REVEAL

FP7-610928

REVEALing hidden concepts in Social Media

Deliverable D1.2

Legal /regulatory requirements analysis

Editor(s):	Joyce Verhaert, Aleksandra Kuczerawy, Prof. Peggy Valcke
Responsible Partner:	KU-Leuven
Status-Version:	Final – v1.1
Date:	05/05/2014
EC Distribution:	Public

Project Number:	FP7-610928
Project Title:	REVEAL

Title of Deliverable:	Legal /regulatory requirements analysis
Date of Delivery to the EC:	05/05/2014

Workpackage responsible for the Deliverable:	WP1 - User Requirements and Regulatory Framework
Editor(s):	Joyce Verhaert, Aleksandra Kuczerawy, Prof. Peggy Valcke
Contributor(s):	ATC, DW, INTRASOFT
Reviewer(s):	ATC
Approved by:	All Partners

Abstract:	The aim of this deliverable is to provide an outline and analysis of the legal framework for the REVEAL project. Deliverable D1.2 focuses on the topic of privacy and data protection. This is a crucial aspect of achieving legally compliant project result.
Keyword List:	Data protection, privacy, controller, processor, applicable law, Data Protection Directive, Data Protection Regulation

DOCUMENT DESCRIPTION

Document Revision History

Version	*Date*	*Modifications Introduced*	
		Modification Reason	*Modified by*
v0.2	07/04/2014	Creation of the document structure	KU-Leuven
v0.3	11/04/2014	First draft of the document	KU-Leuven
v0.4	18/04/2014	Second draft of the document	KU-Leuven
v0.5	23/04/2014	Third draft of the document	KU-Leuven
v0.6	25/04/2014	Fourth draft of the document – for internal review	KU-Leuven
v0.7	27/04/2014	Fifth draft of the document – integration of the first batch of comments	KU-Leuven
v0.8	29/04/2014	Sixth draft – integration of the final comments	KU-Leuven
v0.9	30/04/2014	Final version of the document – for submission	KU-Leuven
v1.0	01/05/2014	Provision of internal review comments	ATC, DW, INTRASOFT
v1.1	05/05/2014	Address of received comments and final formatting	KU-Leuven

CONTENTS

DEFINITIONS, ACRONYMS AND ABBREVIATIONS

Acronym	Title
DPD	Data Protection Directive
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
CJEU	Court of Justice of the European Union
DPR	Data Protection Regulation

1. Executive Summary

Deliverable D1.2 is the first of the legal deliverables in REVEAL. It provides a presentation and analysis of the legal framework applicable to this project. D1.2 focuses in its scope on the privacy and data protection aspects of the project. It provides legal requirements in this area that should be adhered to during the project lifetime. The ultimate objective of this deliverable is to ensure that the final outcome of the project complies with European legislation in this area.

The decision to put all the attention of D1.2 on privacy and data protection stems from the fact that this is the most crucial legal aspect of REVAL. The implementation of the defined requirements will have a direct impact on future REVEAL users. Moreover, privacy and data protection were defined as an ethical issue in the project description. Compliance with the outlined legal framework will be therefore be monitored by the REVEAL Ethical Committee. Other legal aspects of REVEAL, namely media law aspects and intermediary liability, will be addressed immediate after the provision of this documentation.

D1.2, additionally, provides a legal evaluation of the user requirements. These requirements are defined in D1.1, however, for the purpose of clarity, their legal assessment can be found in D1.2. This is because all the relevant legal concepts are explained in the presented deliverable D1.2.

2. Introduction

A question that has emerged in the REVEAL project is how to comply with current and future privacy regulations.

This deliverable aims to provide a coherent view of the current legal framework regarding privacy protection. An overview is provided of the current legal framework regarding privacy protection in the EU. More in detail, the main focus of this deliverable lays out the EU framework regarding data protection found in Directive 95/46/EC[1]. In chapter 4.4 the scope of application of the Directive is presented. Next, chapter 4.5 provides a list and analysis of the legal requirements for personal data processing. These requirements will have to be taken into account in the development of the technical side of the project. Further on, in chapter 5 other relevant concepts of data protection are discussed. The chapter covers topics such as privacy by design, transfer of personal data to third countries, processing of personal data versus freedom of expression, and processing of personal data from social networks. All these aspects are relevant for REVEAL.

