The purpose limitation principle in the General Data Protection Regulation

Juan Carlos Cersosimo

Student Number	2011987
Supervisor	Hosna Sheikhattar LLM
Second Reader	Dr Nadezhda Purtova
Place and Date	Tilburg, 2018

Table of Contents

Introduction

Problem Statement:

Reviewing the balance of my credit card a few years ago I figured out that for more than a year I paid to my bank an insurance policy for unemployment. This made no sense, since I have never been an employee but an independent legal service provider. After the proper consultation at the bank regarding this matter, I realized that for the renewal of my credit card a year before that, the bank sent to me several documents expressly indicating to sign them all in order to be able to receive the new card. To my surprise among such documentation there was an "acceptance document" for an unemployment insurance that the bank included as an additional offer of services.

These types of situations are the ones that the purpose limitation principle is intended to avoid. The personal data provided to the bank in the case indicated above was limited by the specific and legitimate purposes of processing such personal data for credit/financial purposes, not to offer an insurance policy for unemployment or other services which were not compatible with the original processing purpose.

The purpose limitation principle has been one of the most important principles covered by previous data protection regulation in Europe, such as the DPD[1]. This principle guarantees the data subject that the use and purpose of processing his/her personal data are the ones that were specifically previously specified and informed by the controller to the data subject, before starting with the processing of data.[2] Additionally, this principle provides to the data subject a clear limitation on the further processing of such personal data, since the purpose of any further processing cannot be incompatible with the initial purposes[3].

[1] Directive 95/46/EC of the European Parliament and of the Council of 24TH October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; also referred to as the "DPD"

[2] Article 29 Data Protection Working Party 00569/13/EN WP 203, Opinion 03/2013 on purpose limitation adopted on 2 April 2013; p 9, 12; and Recital 60 of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27TH 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), also referred to as the "GDPR"

[3] Art 6 (1) (b) of the DPD; and Art 5 (1) (b) of the GDPR

In a world where access to information and particularly access to personal data has acquired a value, that at the same time has become a business or at least an important part of it[4], current data protection regulations must provide data subjects with the tools to control in an effective way the use of their personal data. This principle seems to be crucial for the data protection system[5] and particularly for the purposes of restoring the balance of power regarding personal data control between the data controller and the data subject[6].

Due to the nature of the relationship between data subject and controller, the controller is on a privileged position regarding the control of such data subject's personal data. Once a subject's data has been collected, it is consequently under the control of the data controller. This is supported by the fact that the controller has been allowed to process such subject's personal data and to use it as allowed by law. At the same time, this transfer of personal data remarks the need for the data subjects to have the correct instruments in order to limit and control the use of his/her personal data by such data controller. In order to reestablish this imbalance on the personal data control, the purpose limitation principle can be considered as an important instrument for the data subject to limit, control and have some certainty regarding the processing purpose and use of his/her personal data.

Personal data protection has changed and evolved through time in order to protect and develop new rights and principles. These new rights and principles have been created in order to cover gaps or lack of precision of previous personal data protection regulations in EU[7]. Some of these

[4] Asunción E, "The Business of Personal Data: Google, Facebook, and Privacy Issues in the Eu and the Usa." (2017) International Data Privacy Law 7 (1); p 36–47.

[5] Article 29 Data Protection Working Party (n 2) 38. The Opinion indicates regarding the relevance of the purpose limitation principle that *"The concept of purpose limitation plays a crucial role in the application of the Directive. It is an essential first step in applying data protection laws since it constitutes a pre-requisite for other data quality requirements including the adequacy, relevance, proportionality and accuracy of the data collected, along with the rules surrounding data retention periods…"*

[6] Ibid; 5. Article 29 Data Protection Working Party indicates in such opinion that *"The principle of purpose limitation is designed to offer a balanced approach: an approach that aims to reconcile the need for predictability and legal certainty regarding the purposes of the processing on one hand, and the pragmatic need for some flexibility on the other…"*

[7] As an example of the indicated, Article 5 (2) of the GDPR creates the "principle of accountability"; Article 13 (2) (b) of the GDPR creates the "right to data portability". Both of them are new elements covered by the GDPR which were missing in the DPD.

elements incorporated to the General Data Protection Regulation (hereinafter "GDPR")[8] may also be considered a response to the current or upcoming threats of new technologies and business practices[9] that require a different approach from the data protection system and the data protection authorities.[10]

New principles and rights covered by the GDPR, for instance the "principle of accountability"[11], the "right to data portability"[12] or the restrictions and limitations imposed to profiling[13], have been developed in order to ensure a more elaborated and balanced data protection system.

Under such scenario of a new data protection regulation, introducing new rights, procedures and principles within the data protection system it is important to determine which is the functionality and relevance of the purpose limitation principle under this new legal framework and changes brought by the GDPR.

For instance, the GDPR compared to the DPD establishes a data protection system providing several major powers and duties to the controller,[14] which requires the controller's decision making and in some cases its sole discretion.

---

[8] 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)

[9] Recital 58 of the GDPR states an example of such concern regarding new technologies or activities, when indicating regarding the principle of transparency *"…This is of particular relevance in situations where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him or her are being collected, such as in the case of online advertising…".* See also Recital 71 of the GDPR regarding the specific concerns raised regarding the automated processing of personal data including profiling, providing as examples of possible threats carried by such practice the *"automatic refusal of an online credit application or e-recruiting practices without any human intervention";* Additionally Recital 89 points out some concern regarding the use of new technologies in personal data processing.

[10] Article 57 (1) (i) of the GDPR states the following task for the supervisory authorities *"monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies and commercial practices*". This task is new, since it was not expressly covered by the DPD.

[11] Ibid; Article 5 (2)

[12] Ibid; Article 13 (2) (b)

[13] Ibid; Article 4 (4) and 22. See also Recitals 24, 63,70,71,72, and 91

[14] Some examples of such powers and duties granted to the controller in the GDPR are the following: (i) the lawful processing based on the legitimate interests of the controller (Article 6 (1) (f) and Recital 47 and 69); (ii) the powers to ascertain whether a purpose of further processing is compatible with the original purpose for processing (Article 6 (4) and Recital 50); (iii) the obligation to communicate a personal data breach to a data subject and to the supervisory authority (Article 33 and Recital 85 regarding the notification to the supervisory authority; and

This new scenario directly or indirectly may affect the application and effectiveness of the purpose limitation principle, since some of such new powers and duties may allow the controller to avoid the specific requirements and restrictions established by the purpose limitation principle,[15]as a mechanism to restrain the powers of the controller regarding personal data processing.

All of the above raise important questions that need to be answered in order to evaluate and analyze the current regulation and role of the purpose limitation principle according to the GDPR. This principle may require to be reviewed and perhaps reconsidered or redefined against the application of the GDPR. The proposed research aim to evaluate the relevant changes or innovations in the GDPR that may affect the purpose limitation principle.[16]

Research Question:

This thesis aims to answer the question: *has the relevance and interpretation of the purpose limitation principle changed in the GDPR as compared to the DPD?* The intention of the research is to determine if such principle is still the same key principle[17] as it was previously developed through the DPD.

This will provide a complete understanding of the evolution, current significance and relevance of the purpose limitation principle within the EU data protection legal framework. The outcome of this research will reveal which new elements in the GDPR actually may affect or change the

---

Article 34 and Recital 86 regarding the notification to the data subject); (iv) the evaluation of the inherent risks of processing, and determination of carrying-out a data protection impact assessment in cases of high risk (Article 35 and Recitals 83 and 84); (v) the determination to seek the views of data subjects or their representatives on the intended processing (Article 35 (9); (vi) the previous consultation to the supervisory authority before starting with the processing activities when a data protection impact assessment indicates that the processing would result in a high risk to the rights and freedoms of natural persons (Article 36 and Recital 94);

[15] See for instance the powers and duties established in Articles 6 (1) (f); 6 (4); 35 (9); and 49 of the GDPR; and Recitals 47, 50 and 69, and 94 of the GDPR.

[16] For instance, the legal ground for lawful data processing established in Art 6 (1) (f) of the GDPR which provides the controllers with the possibility to process personal data if it is necessary for the purposes or the legitimate interests pursued by such controller or even a third party, establishing an exception to it and a specific reference to data processing of children. This may represent that for any further processing of personal data, the controller may have a "path" to evade the restrictions of the purpose limitation principle and the compatibility requirement between the original processing purposes and the further processing purpose.

[17] Article 29 Data Protection Working Party (n 2) 4, 41. Article 29 Data Protection Working Party states that the purpose limitation principle is listed in the DPD among the key data protection principles. Additionally, Prins, C, and Moerel L, "On the death of purpose limitation" (2015). International Association of Privacy Professionals; accessed 21 November 2017 via https://iapp.org/news/a/on-the-death-of-purpose-limitation/, state that *"The purpose limitation principle has served as a key principle in data protection for many years…"*

interpretation and application of this key principle. Furthermore, it will provide the required knowledge in order for the author to propose additional measures or changes to the GDPR that eventually may help to improve the application of this principle.

Additionally, the outcome of this research will make possible for the author to assess if the purpose limitation principle is still a necessary or effective instrument to limit data processing, as well as to provide the data subject with the required certainty of the processing and given use of his/her personal data.

Subquestions:

(i) Which are the origins and importance of the purpose limitation principle in the European Union? Determining the backgrounds of such an important principle, will provide a clear idea of its evolution. It will also provide an insight of the changes and improvements implemented through the different norms covering the purpose limitation principle in the European Union.

Furthermore, the purpose of this analysis of the origins and legal backgrounds of the purpose limitation principle, is to have a satisfactory notion of what is the purpose limitation principle, and which are the main elements that compose such principle.

(ii) What was the purpose limitation principle under the DPD? It is crucial for the purposes of this thesis to firstly review and analyze how the purpose limitation principle was regulated within the DPD, since such previous legal framework to the GDPR, served as the base for the implementation of such principle within the GDPR and the basis for comparison.

It is definitely necessary to start with the review and comprehension of the legal status and meaning of this principle according to the DPD. Once it is clearly depicted which is the legal scenario regarding the purpose limitation principle under the DPD, it is necessary to make comparisons when applicable, with the new scenario under the GDPR. This will point out the differences between both legal frameworks, specifically on their approach and legal treatment of the purpose limitation principle.

(iii) What was the purpose limitation principle under the GDPR? The purpose of answering such question is obtaining a clear notion of the purpose limitation principle under the most recent and innovative norm regulating data protection in the European Union.

This chapter will help to confirm if there any new elements such as data subjects' rights and data protection principles established through the GDPR and which were not previously present in the DPD (or that have been reformulated under the GDPR) related with the purpose limitation principle. The purpose is to determine the relevance of such new rights and principles regarding the application and interpretation of the purpose limitation principle, and to determine if such novelties reinforce such principle.

For the purposes of verifying and analyzing the above indicated matters, this research will make specific references to the valuable analysis and/or recommendations made by the Article 29 Data Protection Working Party (hereinafter "Article 29 Working Party") on its Opinion 03/2013.[18]

Literature Review:

With the issuing of the DPD and now with the coming implementation of the GDPR in the European Union, data protection has become a "trending topic" worldwide. Authors that have make researches trying to measure the impact of the DPD in other jurisdictions outside the European Union, for instance Birnhack have found that *"there is sufficient evidence to determine that the Directive has become not only a source of comparative law or a source of inspiration, but an effective mechanism to raise the level of data protection worldwide and that it is doing so better than other mechanisms."*[19]

If the DPD has achieved such well known impact, then the GDPR shall be considered as probably the most relevant legal frameworks on the regulation of data protection and a necessary reference for scholars writing and researching this matter. However there are no researches comparing the DPD with the approved version of the GDPR specifically regarding the purpose limitation principle. Moreover, there is no literature showing the legal development of the purpose limitation principle and its current status within the GDPR.

This research aims to contribute with the fulfillment of such gaps in the literature, and provide valuable insights on matters deeply related with the purpose limitation principle, such as further processing of data, legal grounds for lawful processing and the necessity of a compatibility test according to the GDPR. This will depict the current scenario for the purpose limitation principle,

[18] Article 29 Data Protection Working Party (n 2).

[19] Birnhack MD, 'The EU Data Protection Directive: An Engine of a Global Regime' (2008) 24 Computer Law and Security Report 508

including current understanding, threats, contradictions and applicability under the GDPR. Additionally, this research will provide a comparison and analysis of relevant aspects of Opinion 03/2013 on purpose limitation issued by the Article 29 Working Party and the regulation of such principle within the final version of the GDPR, which will allow identifying similarities and determine the current applicability of Opinion 03/2013 according to the GDPR.

On the other hand, issues related with new technological advances associated with data processing, such as "big data," are one of the main topics been researched, particularly regarding the role and impact that the application of the purpose limitation principle causes to such technologies.

