan; Dumortier Jos. "The Accountability Principle in Data Protection Regulation: Origin, Development and Future Directions". Guagnin Daniel and Hempel Leon (Ed.). in **Managing Privacy through Accountability.** London: Palgrave Macmillan, 2012, (49-82).

Balboni, Paolo and Dragan, Theodora. "Controversies and Challenges of Trustmarks: Lessons for Privacy and Data Protection Seals", Rowena Rodrigues and Vagelis Papakonstantinou (Ed.). in **Privacy and Data Protection Seals**. The Hague: TMC Asser Press, 2018, (83-111).

Barnard-Wills, Davis. "The Potential for Privacy Seals in Emerging Technologies", Rowena Rodrigues and Vagelis Papakonstantinou (Ed.). in **Privacy and Data Protection Seals**. The Hague: TMC Asser Press, 2018, (113-132).

Balleisen, Edward J. and Eisner, Marc. "The Promise and Pitfalls of Co-regulation: How Governments can Draw on Private Governance for Public Purpose" in **New Perspectives on Regulation**. David Moss and John Cisternino (Ed.). 1st Edition, Cambridge: The Tobin Project, 2009, (127-150).

Carvais-Palut, Johanna. "The French Privacy Seal Scheme: A Successful Test", Rowena Rodrigues and Vagelis Papakonstantinou (Ed.). in **Privacy and Data Protection Seals**. The Hague: TMC Asser Press, 2018, (49-58).

Chibba, Michelle and Cavoukian Ann. "Privacy Seals in the USA, Europe, Japan, Canada, India and Australia", Rowena Rodrigues and Vagelis Papakonstantinou (Ed.). in **Privacy and Data Protection Seals**. The Hague: TMC Asser Press, 2018, (59-82).

Council of Europe. **Handbook on European Data Protection Law**. Luxembourg: Publications Office of the European Union. 2014.

Craig, Paul and De Búrca. Grainne, **EU Law: Texts, Cases and Materials**, 6th Edition, Oxford: Oxford University Press, 2015.

De Hert, Paul. "The Accountability Principle in Data Protection Regulation: Origin, Development and Future Directions". Guagnin Daniel and Hempel Leon (Ed.). in **Managing Privacy through Accountability.** London: Palgrave Macmillan, 2012, (193-233).

Dienst, Sebastian. "Lawful Processing of Personal Data in Companies", Daniel Rucker and Tobias Kugler (Ed.). in **New European General Data Protection Regulation, A Practitioner's Guide Ensuring Compliant Corporate Practice**. Munich: C.H. Beck, Nomos, Hart Publishing, 2018, (49-105).

Fuster, Gloria González. **The Emergence of Personal Data Protection as a Fundamental Right of the EU**, 1st Edition, Dordrecht Heidelberg New York London: Springer Science & Business, 2014.
Hansen, Marit. "The Schleswig-Holstein Data Protection Seal", Rowena Rodrigues and Vagelis Papakonstantinou (Ed.). in **Privacy and Data Protection Seals**. The Hague: TMC Asser Press, 2018, (35-48).

Kamara, Irene and De Hert, Paul. "Data Protection Certification in the EU: Possibilities, Actors and Building Blocks in a Reformed Landscape. In **Privacy and Data Protection Seals**. The Hague: TMC Asser Press, 2018, (7-34).

Kosta, Eleni. **Consent in European Data Protection Law**. 3rd Edition. Boston: Martinus Nijhoff Publishers, 2013.

Kugler, Tobias. "Practical Examples (1st Part)", Daniel Rucker and Tobias Kugler (Ed.). in **New European General Data Protection Regulation, A Practitioner's Guide Ensuring Compliant Corporate Practice**. Munich: C.H. Beck, Nomos, Hart Publishing, 2018, (195-243)

Lynskey, Orla. **The Foundations of EU Data Protection Law. 1st Edition.** Oxford: Oxford University Press, 2015.

Mario Viola de Azevedo Cunha. **Market Integration Through Data Protection: An Analysis of the Insurance and Financial Industries in the EU**. 1st Edition. Dordrecht Heidelberg New York London: Springer Science & Business, 2013.

Papakonstantinou, Vagelis. "Introduction: Privacy and Data Protection Seals" in **Privacy and Data Protection Seals**. The Hague: TMC Asser Press, 2018, (1-6).