As the Directive is currently undergoing a review, the changes foreseen in the proposed Regulation are also discussed in chapter 6. The Regulation has been accepted by the European Parliament on 12.03.2014. In order to become a law it still has to be adopted by the Council of Ministers. Such acceptance will be subject to negotiations between Parliament and the Council.[2] The actual entry into force of the new Regulation is not likely to happen before the end of 2015. REVEAL will be following the developments in this area to make sure the project is ready for compliance with the new rules. Until they come into force, however, REVEAL will strive to comply with the current legislation.

Moreover, this deliverable also provides an initial legal evaluation of the user requirements defined in D1.1. This evaluation can be found in chapter 7. Such evaluation is a continuous task, due to the fact that with the development of the project the defined requirements might evolve. Moreover, the legal regime will most likely be updated. An update of the legal evaluation, if required, will be conducted at a later stage of the project.

1 Directive 95/46/EC of the European Parliament and of the Council of 24.10.1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive), (OJ L 281, 23.11.1995)

2 Progress on EU data protection reform now irreversible following European Parliament vote, see more at: http://europa.eu/rapid/press-release_MEMO-14-186_en.htm.

3. Scope of the project

The world of media and communication is currently experiencing enormous disruptions: from one-way communication and word of mouth exchanges, we have moved to bi- or multi directional communication patterns. No longer can selected few (e.g. media organizations) act as gatekeepers, deciding what is communicated to whom and what not. Individuals now have the opportunity to access information directly from primary sources, through a channel we label e'-word of mouth', or what we commonly call 'Social Media'. A key problem, however, is that it takes a lot of effort to distinguish useful information from the 'noise' (e.g. useless or misleading information). This challenge has become the focus of various research efforts.

REVEAL aims to discover higher level concepts hidden within information on the basis of content that is being produced by users of social media. The aim is to reveal much more than bare content. Further to discovering what is being said, it will be determined how trustworthy that information is. Contributor impact will be predicted and how much or to what extent all this affects reputation or influence. The main goal is to reveal hidden modalities for the benefit of a better understanding and utilization of the Social Media world.

4. Relevant legal framework

4.1 Introduction

Privacy regulations have only become widespread and commonly accepted since the second half of the 20th century. The right to privacy therefore is a relatively young notion. The modern privacy benchmark at an international level can be found in the 1948 Universal Declaration of Human Rights[3], which specifically protects territorial and communications privacy.[4] Within Europe, the right to privacy can mainly be found in article 8 of the European Convention on Human Rights (ECHR)[5] which dates back to 1950. This provision concerns the private and family life, home and correspondence of the citizen. The Convention created the European Commission of Human Rights and the European Court of Human Rights to oversee enforcement. Both have been particularly active in the enforcement of privacy rights and have consistently viewed the Article's protection expansively and the restrictions narrowly. Although this article is still one of the foundations of European privacy protection, its value in the field of data privacy has been surpassed by the more enforceable instruments of the EU. Furthermore, the EU has included the right to privacy, as well as the right to data protection, in the Charter of Fundamental Rights of the European Union[6], anchoring the value of human rights protection in the Treaty on the European Union[7]. Finally, the right to privacy can be found in two directives: the Data Protection Directive 95/46/EC and the ePrivacy Directive 2009/136/EC[8].

4.2 European Convention of Human Rights: Article 8 the right to privacy

With the rise of the new information age, in which IT systems increasingly process personal data, public concern about privacy arose. Legal systems needed to respond to the new risks created by the flows of personal data. Not only national legal systems, but also the international community adopted relevant legal instruments. The 1948 United Nations Universal Declaration of Human Rights recognized privacy as a fundamental human right.

The right to respect one's private and family life is also stated in Article 8 ECHR concluded in 1950 in the framework of the Council of Europe and is one of the human rights and fundamental freedoms listed therein.