Authors like Zarsky[20] have researched on big data and have specifically addressed the incompatibility between such data processing practices and the existence of the purpose limitation principle and all the restrictions that such principle carries for big data operations. Other authors like Coudert, have also addressed such issues but not entirely arriving to the straight conclusion that there is an incompatibility between purpose limitation principle and big data, since for such author the principle remains to be a *"cornerstone principle of data protection framework and as such it should continue to play a pivotal role in ensuring the foreseeability of data processing activities"*[21]

There are other authors, like Rauhofer[22], Moerel and Prins[23], and Cannataci and Bonnici[24] that have focus on the idea that we may be facing the "end," "death," or "dawn" of the purpose limitation principle. Other authors like Brouwer, have addressed the erosion of the purpose limitation principle but through more positive conclusions with the purpose of restating *"the meaning of purpose limitation by emphasizing its close relation with the principle of legality."*[25]

[20] Zarsky TZ, 'Incompatible: The GDPR in the Age of Big Data' (2017) Vol. 47 Seton Hall Law Review, 26

[21] Coudert F, Dumortier J and Verbruggen F, 'Applying the Purpose Specification Principle in the Age of "big Data": The Example of Integrated Video Surveillance Platforms in France' (2012); accessed 15 March 2018 via http://ssrn.com/abstract=2046123.

[22] Rauhofer J, '"Look to Yourselves, That We Lose Not Those Things Which We Have Wrought." What Do the Proposed Changes to the Purpose Limitation Principle Mean for Public Bodies' Rights to Access Third-Party Data?' (2014) 28 International Review of Law, Computers and Technology 144

[23] Prins, C, and Moerel L (n 17)

[24] Cannataci JA and Bonnici JPM, 'The End of the Purpose-Specification Principle in Data Protection?' (2010) 24 International Review of Law, Computers and Technology 101.

[25] Brouwer E, "Legality and Data Protection Law: The Forgotten Purpose of Purpose Limitation" in Besselink LFM, Pennings F and Prechal S (eds), The Eclipse of the Legality Principle in the European Union, Chapter 14 (2011) 274.

However, it is important to note that per the references made on their research most of these authors based their researches in previous drafts of the GDPR, which were supposing a real threat to the application and conception of the purpose limitation principle, since such drafts were implementing a maximum level of erosion of the purpose limitation principle.

Other authors as for instance Cavoukian, have addressed the problematic of erosion of the purpose limitation principle in a more practical and realistic way, indicating that the *"central problem here is that eliminating purpose limitation gives an unprecedented free hand to data users/controllers…, to unilaterally decide why, what, or when personal data should be collected, used and disclosed, with little input from data subjects or oversight authorities."*[26]

A significant part of the existing literature assesses the issue of the purpose limitation principle as part of an integral review of the correspondent legal bodies (the DPD and the GDPR). The specific review of the principle is usually included within a chapter or through relevant sections or references of their researches, as a relevant part of researching the legal framework as a whole. Most of the times, such researches are made by several authors each of them approaching different matters related with data protection.[27]

In general terms the existent literature is sufficient and of relevance in order to be able to answer the research question of this thesis. Together with such available literature, Opinion 03/2013 issued by the Article 29 Working Party is a very important source of information when assessing the purpose limitation principle, particularly regarding further processing and the compatibility assessment as further indicated in this thesis.

Methodology:

In order to answer the proposed research question, a doctrinal legal research method will be used. Doctrinal legal research is concerned with the formulation of legal doctrines through interpretative and qualitative analysis of legal rules, characterized by the study of legal texts.[28] The doctrinal legal research will be accomplished through review and comparison of relevant

[26] Cavoukian A, 'Evolving FIPPs: Proactive Approaches to Privacy, Not Privacy Paternalism', Reforming European Data Protection Law (2015); 298.
[27] For instance Cavoukian (n 26).
[28] Chynoweth P, 'Legal Research' in A. Knight and L. Ruddock (ed.), 'Advanced Research Methods in the Built Environment' (Blackwell Publishing Ltd, 2008).

academic literature and elements of the DPD as the previous norm, and the GDPR which will be enforceable on May 25th, 2018.

Furthermore, all the above indicated will be complemented with relevant case-law[29], and a review of the Article 29 Working Party's Opinion 03/2013[30] which will be compared towards the final draft of the GDPR in order to confirm if the aspects reflected on such Opinion were actually implemented in the new regulation.

For such purposes, the exercise of comparing the indicated legal framework together with relevant literature and applicable case-law, will provide a complete and thorough comprehension of the current status and relevant changes within the GDPR that may affect the purpose limitation principle.

The author conducted a systematic search through several databases, such as WorldCat, SSRN and Google Scholar to gather relevant literature directly or indirectly related with the purpose limitation principle, and be able to exclude non relevant literature. The examination of such relevant literature allowed to support the proposed ideas and conclusions, and also to evaluate the existence of a knowledge gap regarding the topic of this research.

Comparing the implementation and interpretation of the purpose limitation principle in the DPD with the GDPR may lead to obtain a better understanding and interpretation of its relevance, and if it requires being reinforced or not. Additionally, other new elements of the GDPR may also be addressed to determine if such elements affect in any way the application of the purpose limitation principle as traditionally understood and interpreted nowadays under the DPD.

Chapter Overview:

The second chapter of this thesis intends to cover the backgrounds on the regulation of the purpose limitation principle in the European Union, assessing the relevance and importance of such principle and establishing its origins. The third chapter will review and analyze the purpose limitation principle under the DPD, as the previous legal framework on the matter before the creation of the GDPR. The fourth chapter will focus on the analysis of the purpose limitation

[29] Case-law from both the European Court of Human Rights (hereinafter "ECtHR") and the Court of Justice of the European Union (hereinafter "CJEU") related with the purpose limitation principle will be located and reviewed.
[30] Article 29 Data Protection Working Party (n 2).

under the GDPR, identifying the new elements included within the GDPR that may affect in any way the application and interpretation of the purpose limitation principle under the GDPR. Particularly, this fourth chapter (together with chapter three) will point out the main differences on the regulation of such principle between the DPD and the GDPR. The thesis will be finalized with a concluding chapter, in which the author will state the answers and conclusions obtained through the research.

Chapter 2: Origins and importance of the purpose limitation principle in the European Union.

The main goal of this chapter is to provide a clear and precise scenario of the backgrounds for the regulatory development of the purpose limitation principle within the European Union, which provided the legal basis for the issuing of the DPD and the GDPR. It will answer the question on which were the origins and the importance of the purpose limitation principle in the European Union. Particularly it will focus on the legal approach and treatment provided to the data protection principle through an overview of the OECD Guidelines,[31] Convention 108,[32] the inclusion of the right to data protection within the Charter of Fundamental Rights of the European Union[33] and the specific reference to the purpose limitation as part of such right, and the relevant case law of the European Court of Human Rights ("ECtHR").

Section 2.1 will focus on the origins and rationales behind the principle of purpose limitation in the European Union, its conceptualization and definition, meaning what is intended to achieve through this principle and which are the major elements that compose such principle. This Section will provide an explanation of the legal backgrounds and evolution of this principle within the European Union, excluding the Charter (which will be reviewed in the following section) and as previously indicated, excluding as well the DPD and the GDPR which will be further reviewed and analyzed on the following chapters.

[31] Organisation for Economic Cooperation and Development (OECD), Guidelines Governing the Protection of Privacy and Transborder Flow of Personal Data 23rd September, 1980, hereinafter the "OECD Guidelines"
[32] Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28th January 1981 (hereinafter "Convention108").
[33] Charter of Fundamental Rights of the European Union (2000/C 364/01), 18th December 2000, hereinafter the "Charter"

Furthermore, Section 2.1 will be divided in three subsections as follows: (i) Subsection 2.1.1 which will analyze the notion of the purpose limitation principle in the European Union and the issuing of the OECD Guidelines as a first step of the evolution of such principle; (ii) Subsection 2.1.2 will analyze and review the inclusion and treatment of the purpose limitation principle within Convention 108 as the first legal body formally stating the purpose limitation principle; (iii) Subsection 2.1.3 will provide some specific examples on how was the purpose limitation principle developed and affected through the case law of the ECtHR.

Section 2.2 will review the inclusion of the right to data protection within the Charter and the implications of such inclusion, meaning granting such right with the protection and relevance of a fundamental right within the European Union.

The identification, analysis and review of legal backgrounds of the regulation of the purpose limitation principle will provide a complete overview of the past of such principle, and will help to understand its present and visualize its future within the European Union.

2.1 Conceptualization and backgrounds of the purpose limitation principle:

2.1.1 Notion of the purpose limitation principle in the European Union and the issuing of the OECD Guidelines:

Certainly the purpose limitation principle has been one of the cornerstones of the European Union's data protection regime.[34] It is a principle created with the goal of protecting data subjects through the establishment of limits on how data controllers are able to use their collected data.[35] It is an important data protection principle, created in order to provide transparency to data processing, to assess a legitimacy of data processing and to prevent the abuses of the controller's powers.[36]

The purpose limitation principle provides an important balance of interests between the controllers' necessities of collecting, storing and processing personal data and the right of the

[34] Zarsky (n 20) 1006. Other authors such as Cannataci and Bonnici (n 30) describing the principle as of "purpose-specification", have indicated that such principle establishes that a citizen needs to be informed why his/her personal data is being collected and the specific purposes for which it will be processed and kept, and which represents a central protection in data protection regulation.
[35] Article 29 Data Protection Working Party (n 2) 3.
[36] Coudert (n 21)

data subjects to have respect of their private life[37]and obtaining the required protection of their personal data. It provides to data subjects the possibility to have some level of control over their personal data processing,[38]feeling certain level of confidence and trust[39] provided by the knowledge of the uses and purposes of their personal data been processed,[40]and intending to reduce a priori the risks of harm against the data subjects.[41]

Furthermore, the purpose limitation principle seeks the foreseeability of data processing activities.[42] For such reason, in order for the data subject to foresee the scope of his or her personal data processing, it is important for the data subject to clearly know the purposes of such processing. That knowledge of the processing purposes will provide the data subject with confidence and trust towards the processing of his or her personal data. Additionally, foreseeability and knowledge of the data processing purposes by the data subjects is perceived as a relevant component of data protection and are of major concern for the general public.[43]

For the purpose of illustrating the above mentioned, if a data subject knows that certain of his or her personal data was collected for the purposes of obtaining financial services, such as for example a loan secured through a mortgage, such data subject may expect for his personal data to be used by the controller in order to offer to the data subject the acquisition of a credit card or other financial products. The processing of personal data for such purposes may be foreseen and reasonably expected by the data subject.

---

[37] Cannataci (n 24) 102.

[38] Zarsky (n 20) 1006.

[39] Coudert (n 21). The authors identify one of the main functions of the purpose specification, as a *"tool of trust, providing legal certainty to data subjects, in that it requires personal data not to be processed beyond their reasonable expectations."*

[40] Article 29 Data Protection Working Party (n 2) 4. Regarding this matter the Article 29 Data Protection Working Party has indicated that *"When we share personal data with others, we usually have an expectation about the purposes for which the data will be used. There is a value in honouring these expectations and preserving trust and legal certainty, which is why purpose limitation is such an important safeguard, a cornerstone of data protection."*

[41] Coudert (n 21). The authors state that the purpose specification was intended to *"fragment personal data processing activities and forms closed compartments in order to avoid concentration of controlling powers by limiting the amount of information processed and shared, reducing a priori the risks of harm"*

[42] Ibid.

[43] Hallinan D, Friedewald M and McCarthy P, 'Citizens' Perceptions of Data Protection and Privacy in Europe' (2012) 28 Computer Law and Security Review; 268. The authors indicated that based on the Special Eurobarometer 359, published on 2011, the public demonstrated concern regarding commercial collection and use of data such as direct mail, spam, cold calling etc and that related to this, they showed concern towards certain data practices linked to this fear (but which also have wider significance), the fear that information would be "used without knowledge", "shared with third parties without agreement" and "that information would be used in different contexts than those in which it was disclosed"

According to the Article 29 Data Protection Working Party, this principle is composed of two main components[44] as follows:

(i) the personal data has to be collected for specified, explicit and legitimate purposes, which is also known as "purpose specification"[45].

(ii) for such personal data not to be further processed in a way incompatible with those purposes, meaning that a "compatible use"[46] with the original purposes is required in order for the controller to further process the collected personal data.

The evolution of the relevant legislation implemented through the years, allowed the creation of such notion of the purpose limitation principle. Starting with the OECD Guidelines issued in 1980 for the first time, and reviewed in 2013.[47] The OECD Guidelines were created in order to help in the harmonization of national privacy legislation, in the form of a recommendation adopted by the Council of the OECD and it became applicable in September 23rd, 1980. The intention was to establish a *"consensus on basic principles"*[48] which may further be implemented within national legislation or help in the creation of such legislation in countries which do not have it at that time.

The purpose limitation principle was then covered through the OECD Guidelines in the form of three important principles as follows:

(i) the "data quality principle" requiring the collected personal data to be relevant to the purposes to which it will be used and to the "extent necessary for those purposes";[49]

(ii) the "purpose specification principle", closely related to the data quality principle and the use limitation principle explained below[50], represents the fundamental core of the current notion of the purpose limitation principle covering both of its main elements ("specification of the purposes" and the "compatibility use"). This principle states that the *"purposes for which*

[44] Article 29 Data Protection Working Party (n 2) 3.
[45] Ibid; 11
[46] Ibid; 12
[47] OECD Guidelines (n 31)
[48] Preface of the OECD Guidelines (n 31).
[49] OECD Guidelines (n 31), Paragraph 8
[50] Ibid; Paragraph 54. This paragraph expressly indicates that "The Purpose Specification Principle is closely associated with the two surrounding principles, i.e. the Data Quality Principle and the Use Limitation Principle"

personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose";[51] and

(iii) the "use limitation principle" which establishes that the personal data *"should not be disclosed, made available or otherwise used for purposes other than those specified"*[52] and establishing two general exceptions to such principle.[53] This principle intended to avoid the inclusion of new purposes introduced arbitrarily[54] making emphasis on the requirement of compatibility of the new purposes with the original ones.