Raab, Charles. "The Meaning of 'Accountability' in the Information Privacy Context". Guagnin Daniel and Hempel Leon (Ed), in **Managing Privacy through Accountability.** London: Palgrave Macmillan, 2012, (15-31).

Rodrigues, Rowena. "Conclusion: What Next for Privacy Seals?", Rowena Rodrigues and Vagelis Papakonstantinou (Ed.). in **Privacy and Data Protection Seals**. The Hague: TMC Asser Press, 2018, (149-155).

Rodrigues, Rowena and Papakonstantinou, Vagelis (Ed.). **Privacy and Data Protection Seals**. The Hague: TMC Asser Press, 2018.

Rucker, Daniel and Kugler Tobias. **New European General Data Protection Regulation A Practitioner's Guide Ensuring Compliant Corporate Practice**. 1st Edition. Munich: C.H. Beck, Nomos, Hart Publishing, 2018.

Rudgard, Sian. "Origins and Historical Context of Data Protection Law.", Eduardo Ustaran (Ed.). in **European Privacy. Law and Practice for Data Protection**

Professionals, Portsmouth: International Association of Privacy Professionals (IAPP), 2012, (3-17).

Schrey, Joachim. "Data Privacy in Private Companies", Daniel Rucker and Tobias Kugler (Ed.). in **New European General Data Protection Regulation, A Practitioner's Guide Ensuring Compliant Corporate Practice**. Munich: C.H. Beck, Nomos, Hart Publishing, 2018, (105-193).

Voigt, Paul and von dem Bussche, Axel. **The EU General Data Protection Regulation (GDPR) A Practical Guide.** 1st Edition. Cham: Springer, 2017.

Waelbroeck, Patrick. "An Economic Analyses of Privacy Seals", Rowena Rodrigues and Vagelis Papakonstantinou (Ed.). in **Privacy and Data Protection Seals**. The Hague: TMC Asser Press, 2018, (133-147).

ARTICLES

Bignami, Francesca. "The Case for Tolerant Constitutional Patriotism: The Right to Privacy before the European Courts". **Cornell International Law Journal**. Vol.41, No.8, 2008.

Bignami, Francesca. "Cooperative Legalism and the Non-Americanization of European Regulatory Styles: The Case of Data Privacy". **American Journal of Comparative Law**. Vol.59, No.2, 411–461, 2011.

Bonatti, Piero; Kirrane, Sabrina; Polleres Axel and Wenning Rigo "Transparent Personal Data Processing: The Road Ahead.". **International Conference on Computer Safety, Reliability, and Security.** Cham**:** Springer, 12 September 2017, (337-349), **https://www.specialprivacy.eu/images/documents/TELERISE17.pdf**, (last accessed 10 June 2018).

Bovens, Mark. "Analysing and assessing accountability: a conceptual framework". **European Law Journal**. Vol.13, No.4, (447–68), 2007

Bovens, Mark. "Two Concepts of Accountability: Accountability as a Virtue and as a Mechanism". **West European Politics**. Vol. 33, No. 5, 946–967, September 2010.

Butarelli, Giovanni. "The EU as a Clarion Call for a New Global Digital Standard". **International Data Privacy Law.** Vol.6, No.2, 2016.

Cavoukian, Ann. Privacy by Design. The 7 Foundational Principals. 2011 **https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf**, (last access 7 August 2018).

Centre for Information Policy Leadership GDPR Implementation Project (CIPL). Discussion Paper. "**Certifications, Seals and Marks under the GDPR and their Roles as Accountability Tools and Cross-Border Data Transfer Mechanisms**". 2017.https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_certifications_discussion_paper_12_april_2017.pdf12 (last access 8 July 2018).

De Simone, Christian. "Pitting Karlsruhe Against Luxembourg? German Data Protection and the Contested Implementation of the EU Data Retention Directive". **German Law Journal**. Vol. 11, No: 3, 291-317, 2010.

Fox, Jonathan. "The uncertain relationship between transparency and accountability." *Development in practice* Vol.17, No. 4-5, 663-671, 2007.

Gavison, Ruth E. "Privacy and the Limits of Law". **The Yale Law Journal**. Vol. 89, No. 3, 421-471. (May 2012).

Hood, Christopher. "Accountability and transparency: Siamese twins, matching parts, awkward couple?". **West European Politics**. Vol.33, No.5, 989-1009. 2010.