Article 8 of the Convention reads as follows:

"1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

3 Universal Declaration of Human Rights, 1948 (http://www.un.org/en/documents/udhr/).
4 See Article 8 of the Convention.
5 European Convention on Human Rights (http://www.echr.coe.int/Documents/Convention_ENG.pdf).
6 OJ. C 83 of 30 March 2010, 393.
7 Articles 7 and 8 of the Charter.
8 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (e- Privacy Directive), (OJ L 201, 31.7.2002)

The notion of one's private life is a broad term and is not susceptible to an exhaustive definition. The European Court of Human Rights in Strasbourg (hereinafter the 'Court')[9] recognized in several decisions that the concept of private life *extends to aspects relating to personal identity*, such as a person's name or a person's picture. [10] In addition, the Court stated that Article 8 of the Convention *protects a right to identity and personal development*, also in interaction with other persons, even in a public context.[11] It furthermore *includes, beyond a person's name, other means of personal identification* and of linking to a family and *the right to establish and develop relationships* with other human beings, in professional or business contexts as in others, and with the outside world.[12]

The concept of the right to respect one's private life hence knows a continuing evolution in the case law of the Court and of the national courts. They are often confronted with cases which challenge the application of existing rules, including cases involving new technologies. Legal provisions and legislation in the EU should take this fundamental right to privacy, as interpreted by the courts, into account. Already in 1969, the European Court of Justice ruled in a case in which an identity issue was raised, that identity is an important aspect of privacy. Moreover, the Court ruled that 'the Community's measures should be set aside if they fall short to respect a fundamental human right.'[13]

4.3 Charter of Fundamental Rights of The European Union: Articles 7 and 8

The Charter of Fundamental Rights of the European Union (Charter) contains various human rights provisions. Specifically, this instrument includes an explicit right to respect for privacy (Article 7) and an explicit right to protection in case of personal data processing (Article 8). The Charter was proclaimed and published in December 2000.[14] Subject to the ratification of the Treaty of Lisbon, the provisions of the Charter become legally binding in the EU Member States[15].

Article 7 of the Charter states as follows:

'Respect for private and family life

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

Article 8 of the Charter states as follows:

---

9 The European Court of Human Rights was set up in 1959 by the Council of Europe to decide upon claims for alleged violations of the European Convention on Human Rights of 1950. The Court has its seat in Strasbourg. The decisions of the Court are also available from the HUDOC Portal of the Court, which provides free online access to its case-law (http://www.echr.coe.int/ECHR/EN/Header/Case-Law/HUDOC/HUDOC+database/).

10 In a case of 1995, it was stated that the *unforeseen use* of photographs may amount to an invasion of privacy. See European Court of Human Rights, decision *Friedl v. Austria* of 31 January 1995.

11 See European Court of Human Rights, decision Peck v. United Kingdom of 28 January 2003, §57. See also European Court of Human Rights, decision Odièvre v. France of 13 February 2003 : matters of relevance to personal development include details of a person's identity as a human being and the vital interest protected by the Convention in obtaining information necessary to discover the truth concerning important aspects of one's personal identity, such as the identity of one's parents.

12 See European Court of Human Rights, decision Burghartz v. Switzerland of 22 February 1994, §24.

13 Case 29/69, Erich Stauder v. City of Ulm, (1969) Eur. Comm. Rep. 419. In this case, Mr. Stauder contested the requirement that he had to identify himself in order to obtain coupons allowing him to purchase butter at a reduced fee.

14 *O.J.* C 364/1,18 December 2000.

15 Since the adoption of the Treaty of Lisbon on 1 December 2009, the Charter became legally binding. Article 6(1) of the Treaty on European Union (TEU) now provides that '[t]he Union recognises the rights, freedoms and principles set out in the Charter of Fundamental Rights of the European Union […], which shall have the same legal value as the Treaties'. The Charter is equally applicable to all EU Member States, however, a Protocol was adopted to clarify its application to the United Kingdom and Poland, it does not limit or rule out its impact on the legal orders of these two Member States.

'Protection of personal data

1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority.'

The Charter in fact reaffirms these specific fundamental rights and freedoms as already set forth in the constitutions of the Member States and international treaties, in particular in the European Convention of Human Rights and Fundamental Freedoms. These provisions shall be applied in conformity with the interpretation of Article 8 ECHR by the European Court of Human Rights.