2.1.2 The purpose limitation principle within Convention 108:

The notion of purpose limitation was then established as a specific and independent data protection safeguard, by the Council of Europe through Convention 108. This legal body *"introduced the concept of the protection of personal data in Europe."*[55] Article 5 of such Convention establishes the basic principles of data protection, indicating that any personal data undergoing automatic process shall be: *"stored for specified and legitimate purposes and not used in a way incompatible with those purposes;*[56]*... adequate, relevant and not excessive in relation to the purposes for which they are stored;*[57]*... preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored."*[58]

The inclusion of the purpose limitation principle as an essential principle of data protection[59] was labelled by the Article 29 Data Protection Working Party as an "important step" since *"a legal*

[51] Ibid; Paragraph 9
[52] Ibid; Paragraph 10
[53] Ibid. The principle had two exceptions for the use limitation principle allowing to use the personal data for different purposes that the previously specified in case in which there is a provided consent of the data subject or his/her representative, or by the authority of law
[54] Ibid; Paragraph 54
[55] Article 29 Data Protection Working Party (n 2) 7
[56] Article 5 (b) of Convention 108.
[57] Ibid; Article 5 (c).
[58] Ibid; Article 5 (e).
[59] Article 29 Data Protection Working Party (n 2) 7

basis and specification of a legitimate purpose are now required in all circumstances where personal data are processed."[60] As the first legal norm regulating data protection and specifically stating the purpose limitation principle as an important principle for such data protection, it could be said that Convention 108 established the legal pillar in which further norms adopted within the European Union for data protection were based on.[61]

Convention 108 clearly included the purpose limitation principle not only as an independent element of data protection introducing the concepts of "specified and legitimate purposes" and "incompatibility", but also as a notion which is present in other principles or requirements for data processing. For example, as indicated above the personal data must be adequate, relevant and not excessive specifically regarding the purposes for which it is stored (data minimization principle).

Furthermore, as an example of the influence and consequent repercussion of the content of Convention 108 on other legal bodies adopted later on in the European Union for the regulation of data protection, the notion of "incompatibility" established within Convention 108 was also used for the DPD.

There are also several examples of how the purpose limitation works indirectly as an element of data protection which is related with other data protection safeguards, and not only as a separate principle. Such association within the different data protection principles was also pointed out in the OECD Guidelines.[62]

2.1.3 Court cases of the ECtHR:

The concept of purpose limitation has been also developed through the privacy case law of the European Court of Human Rights ("ECtHR") specifically under the coverage of Article 8 of the

[60] Ibid.

[61] Ibid; 8. Article 29 Data Protection Working Party indicated that such early texts provided *"some elements of what will later become key building blocks of the right to the protection of personal data, including the principle of purpose limitation"*

[62] OECD Guidelines (n 31) Paragraph 50. It indicates that the principles stated in Paragraphs 7 to 14 of the Guidelines are "interrelated and partly overlapping" and that "the distinctions between different activities and stages involved in the processing of data which are assumed in the principles, are somewhat artificial and it is essential that the principles are treated together and studied as a whole"

European Convention on Human Rights ("ECHR"),[63] which incorporated the right to privacy specifically through the right to respect every person's private and family life, home and correspondence. On a case by case basis, the ECtHR has then *"recognized aspects of the data protection doctrine"*[64] through its case law.

For instance ECtHR's judgement on S. and Marper v. the United Kingdom[65] expressly referred to the relevance of personal data protection and its association with the right to respect privacy. In such case the Court indicated that the following:

"…protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the Convention. The domestic law must afford appropriate safeguards to prevent any such use of personal data as may be inconsistent with the guarantees of this Article ... The need for such safeguards is all the greater where the protection of personal data undergoing automatic processing is concerned, not least when such data are used for police purposes. The domestic law should notably ensure that such data are relevant and not excessive in relation to the purposes for which they are stored; and preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored …"[66]

As indicated above, the ECtHR highlighted the *"fundamental importance"* of personal data protection for a person to duly enjoy his/her right to respect of privacy. The ECtHR provides a direct association of both the protection of personal data and the right to privacy according to the content of Article 8 of the ECHR. The ECtHR emphasizes in the need of having appropriate safeguards and makes a direct reference to the principle of purpose limitation when indicating that such data must be *"relevant and not excessive"* regarding the purposes of its storage, and that it must be kept *"for no longer than is required"* for the purposes of such storage of data.

In other cases the ECtHR has been very insistent in the fact that when there is an interference with the right to respect private life according to Article 8 of the ECHR, it has to be

[63] Convention for the Protection of Human Rights and Fundamental Freedoms, 4th November 1950 (hereinafter "ECHR")
[64] Koning M.E., 'Purpose Limitation' in van Lieshout M, and Hoepman JH (eds), P.I.Lab, 4 years later; p 139-148; accessed 19 March 2018 via https://merelkoning.nl/academic-work
[65] S. and Marper v. the United Kingdom, n. 30562/04 30566/04, ECtHR 2008
[66] Ibid.

proportionate to the "aim pursed" which refers to the purposes of data processing. For instance, the ECHR indicated in L.L. v. France that the *"impugned interference with the applicant's right to respect for his private life, in view of the fundamental importance of the protection of personal data, was not proportionate to the aim pursued and was therefore not necessary in a democratic society for the protection of the rights and freedoms of others"*[67]

The ECtHR then came to an important conclusion, which is that if an interference with the right to respect private life lacks of proportionality to the aim pursued, it is consequently not necessary in a democratic society as required according to Article 8 (2) of the ECHR[68]

There are other relevant cases resolved by the ECtHR involving aspects associated with the concept of purpose limitation on personal data within the right to privacy, as for instance the cases of data collection made by national secret services,[69] and the cases related with disclosure or retention of personal medical data of subjects.[70] Additionally, there is plenty case law by the ECtHR regarding the importance of law foreseeability[71] which could be also applicable to the requirement of foreseeability by the data subject of the purposes for data processing.

2.2 Purpose limitation principle in the Charter of Fundamental Rights of the European Union (the "Charter") as part of the fundamental right to data protection:

After the creation of the DPD, the right to data protection was also included as a fundamental right as part of the Charter. It was stated as a separate and independent right, different from the right to respect private and family life which was established through Article 7 of the Charter.

[67] L.L. v. the France, n. 7508/02, ECtHR 2006

[68] Article 8 of the ECHR establishes that any interference with such right must be necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

[69] As for example: Rotaru v. Romania n. 28341/95, ECtHR 2000; and Amann v. Switzerland, n. 27798/95, ECtHR 2000.

[70] As for example Z v. Finland n. 22009/93, ECtHR 1997; Armoniene v. Lithuania n. 36919/02, ECtHR 2008; Biriuk v. Lithuania n. 23373/03, ECtHR 2008; K.H. and Others v. Slovakia N. 32881/04, ECtHR 2009

[71] For instance Amann v. Switzerland, n. 27798/95, ECtHR 2000; Rotaru v. Romania, n. 28341/95, ECtHR 2000;Leander v. Sweden, n. 9248/81, ECtHR 1987; Malone v. The United Kingdom, n. 8691/79, ECtHR 1985; Kruslin v. France, n. 11801/85, ECtHR 1990.

The specific right to data protection was included as a fundamental right under Article 8 of the Charter. As part of such new fundamental right to data protection[72], it was included an express reference to the purpose limitation when indicating that personal 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…"*[73]

In general terms, the issuing of the Charter is a very important step for the development of data protection in Europe, but particularly it can also be considered as an "upgrade" of the purpose limitation principle. As an integral part of the right to data protection, this principle is at the core of the fundamental right to data protection as recognized by the Charter.[74] The inclusion of the purpose limitation principle's essence within the European legal framework of fundamental rights is of major relevance, since such principle is now covered within the special legal treatment and protection which is only granted to "fundamental rights".[75]

Another contribution of the Charter to the purpose limitation principle was the clear differentiation it includes between the requirement for purpose specification and the requirement of an appropriate legal ground. Article 8.2 clearly refers in a separate manner to each of these requirements, meaning that both requirements can be considered as "cumulative"[76] for data processing, but separately individualized and differentiated from each other.

It was then reasonable to expect that the GDPR did not leave this relevant principle outside of its regulation. Consequently the GDPR was finally drafted and issued complying with the protection and respect that such a core principle of data protection requires, since in general terms, the GDPR has to respect *"all fundamental rights and observes the freedoms and principles recognised in the Charter."*[77]

[72] Article 29 Data Protection Working Party (n 2) 10. The Article 29 Data Protection Working Party emphasizes that the inclusion of data protection as a fundamental right makes the Charter to be apart from other key human rights instruments that usually have treated the right to data protection as an extension of the right to privacy.
[73] Article 8 (2) of the Charter
[74] Coudert (n 21).
[75] Zarsky (n 20) 1006. The author refers to the purpose limitation principle as one of the cornerstones of the EU's data protection regime which is clearly noted in article 8(2) of the Charter of Fundamental Rights of the European Union.
[76] Article 29 Data Protection Working Party (n 2) 12.
[77] Recital 4 of the GDPR

Since the purpose limitation principle is part of the fundamental right to data protection stated within the Charter, it leaved no choice to the drafters of the GDPR but to fully include this principle within the GDPR.[78] Zarsky[79] provides as an example of a possible scenario if such principle would have been ignored or diluted within the GDPR; this could lead to a situation similar to the invalidation of Directive 2006/24/EC by the CJEU.[80] The CJEU invalidated Directive 2006/24/EC stating that such Directive 2006/24/EC *"exceeded the limits imposed by compliance with the principle of proportionality in the light of Articles 7, 8, and 52(1) of the Charter."*[81]

Furthermore, in order to confirm and reinforce the above indicated position regarding the provided example of the invalidation of Directive 2006/24/EC it is important to stand out the Data Protection Supervisor's position when indicating that:

"... it is compulsory to ensure that any new instrument relating to information exchange in the EU is proposed and adopted only if the purpose limitation principle has been duly considered and that any possible exceptions and restrictions to this principle are decided on a case-by-case basis... Any other practice would be contrary to Article 8 of the Charter of Fundamental rights of the Union and to the EU law on data protection"[82]

Something similar to the above indicated invalidation of Directive 2006/24/EC may have suffered at some point the GDPR if the purpose limitation principle would have been excluded, only partially included, or even somehow eroded within such new data protection legal framework.

[78] Zarsky (n 20) 1006. The author indicates that given the purpose limitation's enshrinement within the EU's primary legal source, meaning the Charter of Fundamental Rights of the European Union, the GDPR's drafters had no choice but to incorporate it in full within the GDPR. *"Any step short of that would have risked the invalidation of the GDPR by the European Court of Justice"*.

[79] Ibid.

[80] Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

[81] Joined Cases C-293/12 and C-594/12 Digital Rights Ireland v. Minister for Communications, Marine and Natural Resources and others [2014] CJEU

[82] EDPS, Opinion of the European Data Protection Supervisor on the communication from the Commission to the European Parliament and the Council - 'Overview of information management in the area of freedom, security and justice', C 355/03 (2010).

Of course there are some authors that do not agree with the idea of having such a "light" right labelled as a "fundamental right" indicating for example that it is not a "true fundamental right".[83] This is a simplistic way of arguing that the right to data protection has not achieved yet the level of fundamental right, and so it is not "worthy" of being considered as such. However, legal rights and duties are not fixed and rather are subject to constant evolution and change, especially regarding the society's perception and interpretation of them. It is clear that the right to data protection has acquired through the years an important level of relevance and consideration[84] by the general public in Europe, and that its inclusion as a fundamental right based on such acquired and current relevance is more than justified.

Notwithstanding the above indicated the fundamental right to data protection is not an absolute right,[85] and such condition is then extended to the purpose limitation principle as part of such fundamental right. For that reason, certain level of interference and erosion to such principle is not only acceptable, but necessary in order to balance it with other fundamental rights and principles as well as with the different interests involved within the activity of data processing, such as the interests of controllers and the interests of data subjects.

According to the Charter,[86] the exercise of the right to data protection may be limited in certain cases. Any limitation on the exercise of the right to data protection must comply with certain requirements, namely (i) the limitation must be provided by law respecting the essence of such rights and freedoms; and (ii) the limitation is necessary, according to the principle of proportionality, and it genuinely meets the objectives of general interest or the need to protect the rights and freedoms of others. Furthermore, Article 8(2) of the Charter implies that personal data

[83] Bergkamp L, 'EU Data Protection Policy - The Privacy Fallacy: Adverse Effects of Europe's Data Protection Policy in an Information-Driven Economy' 31. The authors indicated regarding the inclusion of the right to data protection as a fundamental right within the Charter, the following: *"An unfortunate consequence of including this right among truly fundamental rights, such as the prohibition of torture and slavery and the freedom of expression, is that the notion of fundamental right seriously devaluates, with adverse consequences for the respect for the core human rights"*

[84] Hallinan (n 43) 263. The authors indicated that *"From the survey results it is clear that the public allocates data protection and privacy significant importance… it is notable that the majority of Europeans appear familiar with the key rights the data protection framework offers…"*

[85] Joined Cases C 92/09 and C 93/09 Volker und Markus Schecke and Eifert v. Land Hessen [2010] CJEU. The Court indicated that *"The right to the protection of personal data is not, however, an absolute right, but must be considered in relation to its function in society"* Additionally, Recital 4 of the GDPR clearly confirms the above, adding that the right to data protections has to *"be balanced against other fundamental rights, in accordance with the principle of proportionality"*

[86] Article 52 of the Charter.

may be processed in cases in which certain requirements and conditions are met. These limitations to the right to data protection within the Charter, reveal that it is not an absolute right and that there may be collisions with other individual rights.