Kuner, Christopher. "Regulation of Trans border Data Flows under Data Protection and Privacy Law: Past, Present and Future". **OECD Digital Economy Papers**. No. 187, 2011. **http://dx.doi.org/10.1787/5kg0s2fk315f-en** (last accessed 2 June 2018).

Kuner, Christopher. "Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law". **International Data Privacy Law**. Vol.5, No.4., 235-245, 2015.

Kuzeci, Elif. **"**İstatistikî Birimler ve Bilgilerin Geleceğini Belirleme Hakkı**".** ***İnsan Hakları Yıllığı,*** Vol. 32, 2014**,** (53-75).

https://www.academia.edu/37176330/%C4%B0statistik%C3%AE_Birimler_ve_Bilgilerin_Gelece%C4%9Fini_Belirleme_Hakk%C4%B1_Statistical_Units_and_Right_to_Informational_Self-Determination, (last accessed 11 October 2018).

Lachaud, Eric. "Why the Certification Process Defined in the General Data Protection Regulation cannot be Successful". **Computer Law & Security Review.** Vol.*32*, No.6, (814-826), 2016.

Lachaud, Eric. "The General Data Protection Regulation and the Rise of Certification as a Regulatory Instrument". **Computer Law & Security Review**. The

International Journal of Technology Law and Practice. September 2017. doi:10.1016/j.clsr.2017.09.002.

Maldoff, Gabriel. "The Risk-Based Approach in the GDPR: Interpretation and Implications", https://iapp.org/resources/article/the-risk-based-approach-in-the-gdpr-interpretation-and-implications/ (last access 10 October 2018).

Martinez, Garcia Marian; Verbruggen, Paul; Fearne Andrew. "Risk-based approaches to food safety regulation: what role for co-regulation?". **Journal of Risk Research.** Vol.16, No.9. 2013.

Pearson, Siani; Wainwright, Nick. "An interdisciplinary approach to accountability for future internet service provision". **Int. J. Trust Management in Computing and Communications**. *Vol. 1, No. 1, 2013.*

Periñán, Bernardo. "The Origin of Privacy as a Legal Value: A Reflection on Roman and English Law". **American Journal of Legal History.** Vol.52, No.2., 183–201, 2012.

Senden, Linda. "Soft Law, Self-regulation and Co-regulation in European Law: Where Do They Meet?". **Electronic Journal of Comparative Law**. Vol.1, No.2., 1-27, January 2005.

Schwartz, Paul M. and Solove, Daniel J. "Reconciling Personal Information in the United States and European Union". **California Law Review**. Vol.4, No.102, 2014.

Raab, Charles. "Information Privacy: Ethics and Accountability". September 2016, at *SSRN: https://ssrn.com/abstract=3057469 or http://dx.doi.org/10.2139/ssrn.3057469* (last access 1 November 2018).

Raban, Yoel. "Privacy Accountability Model and Policy for Security Organizations". **IBusiness.** Vol.4., No.2, 2012.

Rodrigues, Rowena et al., "The Future of Privacy Certification in Europe: An Exploration of Options under Article 42 of the GDPR". **International Review of Law, Computers & Technology**. Vol.30, No.3, 248-270, DOI: 10.1080/13600869.2016.1189737 , 2016.

Rodrigues, Rowena and Wright, David. "Developing a Privacy Seal Scheme (that works)". **International Data Privacy Law**. Vol. 3, No. 2 , 2013.

Tranberg, Charlotte Bagger. “Proportionality and Data Protection in the Case Law of the European Court of Justice”. **International Data Privacy Law**. Vol.1, No.4, 239–248, 2011.

Trubek, David M. and Cottrell, M. Patrick and Nance, Mark. “'Soft Law,' 'Hard Law,' and European Integration: Toward a Theory of Hybridity”. **U of Wisconsin Legal Studies Research Paper** No. 1002. November 2005. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=855447. (last access 10 December 2018).

Weber, Rolf H. “Transborder Data Transfers: Concepts, Regulatory Approaches and New Legislative Initiatives”. **International Data Privacy Law.** Vol.*3*, *No.*2, (117-130), 2013.

Zimmermann, Christian. **A Categorization of Transparency-Enhancing Technologies**. https://arxiv.org/pdf/1507.04914.pdf, (last access 1 October 2018).

REPORTS

Bartle, Ian and Vass, Peter. Self-Regulation and the Regulatory State-A Survey of Policy and Practice” Research Report 17. Centre for Study of Regulated Industries, University of Bath, 2005.