It is important to distinguish between the concept of data protection from the fundamental human right to privacy. Privacy is an individual right while data protection legislation is a tool which implements that right. In other words: data protection is a type of privacy protection manifested in legislation.

4.4 Directive 95/46/EC

In 1980, the Organization for Economic Cooperation and Development (OECD) adopted the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.[16] The Guidelines' objective was to reconcile the fundamental but competing values such as privacy and the free flow of information. In 1981, the Council of Europe followed by enacting the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data ('Convention 108')[17]. This convention is the first legally binding international instrument adopted in the field of data protection. Its purpose being: *"to secure [...] for every individual [...] respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data."*[18] It obliges the signatories to enact legislation concerning the automatic processing of personal data, which many duly did. But despite these efforts, diverging data protection legislations were a fact. As a result, the European Commission proposed the Data Protection Directive (hereafter DPD). The DPD was adopted in 1995 and thereafter had to be transposed in the different Member States by 24 October 1998. This centrepiece of EU legislation on personal data protection had two objectives in mind: to protect the fundamental right to privacy with respect to processing of personal data and to guarantee the free flow of personal data between Member States[19].[20]

The human rights approach to the treatment of personal data of the DPD as a central source for the EU law on information privacy is clearly stated in the Directive itself. Article 1(1) states that '*Member*

16 OECD Recommendation of the Council of 23 September 1980 concerning guidelines governing the protection of privacy and transborder flows of personal data [C(80)58/FINAL]. (http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm).

17 Council of Europe – ETS n°108 – Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1980. (http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm).

18 Article 1 of the Convention.

19 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), p. 1.

20 Article 1 of the Directive.

States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.'

The Directive 95/46/EC requires each Member State to set up its own Supervisory Authority or Data Protection Authority (DPA). Such agency is dedicated to privacy protection and the administration of domestic data protection law. DPAs also have enforcement powers, in addition to data subjects' private rights of action. Representatives of the authorities designated by each Member State, along with a representative of the authority or authorities established for the Community institutions and bodies, as well as a representative of the Commission comprise the Article 29 Data Protection Working Party. This group was named after article 29 of the Directive, which envisaged its creation.[21] The role of the Working Party is to provide interpretation of the provisions of the EU Data Protection framework.[22] It aspires to harmonize the application of data protection provisions across the European Union, and publishes opinions and recommendations on various data protection issues. These opinions are an indication of the trends and the direction in which privacy and data protection in the EU is headed. They provide a deep analysis of very specific issues and, for this reason they will be often called upon. For the REVEAL project, the most important documents include Opinion 1/2010 on the concepts of 'controller' and 'processor' of 16 February 2010[23], Opinion 5/2009 on online social networking of 12 June 2009[24] and Opinion 4/2007 on the concept of personal data of 20 June 2007[25], as well as the most recent Opinion 6/2014 on the notion of legitimate interest of the data controller of 9 April 2014[26].

Directive 95/46/EC requires all EU Member States to enact their own domestic laws adopting (or "transposing") the provisions of the Directive. The Directive is not limited to electronic (computerized) data, and therefore reaches not only files on paper, but also the Internet and even oral communications. Furthermore, the Directive 95/46/EC required each Member State to pass a data protection law that applies to both government and private entities.

The deadline for Member States to pass their local data laws was October 25, 1998, but in fact full implementation took several years more.

Rapid technological developments have, however, brought new challenges for the protection of personal data which were unforeseen by the original drafters of the Directive. As a result, in January the European Commission a **proposal for an updated data protection Regulation** (See *Chapter 6*). Last March 2014, the European Parliament approved the Data Protection Regulation. To become law the proposed Regulation must be adopted by the Council of Ministers. The European Parliament will negotiate the final text of the Regulation with the EU Council as soon as the Council defines its position.[27] As the proposed Regulation is still undergoing the legislative process at the European level, this deliverable focuses mainly on the current Directive. Where relevant, however, specific references to the proposed Regulation are made.

---

21 See http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm.

22 For more information: http://ec.europa.eu/justice/data-protection/article-29/index_en.htm.

23 Article 29 Working Party, Opinion 1/2010 on the concepts of "controller" and "processor", WP166, 16 February 2010.

24 Article 29 Data Protection Working Party, Opinion 5/2009 on online social networking, WP163, 12 June 2009.

25 Article 29 Data Protection Working Party, Opinion 4/2007 on concept of personal data, WP136, 20 June 2007.

26 Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interest of the data controller under Article 7 of the Directive 95/46/EC, WP217, 9 April 2014.