Chapter 3: The purpose limitation principle in the DPD.

Chapter 3 will provide a comprehensive description on how is the purpose limitation principle structured and treated within the DPD. Consequently it will answer the question on what was the purpose limitation principle under the DPD, and will focus on reviewing the approach and treatment provided to the purpose limitation principle under the DPD pointing out all relevant legal elements related with such principle. It will also include a review of the Article 29 Working Party Opinion 03/2013 on purpose limitation, and the relevant findings and interpretations included within such Opinion.

Section 3.1 will refer to the scope and restrictions of the purpose limitation principle within the DPD. The intention of this section would be to analyze from a normative perspective how is the purpose limitation structured, defined and conceptualized through the DPD. It will reveal which are the relevant elements that compose or relate with such principle under the DPD.

This analysis is of high relevance since the DPD preceded the GDPR, so the review of such legal body will start revealing the main legal differences and similarities between the DPD and the GDPR regarding the treatment of the purpose limitation principle, and will provide the required knowledge of the DPD in order to understand the analysis made in the following chapter regarding the GDPR.

Section 3.2 will provide a review of the Article 29 Working Party Opinion 03/2013 on purpose limitation. Such Section 3.2 will be divided in two subsections as follows: (i) Subsection 3.2.1 will explain which are the backgrounds and the relevance of the opinions and recommendations issued by the Article 29 Working Party; and (ii) Subsection 3.2.2 will analyze how the Article 29 Working Party assessed through Opinion 03/2013 the compatibility for further processing.

3.1 Scope and restrictions of the Purpose Limitation Principle within the DPD

The purpose limitation principle was established in Article 6, Section (b) of the DPD, which states that personal data must be *"collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes…"*[87] With such statement, the DPD clarifies that the purposes of data processing have to be specified[88] and manifested by the controller to the data subject before starting with such data processing,[89] and that any personal data processing for unclear, undefined or unlimited purposes is unlawful.[90]

The above indicated is clearly confirmed and clarified through Recital 28 of the DPD which indicates that the personal data to be collected *"… must be adequate, relevant and not excessive in relation to the purposes for which they are processed; whereas such purposes must be explicit and legitimate and must be determined at the time of collection of the data."*[91] In order for the processing purposes to be considered legitimate they need to have a legal ground for processing (which are stated in Article 7 of the DPD) and also they need to comply with a general lawfulness in regards of other applicable areas of law.[92]

Furthermore, the DPD establishes that further processing in an incompatible way with the originally specified purposes is not allowed.[93] Further processing should be understood as *"any processing following collection, whether for the purposes initially specified of for any additional purposes."*[94] It also establishes that the data involved in such further processing must be

[87] Article 6 (b) of the DPD.
[88] Article 29 Data Protection Working Party (n 2) 12. The Article 29 Working Party states that specified means *"sufficiently defined to enable the implementation of any necessary data protection safeguards, and to delimit the scope of the processing operation.."*
[89] European Union Agency for Fundamental Rights, Handbook on European Data Protection Law (2014), p 68. Available also online at < http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf> accessed 8 February, 2018.
[90] Ibid.
[91] Recital 28 of the DPD.
[92] Article 29 Data Protection Working Party (n 2) 12, 20.
[93] Recital 28 and Article 6(b) of the DPD.
[94] Article 29 Data Protection Working Party (n 2) 21.

adequate, relevant and not excessive in relation to the purposes for which the data will be further processed.[95]

As an additional element, it is included a specification for the further processing of personal data for historical, statistical or scientific purposes, for which such further processing shall not be deemed as incompatible with the original purposes of data processing, as long as appropriate safeguards are provided by the Member States.[96] This means that the compatibility of further processing for historical, statistics or scientific purposes will be directly determined by the existence of such appropriate safeguards specified by the Member States.

The characteristics of the required safeguards to be provided by the Member States for the further processing for historical statistical or scientific purposes are barely described by the DPD when indicating that the safeguards must be *"suitable safeguards"*[97] and that such safeguards *"must in particular rule out the use of the data in support of measures or decisions regarding any particular individual"*[98]

It is also important to note that most of the other sections of Article 6[99] state a specific reference to the purpose of data collecting, using it as an instrument to delimitate the use and nature of such data. For instance, section (d) provides that the purposes of data collection or the purposes for which data is been further processed, would serve as the criteria in order to determine if such data is inaccurate or incomplete.[100] Following this same interpretation, the Article 29 Working Party has indicated that ensuring that the purpose for processing is specific, explicit and legitimate is a *"prerequisite for other data quality requirements, including adequacy, relevance and proportionality…"*[101]

The evident change between Article 5 of Convention 108 and Article 6 of the DPD regarding the purpose limitation principle is that on the drafting of Article 6 of the DPD there is a clear

[95] Recital 28 and Article 6(c) of the DPD.
[96] Ibid; Article 6 (b).
[97] Ibid; Recital 29.
[98] Ibid. Also the Article 29 Data Protection Working Party (n 2) 28 indicated that "The term 'rule out' suggests that the safeguards should indeed be strong enough to exclude or at least minimize any risks to the data subjects" and that "in order to ensure appropriate safeguards, the term 'measures or decisions' should be interpreted in the broadest sense
[99] Ibid; Article 6 (c), (d) and (e).
[100] Ibid; (d).
[101] Article 29 Data Protection Working Party (n 2) 12.

intention to include the "explicitness" requirement as an additional limitation to be incorporated as part of the purpose limitation principle. Requiring the purposes for processing to be "explicit" means that they need to be *"sufficiently unambiguous and clearly expressed"*[102] meaning *"clearly revealed, explained or expressed in some intelligible form"* [103]

From the essence of Recital 28 of the DPD, it seems that the intention of having such explicit purposes is closely related with having such purposes determined by the controller at least at the time of, and not later than, the start of processing. The requirement for the purposes to be explicit is then related "hand by hand" with the data subject's foreseeability and predictability, the clear understanding and acknowledgement of the processing purposes.

This is reinforced by the fact that the DPD expressly establishes for the controller to provide the data subject with the information related to the intended purposes of the data processing.[104] It is also important to link such obligation for the controller to inform the data subject, with the right of the data subject to have access and confirm the information related to the purposes of the processing made by a controller.[105] The possibility for the data subject to know the purposes of processing as part of the right to have access to his/her processed data, was also extended to the knowledge of the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed.[106]

Additionally to the above indicated, the DPD included another proceeding that was required to be followed by the data controller, which is the notification to the Supervisory Authority.[107] According to Articles 18 and 19 of the DPD, the controller was obliged to notify the Supervisory Authority *"before carrying out any wholly or partly automatic processing operation or set of such operations intended to serve a single purpose or several related purposes."*[108] As part of the information to be provided within such notification, the data controller was required to disclose the purpose or purposes of the data processing.[109]

[102] Ibid; 17
[103] Ibid; 12
[104] Article 10 (b) of the DPD.
[105] Ibid; Article 12 (a)
[106] Ibid.
[107] Ibid; Article 28 and 18(1)
[108] Ibid; Article 18 (1)
[109] Ibid; Article 19

Recital 48 DPD intends to provide a justification for such obligation of previous notification, indicating that such procedures were designed to ensure disclosure of the purposes and of the main features of any processing operation *"for the purpose of verification that the operation is in accordance with the national measures taken under this Directive*."[110]

It is clear that the purpose of the notification to the Supervisory Authority was to exercise certain supervision and control over the controller's processing operations. It was implemented with the intention of verifying the controller's compliance with certain aspects of the personal data processing legal framework[111].

The DPD also included the conditions and requirements for the application of the exceptions and restrictions to the purpose limitation principle, and in general terms to the data protection principles established through Article 6 of the DPD. According to Article 13 of the DPD which "*follows the same logic as Article 9 of Convention 108*,"[112] such restrictions and exemptions must constitute a necessary measure in order to safeguard aspects and objectives of the Member States' general interest, criminal prosecution and security[113] or to the *"protection of the data subject or of the rights and freedoms of others"*[114]

3.2 Article 29 Working Party Opinion on Purpose Limitation:

3.2.1 Backgrounds and relevance of the opinions and recommendations issued by the Article 29 Working Party:

"Article 29 Working Party" is the short name commonly used to refer to the "Working Party on the Protection of Individuals with regard to the Processing of Personal Data."[115] It is composed of a representative of each supervisory authority or authorities as designated by each Member

[110] Ibid; Recital 48
[111] Recital 25 of the DPD indicates that "the principles of protection must be reflected, on the one hand, in the obligations imposed on persons, public authorities, enterprises, agencies or other bodies responsible for processing, in particular regarding data quality, technical security, notification to the supervisory authority…" Additionally, the contents that should be covered by such notification according to Article 19 of the DPD, are clearly intended to confirm compliance with certain relevant aspects of the legal framework, such as for example indicating the purpose of processing, a description of the category of data subjects and of the data or categories of data related to them, and the proposed transfers of data to third countries.
[112] Article 29 Data Protection Working Party (n 2) 9.
[113] Article 13 (a), (b), (c), (d), (e), and (f) of the DPD
[114] Ibid; Article 13 (g)
[115] Ibid; Article 29

State and by a *"representative of the authority or authorities established for the Community institutions and bodies, and of a representative of the Commission"*[116] Such entity was created according to Article 29 of the DPD, which provides the Article 29 Working Party with the status of an independent advisory entity of the European Commission on matters related with data protection.

As established through Article 30 of the DPD, this entity must support the European Commission on matters related with data protection through its opinions and recommendations on the matter. The opinions and recommendations issued by the Article 29 Working Party are intended to contribute in the development of harmonised policies for data protection within the European Union. In words of Poullet *"it is quite clear that the creation of this common Working Group has, to a large extent, permitted informaI exchanges between the different national Data Protection Authorities. This has contributed to harmonisation in the interpretation of the provisions of the Data Protection Directive as weIl as an exchange of "best practices."*[117]

The opinions and recommendations issued by the Article 29 Working Party regarding data protection are together with relevant case law, one of the most important sources of guidance on the interpretation of the European Union's data protection legal framework. The Article 29 Working Party has provided since its creation, valuable analysis and interpretations of the applicable law on data protection related matters, such as the DPD.

On 2013 the Article 29 Working Party issued Opinion 03/2013 which purpose was to clarify the scope and functionality of the purpose limitation principle.[118] For such reason this Opinion 03/2013 provides valuable input not only for the clear understanding of such principle within the DPD, but it is also a very important instrument that should be used as a reference for the issuing of any further regulations of data protection involving the purpose limitation principle, such as the GDPR. For such reasons, Opinion 03/2013 can be considered as a valuable source of research regarding the purpose limitation principle and the elements that compose such principle.

[116] Ibid.
[117] Poullet Y, 'EU Data Protection Policy. The Directive 95/46/EC: Ten Years after' (2006) 22 Computer Law and Security Report 206.
[118] Article 29 Data Protection Working Party (n 2).

3.2.2 Article 29 Working Party's assessment of compatibility for further processing:

Article 29 Working Party establishes through Opinion 03/2013 two possible ways to assess the compatibility of purposes for further processing. The compatibility test may be (i) formal, which will require a comparison between the purposes for data collection *"with any further uses"*[119] in order to confirm if such uses were *"explicitly or implicitly"*[120] covered; or it may be (ii) substantive, which will *"go beyond formal statements to identify both the new and the original purpose."*[121] This substantive assessment needs for the data controller to take into consideration the way these purposes are or should be understood *"depending on the context and other factors"*.[122] The Article 29 Working Party considers the substantive test to be more flexible and effective, highlighting the condition of such test to adapt to future developments in the society.[123]

Based on the substantive assessment compatibility test, there are several criteria that will help to assess if the purpose for data collection and the purposes for further processing are incompatible or not. Most of these criteria developed by the Article 29 Working Party in its Opinion 03/2013 were then included within the GDPR (for instance Article 6 (4) as well as in Recital 50 of the GDPR). Since the criteria for the compatibility assessment included within Opinion 03/2013 was used as the base to establish such criteria within the GDPR, Opinion 03/2013 is still a current source for interpretation of common aspects of the purpose limitation principle shared between the DPD and the GDPR or as in this case between the content of Opinion 03/2013 and the GDPR.