Rodrigues et al. “EU Privacy Seal Project”. **Inventory and Analysis of Privacy Certification Schemes**. Final Report Study Deliverable 1.4. Luxembourg: Publications Office of the European Union, 2013.

The House of Lords EU Committee. **Report on Online Platforms and the Digital Single Market**. Select Committee on European Union. 2016.

LEGISLATIONS

Charter of Fundamental Rights of the European Union, 26 October 2012.

Landesdatenschutzgesetz Schleswig-Holsteinisches Gesetz zum Schutz Personenbezogener Informationen, (GVOBl. Schl.-H. S. 169), 9 February 2000 http://www.dsb.m.itkcms.de/dokumente/160/151010084146Schleswig-Holstein.pdf, (last access 10 July 2018).

European Parliament. European Parliament Resolution on the Impact of Advertising on Consumer Behavior. **2010/2052(INI)**, 15 December 2010.

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).

European Commission. Communication 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, COM 609 final, Brussels, 4 November 2010.

European Commission. Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee of the Regions, A European Consumer Agenda - Boosting confidence and growth SWD 132 final Brussels. 2012.

Council of the European Union, A Comprehensive Approach on Personal Data Protection in the European Union, Council Conclusions on the Communication to the European Parliament and the Council Brussels, 2011.

GUIDELINES/ OPINIONS / RECOMENDATIONS

Art 29 WP. WP 15. 1999. Opinion 1/99 concerning the level of data protection in the United States and the ongoing discussions between the European Commission and the United States Government, (last access 11 September 2018).

Art 29 WP. WP 108. 2005. Working Document Establishing a Model Checklist Application for Approval of Binding Corporate Rules, (Last access 11 September 2018).

Art 29 WP. WP 169. 2010 Opinion 1/2010 on the concepts of controller and processor.

Art 29 WP. WP 173. 2010 Opinion 3/2010 on the principle of accountability (last access 24 August 2018).

Art 29 WP. WP 203. 2013. Opinion 03/2013 on purpose limitation (last access 9 September 2018).

Art 29 WP. WP 217. 2014. **Opinion 06/2014 on the "Notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC"**(last access 22 August 2018).

Art 29 WP. WP 238. 2016. Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision, (last access 10 July 2018).

Art 29 WP. WP 259. 2018. Guidelines on Consent under Regulation 2016/679.

Bitkom views on EDPB Certification Guidelines under Regulation 2016/679 **https://www.bitkom.org/noindex/Publikationen/2018/Positionspapiere/Bitkom-views-on-EDPB-Certification-Guidelines-under-Regulation-2016679/20180711-Bitkom-Position-Paper-on-the-EDPB-Guidelines-on-Certification.pdf**, (last access10 July 2018).

Council of Europe. The Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD Guidelines). Preface, Part 1.

European Commission. Commission Staff Working Paper Impact Assessment. Brussels. 21 January 2012.

European Data Protection Board (EDPB). Guidelines 1/2018 on Certification and Identifying Certification Criteria in Accordance with Articles 42 and 43 of the Regulation 2016/679. 25 May 2018.

European Union Agency for Network and Information Security (ENISA). **Recommendations on European Data Protection Certification**. 2017. **https://www.enisa.europa.eu/publications/recommendations-on-european-data-protection-certification**. (last access: 11 July 2018).

Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament. the Council, the Economic and Social Committee and the Committee of the Regions**.** OJ C 181/01. 22.06.2011

CASES and DECISIONS

Federal Trade Commission, *FTC v Toysmart.com, LLC, and Toysmart.com, Inc.*, District of Massachusetts, Civil Action No.00-11341- RGS, **https://www.ftc.gov/enforcement/cases-proceedings/x000075/toysmartcom-llc-toysmartcom-inc**, (last access 10 July 2018).

Information Commissioner's Office (ICO), Monetary Penalty Notice, 24 October 2018, **https://ico.org.uk/media/action-weve-taken/mpns/2260051/r-facebook-mpn-20181024.pdf**, (last access 1 November 2018).

Judgment of the Court of 6 November 2003, *Linqvist*, C-101/0, EU:C:2003:596

Judgement of the Court of 20 May 2003. *Österreichischer Rundfunk*, joined Cases C-465/00, C-138/01 and C-139/01 EU:C:2003:294.

Judgment of the Court (Grand Chamber) of 16 December 2008, *Satakunnan Markkinapörssi and Satamedia* Case C-73/07, EU:C:2008:727.