27 Progress on EU data protection reform now irreversible following European Parliament vote, see more at: http://europa.eu/rapid/press-release_MEMO-14-186_en.htm .

In the following section an analysis of the provisions of the Data Protection Directive is presented. The basic concepts and main principles of personal data protection are provided with the indication of specific problems that might occur in the frame of the REVEAL project. The REVEAL platform will most likely be implemented in Greece. Therefore, in addition to the Directive, also the Greek law on the Protection of Individuals is mentioned, when it differs from the Directive (*See Chapter 4.4.3*)

For the purposes of coherence, this Chapter follows the same structure as the Directive. The first section describes the relevant scope of application. Once it is clear to what extent and under which circumstances the DPD applies, the following section evaluates the rights and obligations that ensue from this applicability.

In order to determine what rules should be followed by REVEAL we must determine whether the activities in the context of this project fall within the scope of application of the European legal framework for data protection. The scope of application can be subdivided into the **material, personal and territorial scope**. This means that applicability of the data protection framework depends on ***what*** kind of data is being processed, ***who*** is actually processing the data and ***where*** the entity processing personal data is located.

4.4.1 Material Scope

The material scope of application relates to the actual activities that are covered by data protection law. Following article 3(1), the DPD is only applicable to *'the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system'.* As a result, there are two elements which determine the material scope, namely (a) personal data and (b) processing. These concepts will be explained hereafter in more detail.

4.4.1.1 Personal data

The core of the DPD is the notion of personal data which is defined very broadly as '*any information relating to an identified or identifiable natural person […]'*.[28] Such a natural person is called a data subject.

This definition of personal data contains four main building blocks, which are closely intertwined:

(a) "any information"
(b) "relating to"
(c) "an identified or identifiable" [natural person]
(d) "natural person"

These four building blocks will be analyzed separately.

Any information

The wording "any information" calls for a wide interpretation. With regard to the **nature** of the information, personal data includes any sort of statements about a person. It covers "**objective**" information, such as the presence of a certain substance in someone's blood.[29] In addition, it includes

[28] Article 2(a) DPD. Article 2(a) of the Greek law provides quite a similar definition: 'any information relating to the data subject. Personal data are not considered to be the consolidated data of a statistical nature when data subjects may no longer be identified.'

[29] Opinion 4/2007 on the concept of personal data of the Article 29 Working Party, p. 6.

"**subjective**" information such as opinions or assessments.[30] For information to be regarded as 'personal data', it is not necessary that the information is true or proven. With regard to the **content** of the information, personal data includes data providing any sort of information (information touching the individual's private and family life, information regarding whatever types of activity are undertaken by the individual, information concerning working relations or the economic or social behaviour of the individual, etc.).[31] Personal data includes information on individuals, regardless of the position or capacity of those persons (as consumer, patient, employee, customer, etc). [32]

With regard to the **format** or the **medium** on which that information is contained, the concept of personal data includes information available in whatever form (alphabetical, numerical, graphical, photographical or acoustic etc.).[33] It includes information kept on paper, as well as information stored in a computer memory by means of binary code, or on a videotape. [34] Sound and image data qualify as personal data insofar as they may represent information on an individual. If, for instance, during telephone banking the customer's voice giving instructions to the bank is recorded on tape, those recorded instructions should be considered as personal data.[35]

"Any information" also covers personal information considered to be "**sensitive data**" (See *below*).[36]

Relate to… "an identified or identifiable"

Information does not necessarily have to be *about* a person in order to be qualified as personal data. It can also be other information that is used to make decisions vis-à-vis individuals (e.g. phone records for billing purposes) or has an impact on them (e.g. surveillance cameras). [37] At the very least, the information needs to **relate to an identifiable person.** This has been further defined by the DPD as '*one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.*'[38]

A person can be considered as "**identified**" when, within a group of persons, he or she is "distinguished" from all other members of the group. [39] Accordingly, the natural person is "**identifiable**" when, although the person has not been identified yet, it is possible to do so. [40]