The Article 29 Working Party found the following criteria for the compatibility test which were included in Opinion 03/2013:[124]

(i) The relationship between the purposes for which the data have been collected and the purposes of further processing: These criteria refer to the relationship existing between the

[119] Ibid; 21
[120] Ibid.
[121] Ibid.
[122] Ibid.
[123] Ibid; 22
[124] Ibid; 23-27

purposes for collection and the purposes for further processing, focusing on the essence of both processing purposes. For instance the purpose for further processing is a consequence or logical further step in the specific data processing

(ii) The context in which the data have been collected and the reasonable expectations of the data subjects as to their further use: This criteria refers to cases in which, according to the Article 29 Working Party a reasonable person will consider the further data processing not only as unexpected or surprising, but also inappropriate or objectionable. It entails a relevant element in order to determine such context, which is the nature of the relationship between data subject and data controller, which also *"requires an investigation into the balance of power between the data subject and the data controller."*[125] This refers to particular cases in which it shall be assessed for example how mandatory was for the data subject to provide such data for processing. It mainly focus on what is expected or customary within the specific context accordingly to the relationship existing between data controller and data subject, and to take into account the characteristics and context details of the specific data processing;

(iii) The nature of the data and the impact of the further processing on the data subjects. These criteria focus on the type of data and on the impact that the further processing of such data may cause to the data subject. According to this criteria, when assessing compatibility the data controller needs to determine if sensitive data or any other type of personal data which requires a special protection would be involved in the further processing. It is also important to envisage and define which could be the negative and the positive consequences of the further processing, such as for example, *"situations where the processing may lead to the exclusion or discrimination of individuals"*[126]

(iv) The safeguards applied by the controller in order to ensure fair processing and to prevent any undue impact of the data subjects: This refers to the actions and measures that data controllers may undertake in order to ensure a safe and fair further processing. It includes the use of *"anonymization, pseudonymisation, and aggregation of data."*[127]

[125] Ibid; 24
[126] Ibid; 25.
[127] Ibid; 26.

Chapter 4: The purpose limitation principle in the GDPR.

This chapter will provide a review and comprehension of the current legal status and meaning of the purpose limitation principle according to the GDPR. It will answer the question on what is the purpose limitation principle under the GDPR, and will assess specific elements which are relevant for the understanding of the purpose limitation principle under the GDPR. In order to be able to confirm which is the current status and legal treatment for the purpose limitation principle under the GDPR, it is definitely necessary to review aspects such as the intended reduction of the principle's scope within the previous drafts of the GDPR, the further processing of data and the compatibility test among other relevant aspects.

While depicting the legal scenario for the purpose limitation principle under the GDPR, and where it is applicable within this chapter, there will be direct references and comparisons with the previous norm, meaning the DPD. This will point out the differences and similarities between both legal frameworks, particularly on their approach and legal treatment of the purpose limitation principle and related matters.

Section 4.1 will make an analysis and review of the intended reduction of the scope of the purpose limitation principle within the previous drafts of the GDPR. This is of particular relevance because it will depict which was the scenario for the purpose limitation principle back in those days in which the GDPR was been discussed, and will help the readers to understand the challenges that this principle may face in the future.

Section 4.2 will focus on the relevance and importance of the purpose limitation principle within the GDPR, specifically regarding the scope and meaning of this principle under Article 5 of the GDPR. Such Article 5 of the GDPR is a very important norm since it lists and explains the main data protection principles covered through the GDPR.

Section 4.3 will provide an analysis of further data processing within the GDPR. It will specifically cover the compatibility test according to the GDPR, and will separately review the content and interpretation of Recital 50 under the GDPR. Such Section 4.3 will be divided in four subsections as follows:

(i) Subsection 4.3.1 will explain further processing within the GDPR. The exceptions for further processing will be individualized and analyzed, and in general terms it will explain how is further processing restricted and allowed under the GDPR; (ii) Subsection 4.3.2 will go through Recital 50 of the GDPR, which is an important explanatory recital closely related with the purpose limitation principle and with the compatibility test. A previous version of such Recital will be analyzed and compared with the current version of it within the GDPR; (iii) Subsection 4.3.3 will explain the compatibility test of the purposes for data collection and further processing under the GDPR. It will point out in which cases the compatibility test should be undertaken by the controller, under which rules and according to which criteria it should be implemented.

Finally Section 4.4 will review the data protection novelties within the GDPR, which were not included within the DPD and which are closely related to the preexistence, application and/or interpretation of the purpose limitation principle. The intention of this section is to reveal some of the data protection rights and principles within the GDPR, which are significantly associated with the purpose limitation principle, evidencing the important role and relevance of such principle within the GDPR.

4.1 Reduction of the scope of the purpose limitation principle within the drafts of the GDPR:

The purpose limitation principle was included within the proposal for the GDPR issued by the Commission. It was specifically stated on Article 5 (b) using a wording which was majorly respectful of the previous wording used for Article 6 (b) of the DPD of such proposal. The main difference between Article 5 (b) of the Commission's proposal and Article 6 (b) of the DPD was that the proposal of the Commission for the GDPR did not include in its Article 5 (b) the compatibility considerations for further processing in the specific cases of data processing for historical, statistical or scientific purposes if the Member State has provided appropriate safeguards to do so.

Notwithstanding the above, the purpose limitation principle was in a serious danger of resulting meaningless in the previous drafts of the GDPR, situation that has been pointed out by several

authors[128] and relevant entities.[129] The scenario established in previous versions of the draft for the GDPR, in which further processing for a purpose that is not compatible with the one for which the personal data have been collected,[130] would have represented a serious erosion of the purpose limitation principle, not only mining the data subject's confidence and trust on his/her data processing by the controller, but also eliminating the required foreseeability for the data subject to envisage the purposes and use to be provided to his/her personal data.

The main source of such a disproportionate erosion of the principle of purpose limitation was the drafting of Article 6 (4) of the previous proposal drafts for the GDPR. The text proposed by the Commission on January, 2012 for Article 6 (4) established the following: *"4. Where the purpose of further processing is not compatible with the one for which the personal data have been collected, the processing must have a legal basis at least in one of the grounds referred to in points (a) to (e) of paragraph 1. This shall in particular apply to any change of terms and general conditions of a contract."*[131]

Such norm allowed further processing notwithstanding the fact that the purposes for further processing were not compatible with the original purposes for data collection. This supposed "exception" was applicable in cases in which the processing was covered by at least one of the grounds for lawful processing, except for the specific ground of necessity for the purpose of the legitimate interests pursued by the controller. The draft for this norm emphasizes that this particularly applies to the changes made on the terms and general conditions of a contract.

Furthermore, the drafting of the text as proposed by the General Approach of the Council on June, 2015,[132] established this same Article 6(4), with some relevant changes made to the original proposal made by the Commission, as follows:

(i) Changes the "not compatible" purposes wording to "incompatible" purposes;

[128] Several authors have addressed this matter. See for instance Prins, C, and Moerel L (n 17); or Rauhofer J (n 22).
[129] Article 29 Data Protection Working Party (n 2) 11.
[130] De Hert P and Papakonstantinou V, 'The Proposed Data Protection Regulation Replacing Directive 95/46/EC: A Sound System for the Protection of Individuals' 135.
[131] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final
[132] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) — Preparation of a general approach, Council document 9565/15, 11th June, 2015

(ii) Clarifies that the exception refers to "further" processing;

(iii) States that the controller for the further processing has to be the same one as for the initial data collection;

(iv) Deletes the following phrase which was included on the Commission proposal draft: *"This shall in particular apply to any change of terms and general conditions of a contract*". Such deletion means that for the Council it was not necessary to make such an emphasis on said cases;

(v) Includes the following wording: *"Further processing by the same controller for incompatible purposes on grounds of legitimate interests of that controller or a third party shall be lawful if these interests override the interests of the data subject."*[133]

Practices of data processing as established in such previous drafts of the GDPR in which the application of the purpose limitation principle is disregarded, to the point in which it represents a serious threat to the applicability and effectiveness of such principle, may affect the whole data protection framework.

In the specific case of the previous drafts for the GDPR, evidently the requirement of purpose specification and the requirement of legitimacy were not treated as two separate cumulative requirements. In the proposed wordings of Article 6 (4) the compatibility test can be considered as disregarded in cases in which there is a legal ground for the further processing accordingly to such drafts. This causes the further processing to be *"considered as a new data processing operation disconnected from the original purpose."*[134]

Additionally to the above indicated, the General Approach of the Council for the GDPR draft established even a more harmful and evident threat to the existence and applicability of the purpose limitation principle.[135] It stated as an additional exception, that further processing for incompatible purposes based on grounds of legitimate interests of that controller or a third party was considered lawful in cases in which such interests override the interests of the data subject.

[133] Ibid.
[134] Article 29 Data Protection Working Party (n 2) 11.
[135] Ibid. 36 As explained by the Article 29 Data Protection Working Party this scenario goes against the spirit of the purpose limitation principle and it removes its substance.

Such a lack of an adequate protection of the purpose limitation principle within the GDPR may have caused the increase of data subjects facing abuses of their rights[136] allowing the data controllers to always have a remedy for the lack of compatibility *"by simply identifying a new legal ground for the processing."*[137] This disproportionate erosion of the purpose limitation principle consequently would imply also the erosion of the other data protection principles and rights[138] which are connected and directly related with such purpose limitation principle.

4.2 Scope and meaning of the purpose limitation principle under Article 5 of the GDPR:

The inclusion of the purpose limitation principle within the GDPR, is intended to provide a more harmonized treatment and approach of such principle within the Member States of the European Union, since *"Regulations are direct effect legal instruments"*[139] that regulate matters in the collectivity of the whole European Union, *"in a common manner for all Member States."*[140]

According to Article 5 of the GDPR, which establishes the principles of data protection, personal data shall be "*collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes".*[141] This wording stating the purpose limitation principle is more or less the same as previously indicated within the DPD.[142] However the drafting of Article 5 of the GDPR includes a novelty compared to Article 6 of the DPD, which is the specific indication and denomination of the data protection principles to which each subsection refers to. So in the specific case of Article 5(1)(b) it is expressly denominated as "purpose limitation".

Such specification provides some clarity regarding the comprehension and harmonization of the data protection principles and their terminology. For instance, in the case of the purpose

[136] Cannataci (n 24) 101
[137] Article 29 Data Protection Working Party (n 2) 36
[138] Koning (n 64).The author states that the purpose limitation principle has a conditional function for the principles of data quality, data minimization and accountability, and that its erosion results in the erosion of all related data protection principles.
[139] De Hert P and Papakonstantinou V, 'The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?' (2016) 32 Computer Law and Security Review 182
[140] Ibid.
[141] Article 5(1)(b) of the GDPR.
[142] Ibid; Article 6 (b)

limitation principle, it has been referred to in the past by some authors as the "purpose specification principle"[143] which only corresponds to one of the two components of the whole "purpose limitation principle".[144]

De Hert indicates regarding the relevance of the terminology clarification implemented in the GDPR that *"each principle now carries its official name (in parenthesis, after being laid down in the Regulation's text), a blessing for legal scholars and practitioners who were always uncertain whether the same principles were referred to in the same way by everyone"*[145]

Recital 39 of the GDPR supports Article 5 of the GDPR when establishing that "*the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data*."[146] It also emphasizes that such data must be adequate, relevant and limited to what is necessary for the processing purposes.[147] The content of Recital 39 of the GDPR is mostly the same as previously included within the drafting of Recital 28 of the DPD.

The requirement for the purposes of data processing to be explicit, demands for personal data to be collected for explicit purposes in order to *"ensure that the purposes are specified without vagueness or ambiguity as to their meaning or intent… no later than the time when the collection of personal data occurs".*[148] This characteristic of the purpose limitation is considered as a contribution to transparency and predictability, allowing the clear identification of the limits on how the controllers may use the collected personal data.[149]

In words of the Article 29 Data Protection Working Party, the requirement for the processing purposes to be explicit allows *"to have a common understanding of how the data can be used… In many situations, the requirement also allows data subjects to make informed choices – for*

[143] De Hert (n 139) 185.
[144] Article 29 Data Protection Working Party (n 2) 3. As previously indicated according to such Opinion the purpose limitation principle is composed of two elements which are the "purpose specification" and the "compatible use".
[145] De Hert (n 139) 185.
[146] Recital 39 of the GDPR
[147] Ibid.
[148] Article 29 Data Protection Working Party (n 2) 17
[149] Ibid.

example, to deal with a company that uses personal data for a limited set of purposes rather than with a company that uses personal data for a wider variety of purposes.''[150]

An additional element related with the purpose limitation principle brought by the GDPR is the controller's accountability. According to such new data protection principle the data controller will be responsible for, and must be able to demonstrate compliance with all the personal data processing principles, including the purpose limitation principle.[151] The principle of accountability states as part of the controller's responsibilities when carrying data processing, the controller's obligation to keep records of processing activities, including specifically the purposes of the data processing.[152]

The right for the data subject to be duly informed is also protected within the GDPR.[153] Specifically regarding the purpose limitation principle, it was established that as part of the information to be provided by the controller to the data subject when personal data is collected,[154] the controller must provide the data subject with the purposes of the processing for which the personal data are intended as well as the legal basis for the data processing.[155]

As in the case of the data subject's right to obtain information explained above, there are several other data protection rights and principles that are deeply linked to the purpose limitation within the GDPR. For instance the data subject's right to have access to the purposes of processing,[156] the data subject's right to obtain from the controller the rectification of incomplete personal data taking into account the purposes of data processing,[157] the right of erasure of the data subject's

[150] Ibid.
[151] Ibid; Article 5 (2)
[152] Ibid; Article 30(1)(b)
[153] Ibid; Articles 13 and 14
[154] It is important to note that Article 13 of the GDPR establishes such right to obtain information from the controller when the personal data is being collected from the data subject, specifying that such information shall be provided when the data is obtained. Article 14 of the GDPR establishes the right to obtain information from the controller where personal data have not been obtained from the data subject, and the drafting of such norm clearly intends to avoid indicating that such information shall be provided when the data is obtained, as it is established in Article 13 for data which is been collected form the data subject.
[155] Article 13(1)(c) and Article 14(1)(c) of the GDPR
[156] Ibid; Article 15(1)(a)
[157] Ibid; Article 16

personal data which is no longer necessary in relation to the purposes for which they were collected or otherwise processed.[158]

4.3 Further data processing: the compatibility test and the content of Recital 50 under the GDPR:

4.3.1 Further processing within the GDPR:

According to the Article 29 Working Party, and based on the wording used on the DPD, there is a differentiation between the *"very first processing operation, which is collection, and all other subsequent processing operations"*[159] meaning that any processing following collection would be "further processing". Based on the close similarity of Article 5 (b) of the GDPR and Article 6 (b) of the DPD, it could be said that such notion of further processing is still applicable to the GDPR.