Judgment of the Court (Grand Chamber) of 6 October 2015, *Maximillian Schrems v Data Protection Commissioner*, Case C-362/14, EU:C:2015:650.

Judgment of the Court (Grand Chamber) 8 April 2014, *Digital Rights Ireland*, C-293/12, EU:C:2014:238.

Judgment of the Court of 19 October 2016, *Breyer*, C-582/14, EU:C:2016:779.

Judgment of the Court (Fourth Chamber), 11 December 2014, *František Ryneš v Úřad pro ochranu osobních údajů,* C-212/13**,** EU:C:2014:2428.

Judgment of the Court (Third Chamber), 30 May 2013, *Worten*, C-342/12, EU:C:2013:355

Judgment of the Court (Third Chamber) of 24 November 2011, *Scarlet*, C-70/10, EU:C:2011:771.

Judgment of the Court (Fourth Chamber), 17 October 2013, *Michael Schwarz v Stadt Bochum*, C-291/12, EU:C:2013:670.

Judgment of the Court (Third Chamber) of 1 October 2015, *Smaranda Bara and Others v Casa Naţională de Asigurări de Sănătate and Others*, *C*-201/14, EU:C:2015:638.

Judgment of the General Court (Eighth Chamber) of 7 July 2011, *Gregorio Valero Jordana v European Commission,* T-161/04, EU: T:2011:337

Judgment of the Court (Grand Chamber), 13 May 2014, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González,* C-131/12, EU:C:2014:317.

STANDARDS/ CRITERIA

Common Criteria for Information Technology Security Evaluation, Part 1, **https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf**, p.34, (last access 8 July 2018).

EuroPrise Criteria Part 1, **https://www.european-privacy-seal.eu/EPS-en/Criteria** (last access 10 July 2018).

ISO/IEC 17067: 2013 Conformity assessment. *Fundamentals of product certification and guidelines for product certification schemes,* https://www.iso.org/standard/55087.html (last access 7 July 2018).

ISO/IEC 17000 : 2004, Conformity assessment — Vocabulary and general principles, **https://www.iso.org/obp/ui/#iso:std:iso-iec:17000:ed-1:v1:en.** (last access 7 July 2018).

WEBSITES and E-Documents

Complaint and Demand for Jury Trial Cambridge Analytica **https://www.cookcountystatesattorney.org/sites/default/files/files/documents/cook_county_sao-facebook_cambridge_analytica_complaint.pdf**, (last access10 October 2018).

Data Protection around the World, **https://www.cnil.fr/en/data-protection-around-the-world,** (last access 10 October 2018).

Edelman, Ben. Certifications and Site Trustworthiness. http://www.benedelman.org/news-092506/**, (last access 10 October 2018).**

European Commission. What is personal data ? **https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en** (last accessed 3 May 2018).

EuroPrise Criteria Part 1, **https://www.european-privacy-seal.eu/EPS-en/Criteria** (last access 10 July 2018).

https://cloudsecurityalliance.org/star/#_overview , (last access 14 July 2018).

https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en

https://www.esrb.org/privacy/, (last access 14 July 2018).

https://www.eprivacy.eu/en/privacy-seals/eprivacyseal/, (last access 14 July 2018).

https://www.merriam-webster.com/dictionary/accountability,(last access10 September 2018).

https://www.privacyshield.gov/EU-US-Framework, (last access 10 October 2018).

https://www.privacyshield.gov/article?id=General-FAQs, (last access 10 October 2018).

https://privacymark.org/, (last access 14 July 2018).

https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazonscraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G, (last access 10 January 2019)

https://www.trustarc.com/products/implement/ (last access 14 July 2018).

Privacy International. "Response to the European Commission's Consultation on Privacy". 2011.https://privacyinternational.org/sites/default/files/2017-12/Privacy_International_Commission_Consultation_on_Privacy_final.pdf, (last access 4 august 2018).

Korff, Douwe. Warning : the EU Council is trying to undermine privacy seals http://eulawanalysis.blogspot.com/2014/10/warning-eu-council-is-trying-to.html, **(last access** 2 September 2018).

PRESENTATIONS

Wojtowicz, Monika. The Idea of Data Protection Seals in Germany An Overwiev, https://dzlp.mk/sites/default/files/u4/Agenda_52179_1.pdf , 2014, Tuvit.