Identification is normally achieved through particular pieces of information which we may call "**identifiers**" and which hold a particularly privileged and close relationship with the particular individual. [41] Examples are outward signs of the appearance of this person, like height, hair colour, clothing, etc. or a quality of the person which cannot be immediately perceived, like a profession, a function, a name etc. [42] As a result, in order for a person to be identified/able, it is not required to have that person's name. The person in question does, however, need to be able to be distinguished from others. For example, the use of unique identifiers in cookies – even though the originating entity does not

30 *Ibid.*
31 *Ibid.*
32 *Ibid.*
33 *Ibid.*
34 *Ibid.*
35 *Ibid.*
36 Article 8(1) DPD and Article 2(b) of the Greek Law.
37 Opinion 4/2007 on the concept of personal data of the Article 29 Working Party, p. 9.
38 Article 2(a) DPD.
39 Opinion 4/2007 on the concept of personal data of the Article 29 Working Party, p. 12.
40 *Ibid,* p. 12.
41 *Ibid*, p. 13.
42 *Ibid*, p. 12.

know the actual name of the browser-user – the originating entity fulfils this requirement. Also, IP addresses[43] are regarded as data relating to an identifiable person.[44]

As a result of the abovementioned, **the pseudonymization of anonymization of information does not necessarily imply that data is not personal anymore**.[45] A mere hypothetical possibility to single out the individual is, however, not enough to consider the person as "identifiable". [46] Full, irreversible anonymization would be an option but technically speaking not achievable.

As regards **"indirectly"** identified or **identifiable persons**, this category relates to the phenomenon of "**unique combinations**".[47] In cases where the extent of the identifiers available does not allow a particular person to be singled out, that person might still be "identifiable". This is because that information might be combined with other pieces of information, which would allow the individual to be distinguished from others.[48]

Some characteristics are so unique that someone can be identified with no effort, but a combination of details on categorical level (age category, regional origin, etc.) may also be conclusive in some circumstances. [49]

"Natural person"

The DPD aims to protect only the fundamental rights and freedoms of natural persons.[50] Nevertheless, some Member States have decided to expand its scope of application, also offering protection to legal persons. The latter is however not the case in Greece[51].

Sensitive data

Special attention should be paid to 'sensitive data', **personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life**. [52] Pursuant to Article 8 DPD, the processing of sensitive data is prohibited unless a specific exception applies (See *Infra*).[53]

As it is the intention in the REVEAL project to collect data from social networks, sensitive data may be revealed. Therefore, there **is a realistic chance that the processing of personal data in the course of this project will involve also the processing of sensitive data.**

---

43 The text of the proposed Regulation explicitly states that IP addresses constitute personal data (Recital 24).
44 *Ibid*, p. 16.
45 See for instance the AOL and Netflix cases. In the first one, researchers retrieved the real identity behind the unique numbers AOL had attributed to the published search queries of over half a million of its users. The same thing happened with movie ratings attached to unique numbers that Netflix had posted. See: Paul Ohm, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization', (13 August 2009) University of Colorado Law Legal Studies Research Paper, <http://ssrn.com/abstract=1450006>, 15 *et seq.* Netflix even had to settle a legal challenge (R. Singel, 'NetFlix Cancels Recommendation Contest After Privacy Lawsuit' (Wired, 12 March 2010) <www.wired.com/threatlevel/2010/03/netflix-cancels-contest>).
46 Opinion 4/2007 on the concept of personal data of the Article 29 Working Party, p. 18.
47 *Ibid*, p. 13.
48 *Ibid*, p. 13.
49 *Ibid*, p. 13.
50 Article 1 DPD.
51 Article 1 of the Greek Law.
52 Opinion 4/2007 on the concept of personal data of the Article 29 Working Party.
53 Article 8(2) DPD.

4.4.1.2 Processing of personal data

In order for the DPD to apply, the personal data needs to be the subject of processing. Processing is defined as '*any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction'*.[54]

This definition is intended to cover all operations performed on personal data throughout its lifecycle, from collection, to use, to destruction. Because it is described in such a broad manner, there is hardly any activity that cannot be categorised as 'processing' under the DPD.