Following the same line, for the similarity on wording regarding further processing, it is relevant to note that the interpretation made by the Article 29 Working Party regarding the wording used to prohibit further processing. Both legal bodies use a double negation rather than a positive statement establishing the requirement of compatibility, when indicating that data cannot be further processed in a manner[160] that is incompatible with the original processing purposes. This basically implies that *"further processing is authorized as long as it is not incompatible."*[161] Then it can also be indicated that the GDPR established a prohibition to further processing in a manner that is incompatible with the original data collection purposes.

With such wording implemented by the legislators, in words of the Article 29 Working Party it seems that *"the legislators intended to give some flexibility with regard to further use."*[162] Such notion of further processing together with the compatibility test may allow having different purposes (original purposes vs further processing purposes) and still the may result compatible,

[158] Ibid; Article 17. The right to erasure is also known as the "right to be forgotten"
[159] Article 29 Data Protection Working Party (n 2) 21.
[160] The main difference between the DPD and the GDPR would be that the GDPR uses the wording "in a manner that" and the DPD uses instead the wording "in a way"
[161] Article 29 Data Protection Working Party (n 2) 21
[162] Ibid.

according to the rules and criteria applicable to the compatibility test for further processing as established within Article 6 (4) of the GDPR.

Additionally, it was established that when the controller intends to further process personal data for a different purpose than the one initially used in order to obtain the personal data ("data collection"), the controller "*shall provide the data subject prior to that further processing with information on that other purpose…"*[163]

The GDPR also included a specification, similar to the one previously stated by the DPD, when indicating that if it is in accordance with Article 89 (1) of the GDPR *"the further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall… not be considered to be incompatible with the initial processing purposes."*[164] Such specific further data processing will be considered according to the GDPR as *"compatible lawful processing operations."*[165] Moreover, it is important to note that the DPD did not include as part of this exception the *"further processing for archiving purposes in the public interest"*[166] which is a novelty included within the GDPR providing a more flexible and wider range for the application of the exception.

In order for this exception to take place regarding the data processing for such specific purposes, in accordance with Article 89(1) of the GDPR processing needs to be subject to appropriate safeguards for the rights and freedoms of the data subject, such as for example data pseudonymisation.[167] The safeguards referred to in Article 89 (1) of the GDPR must ensure that the *"technical and organizational measures are in place"*[168] particularly in order to *"ensure respect of data minimization."*[169] It is important to note that the GDPR is more precise than the DPD regarding the required types and characteristics of the safeguards to be implemented.

Furthermore, the GDPR includes a particular difference regarding the specific case of personal data processing for the purposes of scientific research. Recital 33 of the GDPR highlights that

[163] Articles 13(3) and 14(4) of the GDPR
[164] Ibid; Article 5 (1)(b)
[165] Ibid; Recital 50
[166] Ibid; Article 5 (1)(b).
[167] Ibid; Article 89(1)
[168] Ibid.
[169] Ibid.

when processing data for scientific research it is not always possible to fully identify the purpose for processing at the time of data collection. In such cases, data subjects should be *"allowed to give their consent to certain areas of scientific research…to the extent allowed by the intended purpose."*[170]In such specific cases the GDPR compensates the lack of confident knowledge of the purposes for collection, with the consent provided by the data subjects to certain areas of scientific research.

4.3.2 Recital 50 of the GDPR:

The element of "compatible use" which is one of the two components of the principle of purpose limitation, is however not clearly assessed according to Recital 50 of the GDPR which states that personal data processing "*for purposes other than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected*."[171]. However, the Recital emphasizes that in such case, it will not be required a *"legal basis separate from that which allowed the collection of the personal data."*[172]

Conversely according to this Recital, when the processing is not compatible with the initial purposes used for the personal data collection, then the controller will need to have a new legal basis, different from the initial one, to the effects of proceeding with the new personal data processing. However despite of being confusing, this wording seems to imply that further processing based on incompatible purposes still may be legal if there is a legal ground under Article 6 of the GDPR. Such misleading language is apparently due to a remainder of the wording implemented within the GDPR draft proposal by the General Approach of the Council, in which in its Recital 40 (which is the Recital that served as the base for Recital 50 of the current GDPR) indicates the following:

"The processing of personal data for other purposes than the purposes for which the data have been initially collected should be only allowed where the processing is compatible with those

[170] Ibid; Recital 33
[171] Ibid; Recital 50
[172] Ibid.

purposes for which the data have been initially collected. In such case no separate legal basis is required other than the one which allowed the collection of the data."[173]

It is important to note that such text of Recital 40 of the General Approach of the Council was based on the wording of Article 6 (4) of such General Approach of the Council, in which further processing for incompatible purposes was allowed if there was a legal ground for such further processing as previously analyzed in this thesis. So Recital 40 was clarifying that when there was compatibility of the purposes (for collection and further processing) then no other separate legal basis that the one allowing the data collection was required for such processing. Such exact wording was kept for Recital 50, however the drafting of Article 6 (4) was modified in the finally approved GDPR, meaning that such clarification is not applicable to the current notion of compatibility for further processing as stated in Article 6 (4) of the GDPR.

According to the above indicated, it seems that the wording of Recital 50 was not duly modified accordingly to the finally approved text of Article 6 (4) of the GDPR. Based on such Article 6 (4) of the GDPR a valid and reasonable interpretation of Recital 50 would be to conclude that when there is a confirmed compatibility of the purposes (collecting purposes and further processing purposes) then such further processing may be performed based only in the initial legal ground used for the data collecting, and no additional legal ground has to be allocated by the controller to the further processing of such personal data.

4.3.3 The compatibility test of the purposes for data collection and further processing under the GDPR:

As indicated in Section 4.3.2 above, the GDPR included the possibility of further processing in some specific cases. Limitations on further processing have always being objected by the data processing industry[174] since such limitations have represented a hindrance against using previously obtained personal data for other purposes different than the initial processing or collecting purposes. Additionally, the fast development of big data[175] and the Internet of Things

[173] Proposal for a Regulation of the European Parliament and of the Council (n 132); emphasis added.
[174] De Hert (n 130) 134
[175] Notwithstanding such development of Big Data, for authors such as Zarsky the existence of Article 22 of the GDPR represents an evident example of the GDPR's rejection of the Big Data revolution showing a *"deep distrust towards these automated processes"* (Zarsky (n 20) 1006-1008).

(IoT) has also added some pressure coming from the processing industry seeking the flexibility or erosion of the purpose limitation principle,[176] particularly regarding further processing of personal data.

For such purposes the GDPR has reinforced the possibility of further processing in cases in which the data controller confirmed the compatibility of the processing purposes. It states that *"processing of personal data for purposes other than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected."*[177]

In order for the data controller to confirm the existence of compatibility between the processing purposes (initial purposes for collection and further processing purposes), it is required for the controller to perform a compatibility test, which is intended to be an accurate review of several elements composing the initial data processing, the further processing, and the relationship between the controller and the data subject.

Furthermore, the data controller is accountable to comply with the verification of several criteria as part of the compatibility test in order to be able to ascertain if processing for another purpose is compatible or not with the initial processing purposes. For instance, the controller needs to verify *"any link between the purposes for which the personal data have been collected and the purposes of the intended further processing"*[178] as well as *"the possible consequences of the intended further processing for data subjects."*[179]

Article 6.4 of the GDPR was intended to regulate further processing and the compatibility test. It is not clear why such topic was finally included within Article 6 which covers the lawfulness of

[176] Prins, C, and Moerel L (n 17). The authors have indicated regarding the approach on the previous drafts of the GDPR in which further processing by the same data controller was being allowed even if the further purpose was incompatible with the initial purpose for processing *"if the legitimate interests of that controller or a third party override the interests of the data subject", labeling such measure as the "only feasible way to guarantee protection given that is much better suited to deal with developments such as the Internet of Things (IoT) and big data"* concluding that *"a test based on the legitimate interest is better suited in today's data-driven society than the current test based on the initial purpose for data collection and whether further processing is compatible with such initial purpose."*

[177] Recital 50 of the GDPR.

[178] Ibid; Article 6(4)(a)

[179] Ibid; Article 6(4)(d)

processing, rather than within Article 5 in which further processing is limited.[180] The first paragraph of Article 6 (4) included a particular exception from the compatibility test for further processing based on two specific legal grounds, which are:

(i) when the data subject has given his/her consent for such further processing; and

(ii) when the processing is based on Union or Member State law *"which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1)."* [181]

In such cases, the controller is allowed to further process the personal data "*irrespective of the compatibility of the purposes."*[182] The intended purpose of having both of the above indicated exemptions responds respectively to achieving a reasonable balance between the controller's interest and the rights and freedoms of the data subject, and the necessity of excluding certain matters of public interest nature. However, it is important to note that Recital 50 of the GDPR is precisely a Recital not an Article of the GDPR, meaning that from the strictly legal perspective it is not binding. It functions like a tool for clear understanding and uniform interpretation of the Articles within the GDPR.

Notwithstanding the above said, according to Article 6 (4) consent clearly can be used for further data processing, even for incompatible purposes. The problem with this provision is that it threats the required separation of legitimacy and purpose specification, and their consideration as different cumulative requirements. However, even if it clashes with the notion of separation between the grounds for lawful processing and the purpose specification, the exception is required in order to allow further processing in cases in which the parties are both positive on performing such further processing, despite of the lack of compatibility of the purposes of collection and the purposes for further processing.

Such approach will allow the adaptation of further processing operations to new technologies, and also to comply with new emerging interests of both of the involved parties. What is

[180] De Hert (n 139) 186. The authors considered that apparently the reason why such topic was included within Article 6 instead of Article 5 of the GDPR, is that the *"Commission's initial structure was followed by the Council and the Parliament"*
[181] Article 6(4) of the GDPR.
[182] Ibid; Recital 50

important to note here, is that this major relevance that consent has acquired through the GDPR, must be hand by hand with safeguards that may ensure the data subject giving voluntarily his/her consent for further processing operations, and to actually acknowledge and understand those further processing purposes.

In general terms, Article 23 (1) allows the Member States to restrict through a legislative instrument the scope of the obligations and rights covered through several articles of the GDPR, including Article 5. However such restriction is applicable only in cases in which the provisions on such legislative instrument *"correspond to the rights and obligations provided for in Articles 12 to 22"*[183] of the GDPR. Although it is not completely clear from the implemented wording, it seems that such provision means that through such proceeding the data protection principles (including the purpose limitation principle) may be restricted by the Member States but only when involved the rights and obligations established in Articles 12 to 22 of the GDPR.

If applicable, such restriction needs to be respectful of the *"essence of fundamental rights and freedoms."*[184] It does not specify who should be the subject of such fundamental rights and freedoms, meaning that it has to be interpreted in a broad manner covering the fundamental rights and freedoms of any one who could be affected through such restriction. Additionally, as previously indicated the restriction needs to correspond to a measure which is necessary and proportionate in a democratic society in order to safeguard a restrictive list of objectives.

The objectives covered in Article 23(1) correspond to *"important objectives of general public interest.*"[185] They encompass aspects that for instance involve matters of security, defense, prevention and prosecution of criminal offences, important economic or financial interest of the Union or Member State, enforcement of civil law claims, protection of the data subject or the rights and freedoms of others etc.

The last section of Article 6 (4) of the GDPR provides a list of guidelines or criteria that the controller shall take into account for further processing based in compatibility as an exemption to

[183] Ibid; Article 23 (1)
[184] Ibid.
[185] Ibid; Recital 50

the purpose limitation principle.[186] Such criteria are intended to provide the controller with the parameters to make the required compatibility considerations and evaluations. Following these criteria the controller must determine case by case[187] which further processing purposes should be considered as compatible with the initial processing purposes.

It is important to note that such list of applicable criteria to be taken into account by the data controller, are "inter alia" and as such it is just an indicative list, which means that *"a controller might choose to take into consideration additional criteria."*[188] Furthermore even if these applicable criteria to determine compatibility serve as a limitation to the controller's discretion and as margin for considerations regarding the compatible purposes of processing, at the end of the day it is still up to the controller's decision[189] to determine such compatibility.

Therefore, the GDPR provides to the data controller not only the possibility to further processing in the exempted cases, but also the discretion under certain applicable criteria, to evaluate and decide if the purposes for further processing are compatible or not with the initial data processing purposes.[190] As previously indicated, according to Article 6 (4) of the GDPR in order to proceed with such compatibility test, the controller must take into account the following:[191]

(i) any links between the initial and the further purposes for processing;

(ii) the context of the data collection or processing, providing particular emphasis to the relationship between the controller and the data subject, especially taking into account the "*reasonable expectations of data subjects based on their relationship with the controller"*[192] regarding the further use of their personal data;

---

[186] De Hert (n 139) 186. The authors consider that this exemption is a *"realistic approach in a processing era of among others, ubiquitous computing, big data and the internet of things"*

[187] Article 29 Data Protection Working Party (n 2) 21. The Article 29 Working Party indicated that *"the fact that the further processing is for a different purpose does not necessarily mean that it is automatically incompatible: this needs to be assessed on a case-by-case basis…"*

[188] Ibid.

[189] De Hert (130) 135. The authors indicated regarding the compatibility criterion aspects within the draft for the GDPR, that *"in practice data controllers shall decide alone what is "compatible" and what is not, and it shall be up to individuals to take actions to challenge that decision"*

[190] Ibid. The authors state that it is up to the controller, according to the principle of accountability, to make the necessary evaluations to determine compatibility of the initial purposes with the purposes for further processing.

[191] Article 6(4) (a),(b),(c),(d) and (e) of the GDPR.

[192] Ibid; Recital 50

(iii) the nature of the personal data, providing particular emphasis to special categories of personal data according to the GDPR;

(iv) the possible consequences for the data subjects in the eventuality of performing the further processing of personal data;

(v) the existence of appropriate safeguards such as for example encryption or pseudonymisation, which must be present "*in both the original and intended further processing operations"*[193]

The origin of these criteria is clearly the Article 29 Working Party's Opinion 03/2013. The above indicated criteria structured in Article 6 (4) of the GDPR, corresponds to the same four criteria for the compatibility test developed by the Article 29 Working Party on such opinion. Additionally to these criteria for the compatibility test, if the controller determines the compatibility of the processing purposes, then the controller must "*provide the data subject prior to that further processing with information on that other purpose and other necessary information."*[194]

This is a very important obligation, because it is intended to guarantee the data subject's right to be informed and have knowledge of the processing purposes of his/her personal data. This disposition provides the data subject foreseeability on how his/her personal data will be used and for which purposes. It also provides the data subject with the possibility if applicable, of exercising his/her right to object to the further processing or challenging the compatibility test made by the controller to determine the compatibility between the initial and the further processing purposes.

The purpose limitation principle cannot ignore new data processing practices such as big data and profiling. Consequently, the GDPR has to provide the tools to allow such practices without disregarding the data subjects' right to data protection and to have certain level of control on their personal data processing, such as the one provided by the purpose limitation principle. In this sense, providing data controllers with the possibility to further processing in cases in which the compatibility test results positive regarding the compatibility of the further processing purposes with the initial processing purposes, is a necessary tool in order to provide a reasonable

[193] Ibid.
[194] Ibid; Recital 61. See also Article 13(3).

path to the implementation of big data or profiling technologies that may favor the interests of the involved parties, meaning data controller and data subject.

Zarsky provides an example of the problem that the purpose limitation principle may represent to big data analysis, when indicating that in order to *"comply with the purpose specification rule, entities striving to engage in Big Data analysis will need to inform their data subjects of the future forms of processing they will engage in … and closely monitor their practices to assure they did not exceed the permitted realm of analysis."* [195] According to the author, such requirements might result costly, difficult and even impossible to achieve for such entities and in general terms, he concludes that the purpose specification clearly clashes with the prospect of Big Data analysis. However, the author also foresees a specific feature included within the GDPR that may enable Big Data analysis, which is the notion of compatibility as previously explained.

4.4 Data protection novelties within the GDPR related to the application and/or interpretation of the purpose limitation principle:

There are some new relevant inclusions within the GDPR (comparing it with the DPD) which are associated and related with the purpose limitation principle. For instance, the implementation of new principles and rights, such as the principle of transparency,[196] the principle of accountability,[197] and the right to be forgotten,[198] among others.

The identification of such novelties within the GDPR will provide a notion of the existing interdependence of the purpose limitation principle with other data subject's rights and data protection principles. It will help to answer the question on which is the current relevance and role of the purpose limitation principle within the GDPR as a whole. It will also confirm that most of these data subject's rights and data protection principles somehow depend on the notion of purpose limitation on personal data processing, and that in general terms the purposes for data

[195] Zarsky (n 20) 1006-1008.
[196] Article 5(1)(a) of the GDPR.
[197] Ibid; Article 5(2)
[198] Ibid; Article 17 and Recitals 65 and 66

processing are closely related with several core elements of the collection and processing of personal data.[199]

In this sense, it is important to note that the purpose limitation principle is not a "solitary" principle, but instead a principle which is part of the whole data protection framework, and as such it is related with several other data protection elements. It could be said that its main content is currently developed within Article 5 of the GDPR, but its effects and application are clearly visible all through the GDPR, serving as a functional element of other data protection principles and rights. Consequently, the purpose limitation is an element intrinsically present in other data protection principles and rights established within the GDPR.

The following subsections will list some of such data subject's rights and data protection principles, and will provide a brief explanation regarding how each of them are related with the purpose limitation principle.

4.4.1 The principle of accountability:

According to Article 5(2) of the GDPR, the principle of accountability is understood as the responsibility of the controller to comply with, and to be able to demonstrate compliance with, the rest of principles and data protection safeguards established in Article 5(1). This clearly includes the controller's respect and compliance of the purpose limitation principle. But since the principle of accountability not only requires the controller to comply, but also to be able to demonstrate such compliance, the controller is also responsible to demonstrate respect and compliance of the purpose limitation principle.

Accountability represents an additional and formal duty on the data controller's processing operations and responsibilities. It reinforces the other principles of data processing, establishing the data controller's obligation to comply with such principles and to be able to demonstrate such compliance, though favoring the controller's respect of the purpose limitation principle.

[199] Roos A, 'Core Principles of Data Protection Law' (2006) 39 Comparative and International Law Journal of Southern Africa 111. The author lists for instance aspects such as the amount and the nature of the data that may be collected, the length of time the data may be kept, and the further processing that may be done.

4.4.2 Right to be forgotten:

The right to be forgotten was included as a specific right within the GDPR denominating it as the "right to erasure" or "right to be forgotten."[200] It establishes the right of data subjects to obtain from data controllers and under certain circumstances,[201] the erasure of personal data concerning such data subject, when any of the grounds stated in Article 17(1) are applicable.[202]Although it was stated as a specific and separate right under the GDPR, it is important to note that the DPD already introduced some notions and traces of this right.[203] The existence and applicability of this right under the DPD was made clear through the Google Spain decision.[204]

It is specifically relevant for the purpose limitation principle, the fact that the right to be forgotten is applicable when the data subject's *"personal data is no longer necessary in relation to the purposes for which they were collected or otherwise processed"*.[205] Such scenario has to be analyzed together with the principle of purpose limitation[206] and the principle of storage limitation,[207] since both of such principles establish a limitation to an *"indiscriminate and endless collection of the data and are focused on the different parameters concerning the length of the time of retention and the processing purposes"*[208]

The above mentioned principle of storage limitation as well as the scenario established under Article 17(1)(a) for the application of the right to be forgotten, have a "common denominator". Such common denominator is the previous application of the purpose limitation principle when processing the personal data. They suppose the existence and application of the purpose

[200] Article 17 of the GDPR
[201] Ibid; Article 17(3). Such article establishes exceptions to the applicability of the right to be forgotten when processing is necessary for: (i) exercising the right of freedom of expression and information (Article 17(3)(a); (ii) compliance with a legal obligation of the controller or for the performance of a task carried out in the public interest or in the exercise of an official authority vested in the controller (Article 17(3)(b) (iii) reasons of public interest in the area of public health (Article 17(3)(c); (iv) archiving purposes in the public interest, scientific or historical research purposes or statistical purposes (Article 17(3)(d); (v) for the establishment, exercise or defense of legal claims (Article 17(3)(e).
[202] Ibid.
[203] Article 12(b) of the DPD
[204] Case C-131/12 Google Spain v. Agencia Española de Protección de Datos [2014] CJEU.
[205] Article 17(1)(a) and Recital 65 of the GDPR
[206] Ibid; Article 5(1)(b)
[207] Ibid; Article 5(1)(e)
[208] Mantelero A, 'The EU Proposal for a General Data Protection Regulation and the Roots of the Right to Be Forgotten' (2013) 29 Computer Law and Security Review 229

limitation principle, and that according to such principle, the purposes for data processing were previously defined by the controller in a specified and explicit manner.

4.4.3 The principle of transparency:

The principle of transparency *"establishes an obligation for the controller to keep the data subjects informed about how their data are being used."*[209] The principle of transparency was added to the GDPR as a novelty, even as indicated before in this chapter, the bases and notion of such principle were already developed through the DPD and has been particularly enrichened by the court-cases of the ECtHR.[210]

This principle, as indicated by the Article 29 Working Party, has a strong connection with purpose specification,[211] and goes "hand by hand" with the lawfulness and fairness of data processing. It also has a strong link with the requirement of foreseeability and predictability[212] of the processing purposes, and the data subject's right to know and be informed on the purposes and uses of his/her personal data. All such elements are very important for the purpose limitation principle, since one of the goals that are meant to be achieved through such principle, is to provide confidence to the data subject regarding the processing of his/her personal data, providing the required level of trust between the data controller and the data subject.

The principle of transparency is also closely related with the data subject's right to have access to information and obtain the required communications[213] related to the data processing, concerning *"in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing."*[214]

---

[209] European Union Agency for Fundamental Rights (n 89) 74.
[210] See for instance Haralambie v. Romania, n. 21737/03, ECtHR 2009; or K.H. and Others v. Slovakia, n. 32881/04, ECtHR 2009.
[211] Article 29 Data Protection Working Party (n 2) 13.
[212] Ibid. The Article 29 Working Party indicates in regards of predictability that *"if a purpose is sufficiently specific and clear, individuals will know what to expect"*
[213] Recital 58 of the GDPR establishes that *"The principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used…"* See also Recital 39 and Article 12 of the GDPR.
[214] Ibid; Recital 39

This principle reinforces the relevance of the purpose limitation principle requiring the purposes of data processing to be explicit, legitimate and determined before collection.[215] It could probably be said that there is no other personal data protection principle so closely related to the principle of purpose limitation. The purpose limitation principle has an essential role on the comprehension and delimitation of the principle of transparency, and vice versa.

According to all the above indicated, it is important to note the existence of other data protection principles and rights within the GDPR, which are closely related with the purpose limitation principle in some cases almost in a symbiotic manner. All of these data protection rights and principles have certain level of dependence with the purpose limitation principle. In most cases their functionality and applicability actually depends on the whole notion of purpose limitation.

Those interrelated principles and rights reinforce the relevance and value of the purpose limitation principle within the legal framework for the protection of personal data. It also justifies the inclusion of this principle's notion within the fundamental right to the protection of personal data in the Charter, and consequently its inclusion within the GDPR.

Based on the close relation of the purpose limitation principle with other key elements of the data protection system within the GDPR, it will not be "going too far" to assert that the purpose limitation principle is still a core and relevant principle of data protection within the legal framework of the European Union. A serious degradation or relaxation of this principle under the GDPR would have been a major loss for the data subjects' rights, but also to the whole data protection system, which has been designed taking into account the existence and application of the purpose limitation principle.

Conclusion:

The previous drafts of the GDPR certainly implemented a reduction of the scope of the purpose limitation principle through a significant erosion or degradation of such principle. Particularly, the wording used on Article 6(4) of such drafts to the GDPR regarding the compatibility test for further data processing can be labelled as an "open door" to further processing, regardless of the

[215] Ibid.

purposes being compatible between each other or not. It allowed further processing in cases in which there was a new legal ground for such further processing (excluding processing based on the legitimate interests of the data controller).

This scenario represented a serious and substantial threat to the purpose limitation principle, eroding the essence of such principle and turning it into a "ghost" of what it is intended to be within the data protection legal framework. What was supposed to be an exception (further processing) was turned into the general rule. Under such circumstances, several authors wrote about the visibly coming "death" or "end" of the purpose limitation principle, using titles that directly suggest such future.[216]

Furthermore, the text of the current Recital 50 under the GDPR has some remainders of such threating scenario for the purpose limitation principle as depicted within the previous drafts of the GDPR. Some parts of such recital do not match the current regulation under the GDPR for further processing and for undertaking the compatibility test. An example of the above would be the confusing language implemented in Recital 50 in which seems to imply that further processing based on incompatible purposes still may be legal if there is a legal ground for processing under Article 6 of the GDPR.

Notwithstanding the above, the current GDPR seems to follow the same line regarding the treatment and notion of the compatibility test for further processing, as previously developed and recommended by the Article 29 Working Party in its Opinion 03/2013. In a more structured and detailed way, the GDPR included through its Article 6 (4) the main criteria for the compatibility test as proposed by the Article 29 Working Party within its Opinion 03/2013.

This approach also provides the required level of flexibility for the compatibility test to be performed in order to determine if further processing is allowed. It provides a practical solution towards the new types of data processing technologies recently developed, such as "big data" or the "internet of the things." Moreover, this approach is also susceptible of adapting and accommodating to future data processing technologies or practices, respecting the core and goals of the purpose limitation principle.