The majority of actions with regard to personal data intended in the REVEAL project can therefore in our view be qualified as 'processing' within the definition.

4.4.2 Personal Scope

The most difficult assessment is to determine the DPD's applicability concerning its personal scope. Even though it might be clear that personal data is being processed, it might still be difficult to identify the **entity responsible for this processing.** Determining this factor is relevant to establish who should be held accountable for the undertaken processing activities. Moreover, this will be relevant to define the applicable national data protection legislation.

The key actors within the DPD are (a) the 'Data Controller' (b) the 'Processor' and (c) the 'Data Subject'.

4.4.2.1 Data Controller

The data controller is defined as *'the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data [...]'*.[55] It is crucial to identify the data controller as this will determine which entity will be responsible for the processing and hence for compliance with data protection rules and obligations. From the data subject's perspective, it will also be very important to know who the data controller is, in order to be able to exercise one's rights (See *Chapter 4.5.2*).

The definition of controller contains three main building blocks:

(a) "natural or legal person, public authority, agency or any other body";
(b) "which alone or jointly with others" ;
(c) "determines the purposes and means of the processing of personal data".

Following from the first building block, both natural *and* legal persons can be qualified as data controllers.

[54] Article 2(b) DPD. Article 2(d) of the Greek Law defines the processing of personal data in a similar way as 'any operation or set of operations which is performed upon personal data by Public Administration or by a public law entity or private law entity or an association or a natural person, whether or not by automatic means, such as collection, recording, organisation, preservation or storage, alteration, retrieval, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, interconnection, blocking (locking), erasure or destruction.'

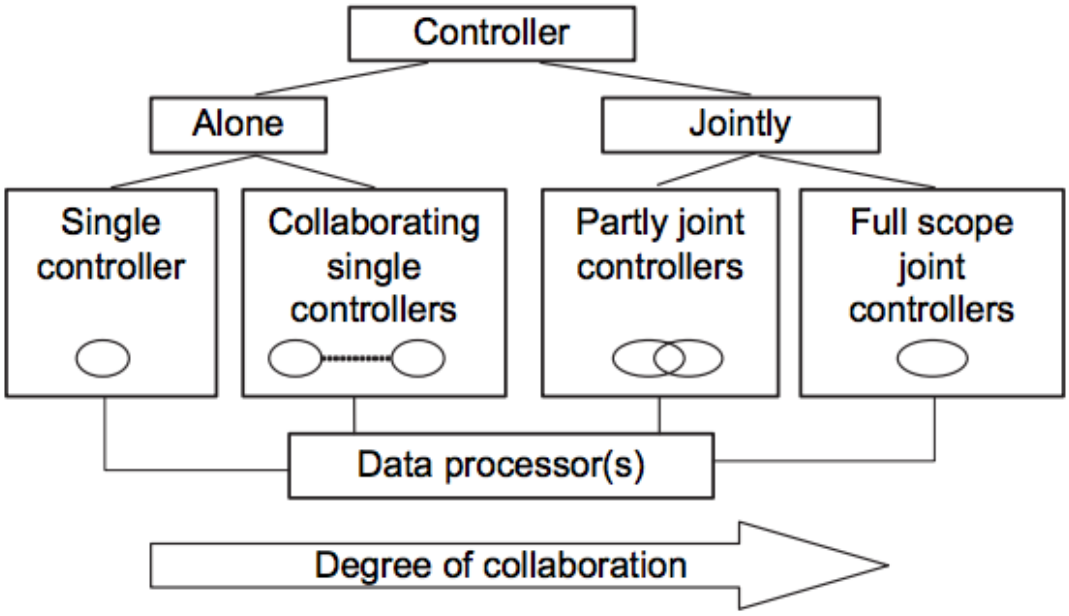
[55] Article 2(d) DPD. See also Article 2(g) of the Greek Law.