[216] See for instance Prins, C, and Moerel L (n 17); Rauhofer J (n 22); Cannataci (n 24), or Brouwer E (n 25).

For the reasons explained above, it is reasonable to indicate that the Article 29 Working Party Opinion 03/2013 is still a current instrument and provides a valuable reference regarding the interpretation of the purpose limitation principle according to the GDPR.

Additionally, it is important to note the major relevance that data protection, and so the purpose limitation principle as well, have acquired through the implementation of the Charter. The inclusion of such an important principle within the fundamental right to data protection demands respect and an effective implementation, under any current or future regulation on the matter. Notwithstanding the above, as indicated through this thesis the purpose limitation principle may be subject to reasonable levels of erosion or degradation. In this way, a fair balance of the interests of the data controller and the data subjects may be achieved.

The existence of some novelties included within the GDPR, keep a close relationship with the purpose limitation principle, reinforcing the notion of such principle and the reasons for its existence and implementation. Most of these data protection principles and rights actually depend on the purpose limitation principle per their close association to the notion of purpose limitation, or some particular aspects of it, such as purpose specification. This is an evident sign of the important role and relevance of the purpose limitation principle within the GDPR, and in general terms for the Member States forming part of the European Union. Any significant erosion of the purpose limitation principle will consequently carry the significant erosion of such other interrelated data protection principles and rights.

Another issue worthy to point out, is regarding the exemption of the compatibility test provided to two legal grounds for lawful processing according to Article 6 (4) of the GDPR. This refers to the cases of further processing based on the data subject's consent and on a Union or Member State law with the specifics required according to the GDPR. Such high level of flexibility responds respectively to achieving a reasonable balance between the controller's interest and the rights and freedoms of the data subject in the first case, and the necessity of excluding certain matters of public interest nature in the second case.

This provision threats the separation between legitimacy and purpose specification, and their consideration as different cumulative requirements. In the opinion of the author of this thesis, even if it clashes with the notion of separation and differentiation between the grounds for lawful

processing and the purpose specification, the exception is reasonable and required in order to allow further processing in cases in which the parties are both positive on performing such further processing, despite of the lack of compatibility of the purposes of collection and the purposes for further processing.

This measure implemented through the GDPR, will allow the adaptation of further processing operations to new technologies, and also to comply with new emerging interests of both of the data controller and the data subject. It will also carry new challenges for the future since with such change "consent" may have acquired more relevance than the other legal grounds for data processing. This means that data processing operations based on the data subject's consent may require particular safeguards that may ensure the data subject giving voluntarily his/her consent for further processing operations, and to actually acknowledge and understand those further processing purposes. Only the further day to day experiences of data controllers and data subjects, acquired once the GDPR is effectively implemented, will reveal if such safeguards are required or not.

Furthermore, it could be asserted that the DPD is to the GDPR what a son or daughter is to a parent. The DPD represents the past and the GDPR the coming future of data protection within the European Union. Their influence on data protection legal frameworks all around the world is undeniable,[217] and both can be considered as two of the most relevant legal sources regulating data protection.[218] There are remarkable similarities between the DPD and the GDPR, especially regarding the direct legal treatment provided to the purpose limitation principle within both frameworks. This means that the text of Article 6(1)(b) of the DPD has several coincidences to the text of Article 5(1)(b) of the GDPR, which are only differentiated by the inclusion within Article 5(1)(b) of the GDPR of an express exemption of incompatibility with the initial purposes for the *"further processing of personal data for archiving purposes in the public interest."*[219]

[217] De Hert (n 139) 194. The authors state that the DPD is the "international standard against which all data protection initiatives in and out of Europe were judged" and that its basic components "are in one way or the other addressed in all data protection instruments around the globe"

[218] Zarsky (n 20) 995. The author states that the impact of the GDPR will "most likely be profound" and that it is perhaps "the most comprehensive and forward looking piece of legislation to address the challenges facing data protection in the digital age."

[219] Article 5(1)(b) of the GDPR.

However as demonstrated through this thesis, it is important to note that there are also remarkable changes, particularly regarding further data processing and the compatibility test between the purposes for collection and the purposes for further processing. The main sources of such differences are Recital 50 and especially Article 6 (4) of the GDPR.

Moreover, despite of the pressure coming from the data processing industry to diminish the role of the purpose limitation within data protection, it is still a necessary and useful principle of data protection. It provides a reasonable balance for the interests of data controllers and data subjects. But it also provides the required foreseeability and predictability for both the data controller and the data subject to obtain a clear common understanding of how the subject's data will be processed and used by the controller. The GDPR has achieved what seems to be a middle point when safeguarding the interests of both parties involved within data processing, allowing further processing in exceptional cases, and in cases in which the compatibility test between purpose for collection and purpose for further processing results positive.

It may be also concluded that the purpose limitation principle cannot ignore new data processing technologies and practices such as big data, profiling and the internet of the things. For such reason, the GDPR provides the tools to allow such practices without disregarding the data subjects' right to data protection and to have certain level of control on their personal data processing, as intended through the purpose limitation principle. Per its functionality and flexibility, the compatibility test is a necessary tool in order to provide a reasonable path to the implementation of big data or other profiling technologies that may adapt and respect the requirements of purpose limitation and at the same time may favor the interests of the data controller and data subject.

Bibliography

Books:

- Brouwer E, 'Legality and Data Protection Law: The Forgotten Purpose of Purpose Limitation' in Besselink LFM, Pennings F and Prechal S (eds) The Eclipse of the Legality Principle in the European Union (Kluwer, 2010) 273

- Cavoukian A, ‘Evolving FIPPs: Proactive Approaches to Privacy, Not Privacy Paternalism’ in Gutwirth S, Leenes R, and De Hert P (eds) Reforming European Data Protection Law 20 (2015) 293

- Chynoweth P, ‘Legal Research’ in A. Knight and L. Ruddock (eds) Advanced Research Methods in the Built Environment (Blackwell Publishing Ltd, 2008) 28

- Colonna L, ‘Data Mining and Its Paradoxical Relationship to the Purpose Limitation Principle’, in Gutwirth, S, Leenes, R and de Hert P (eds) Reloading Data Protection: Multidisciplinary Insights and Contemporary Challenges (2014) 299

- De Hert P and Gutwirth S, ‘Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action’ in Gutwirth S, Poullet Y, De Hert P, de Terwangne C and Nouwt S (eds) Reinventing Data Protection? (Springer, 2009) 3

- Forgó N, Hänold S and Schütze B, ‘The Principle of Purpose Limitation and Big Data’ in Corrales M, Fenwick M and Forgó N (eds.) New Technology, Big Data and the Law (Springer, 2017) 17

- Rodotà S, ‘Data Protection as a Fundamental Right’ in Gutwirth S., Poullet Y., De Hert P., de Terwangne C. and Nouwt S. (eds) Reinventing Data Protection? (Springer, 2009) 77

- Szekely I, ‘The Right to Forget, The Right to be Forgotten – Personal Reflections on the Fate of Personal Data in the Information Society, in Gutwirth S, Leenes R, De Hert P and Poullet Y (eds) ‘European Data Protection: In Good Health?’ (Springer, 2012) 347

Articles and Papers

- Asunción E, ‘The Business of Personal Data: Google, Facebook, and Privacy Issues in the Eu and the Usa’ (2017) 7 International Data Privacy Law 36

- Bergkamp L, ‘EU Data Protection Policy - The Privacy Fallacy: Adverse Effects of Europe’s Data Protection Policy in an Information-Driven Economy’ (2002) 18 Computer Law and Security Report 31

- Birnhack M D, ‘The EU Data Protection Directive: An Engine of a Global Regime’ (2008) 24 Computer Law and Security Report 508

- Cannataci J A and Bonnici J P M, ‘The End of the Purpose-Specification Principle in Data Protection?’ (2010) 24 International Review of Law, Computers and Technology 101

- De Hert P and Papakonstantinou V, “The Proposed Data Protection Regulation Replacing Directive 95/46/EC: A Sound System for the Protection of Individuals” (2012) 28 Computer Law and Security Review 130

- De Hert P and Papakonstantinou V, ‘The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?’ (2016) 32 Computer Law and Security Review 179

- Hallinan D Friedewald M and McCarthy P, ‘Citizens’ Perceptions of Data Protection and Privacy in Europe’ (2012) 28 Computer Law and Security Review 263

- Mantelero A, ‘The EU Proposal for a General Data Protection Regulation and the Roots of the Right to Be Forgotten’ (2013) 29 Computer Law and Security Review 229

- Petković M, Prandi D and Zannone N, ‘Purpose Control: Did You Process the Data for the Intended Purpose?’ (2011) 6933 Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 145

- Poullet Y, ‘EU Data Protection Policy. The Directive 95/46/EC: Ten Years after’ (2006) 22 Computer Law and Security Report 206

- Poullet Y, ‘Data Protection Legislation: What is at Stake for our Society and Democracy?’ (2009) 25 Computer Law and Security Review 211

- Rauhofer J, ‘Look to Yourselves, That We Lose Not Those Things Which We Have Wrought, What Do the Proposed Changes to the Purpose Limitation Principle Mean for Public Bodies Rights to Access Third-Party Data?’ (2014) 28 International Review of Law, Computers & Technology 144.

- Roos A, 'Core Principles of Data Protection Law' (2006) 39 Comparative and International Law Journal of Southern Africa 103

- Zarsky T Z, 'Incompatible: The GDPR in the Age of Big Data' (2017) 47 Seton Hall Law Review 95

Online Articles and Papers

- Coudert F, Dumortier J and Verbruggen F, 'Applying the Purpose Specification Principle in the Age of "big Data": The Example of Integrated Video Surveillance Platforms in France' (2012) ICRI Working Paper Series, accessed 15 March 2018 via http://ssrn.com/abstract=2046123

- Koning M E, 'Purpose Limitation' in van Lieshout M, and Hoepman J H (eds), P.I.Lab 4 years later 139; accessed 19 March 2018 via https://merelkoning.nl/academic-work

- Moerel L and Prins C, "On the death of purpose limitation" (2015) International Association of Privacy Professionals; accessed 21 November 2017 via https://iapp.org/news/a/on-the-death-of-purpose-limitation/

Other Online Materials

- European Union Agency for Fundamental Rights, 'Handbook on European Data Protection Law (2014); accessed 8 February 2018 via https://www.echr.coe.int/Documents/Handbook_data_protection_Eng.pdf

Opinions and Reports by EU Institutions

- Article 29 Data Protection Working Party 00569/13/EN WP 203, Opinion 03/2013 on purpose limitation adopted on 2 April 2013

- Article 29 Data Protection Working Party 844/14/EN WP 217, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC adopted on 9 April 2014.

- European Data Protection Supervisor, Opinion on the communication from the Commission to the European Parliament and the Council - 'Overview of information management in the area of freedom, security and justice', C 355/03 30 September 2010.

- Organisation for Economic Cooperation and Development (OECD): Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, 23 September 1980.

Lectures and Presentations

- Moerel L, 'Big Data Protection: How to Make the Draft EU Regulation on Data Protection Future Proof', Lecture delivered during the public acceptance of the appointment of professor of Global ICT Law at Tilburg University (14 February 2014) accessed 16 May 2018 via https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3126164

European Legislation and Related Texts:

- Charter of Fundamental Rights of the European Union (2000/C 364/01), 18 December 2000

- Convention for the Protection of Human Rights and Fundamental Freedoms, 4 November 1950

- Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28 January 1981

- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

- European's Commission Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), European Commission COM(2012) 11 final, 2012/0011 (COD), 25 January 2012

- European Council's text on the Commission Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation); Preparation of a general approach, Council document 9565/15, 11 June 2015

- European Parliament legislative resolution on the Commission Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) COM(2012) 11 - 2012/0011 (COD) 12 March 2014

- 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)

Case Law

European Court of Human Rights

- Amann v. Switzerland App No. 27798/95 (ECtHR, 16 February 2000)

- Armoniene v. Lithuania App No. 36919/02 (ECtHR, 25 November 2008)

- Biriuk v. Lithuania App No. 23373/03 (ECtHR, 25 November 2008)

- Haralambie v. Romania App No. 21737/03 (ECtHR 27 October 2009)

- K.H. and Others v. Slovakia App No. 32881/04 (ECtHR, 28 April 2009)

- Kruslin v. France App No. 11801/85 (ECtHR, 24 April 1990)

- Leander v. Sweden App No. 9248/81 (ECtHR, 26 March 1987)

- L.L. v. France App No 7508/02 (ECtHR 10 October 2006)

- Malone v. The United Kingdom App No. 8691/79 (ECtHR, 26 April 1985)

- Rotaru v. Romania App No. 28341/95 (ECtHR, 4 May 2000)

- S. and Marper v. the United Kingdom App No. 30562/04 30566/04 (ECtHR, 4 December 2008)

- Z v. Finland App No. 22009/93 (ECtHR, 25 February 1997)

European Court of Justice

- Case C-131/12 Google Spain v. Agencia Española de Protección de Datos (2014)

- Joined Cases C-92/09 and C-93/09 Volker und Markus Schecke and Eifert v. Land Hessen (2010)

- Joined Cases C-293/12 and C-594/12 Digital Rights Ireland v. Minister for Communications, Marine and Natural Resources and others (2014)