The latter building block makes clear that it will be necessary to identify the entity/entities that determine(s) the means and purposes of the processing activities. In other words, **the (natural or legal) person(s) that decide(s) on the *why* and *how* of the processing.** Whoever decides on the *means* and *purpose(s)* of the processing will be qualified as data controller. As a result, the quality of controller is acquired when deciding to process (certain) personal data for a specific purpose and by specific means. Originally what was meant by 'means of processing' is the physical 'machinery' or 'organisation' for processing. Due to technological developments this interpretation has lost some of its value, as the means for processing data are no longer necessarily determined by the data controller (see Infra).[56]

It is possible for the controller to delegate more specific organisational and technical questions regarding the *means.* [57] The entity who carries out such operations on behalf of the data controller is a 'processor' (See *Chapter 4.4.2.2*).

It should also be noted that a processing activity can have **more than one data controller.** Particularly when several persons jointly determine the purpose(s) and means of processing, they will share the ensuing responsibility.[58]

Another option is the situation in which two single controllers collaborate. Also other variations of the relationship are possible.



Source: T. Olsen, T. Mahler, Identity management and data protection law Identity management and data protection law: Risk, responsibility and compliance in 'Circles of Trust' – Part II, computer law & security report 23 (2007) p. 415–426.

In REVEAL, **the role of data control will, most likely, be played by project partner ATC**. The reason for assigning this role to ATC is because it is foreseen that ATC will implement the REVEAL platform, and this being done in Greece. ATC will also host the platform on their servers, consolidate inputs of other partners and conduct the platform maintenance. Other technical partners will be act-

[56] Opinion 1/2010 on the concepts of "controller" and "processor" of the Article 29 Working Party, p. 13.
[57] *Ibid*, p. 14.
[58] *Ibid*, p. 19.

ing as either processors or separate controllers (joint or collaborating), depending on the needs. All the formal requirements resulting from these arrangements will be taken care of with the help of the legal partner KU-Leuven Leuven to ensure compliance with EU and national legal regimes of the partners.

4.4.2.2 Processor

The processor is defined as '*a natural person or legal person, public authority, agency or any other body which processes personal data on behalf of the controller'.*[59]

The existence of a processor depends on a decision taken by the controller. As an entity determining how the processing will be conducted, the controller decides either to process data within his organization, or to delegate all or part of the processing activities to an external organization. In the former case it would be conducted, for example, through staff authorized to process data under his direct authority, and in the latter, through *"a legally separate person acting on his behalf*". In the case of outsourcing the processing activities, the controller makes use of a **processor**. The processor can thus be seen as a mere '**agent' of the controller**.[60]

The two basic conditions for qualifying as processor are (a) being a separate legal entity with respect to the controller and (b) processing personal data on his behalf.

The most important element is the requirement that the processor **acts "on behalf of the controller"**. This means serving someone else's interest and recalls the legal concept of "delegation". With regard to data protection law, a processor is first called to implement the instructions given by the controller[61] at least with regard to the purpose of the processing and the essential elements of the means.[62] Second, a processor has to guarantee data security when processing data.[63]

The role of processor does not derive from the nature of an entity processing data but from its concrete activities in a specific context. [64] As a result, the same entity can act, at the same time, as a controller for certain processing operations and as a processor for others (even on the same data – as explained above).[65]

The lawfulness of the processor's data processing activity is determined by the mandate given by the controller. A processor that goes beyond its mandate and acquires a relevant role in determining the purposes or the essential means of processing is a (joint) controller rather than a processor. [66]

Because of its secondary role, the processor will be subject to a lower level of responsibility with regard to the processing activities. The data controller will remain the principal responsible entity. As mentioned above, a processor only needs to (1) follow the instructions of the controller concerning the use of the data and (2) keep personal data secure from unauthorised access, disclosure, destruction or accidental loss.

59 Article 2(e) DPD. See also Article 2(h) of the Greek Law.
60 Opinion 1/2010 on the concepts of "controller" and "processor" of the Article 29 Working Party, p. 1.
61 Article 16 DPD.
62 Opinion 1/2010 on the concepts of "controller" and "processor" of the Article 29 Working Party, p. 16.
63 Article 17(2)-(3) DPD.
64 Opinion 1/2010 on the concepts of "controller" and "processor" of the Article 29 Working Party, p. 16.
65 *Ibid*.
66 *Ibid*.

4.4.2.3 Data Subject

The third important entity in the context of data protection is the data subject, which is the individual to whom the personal data (directly or indirectly) relates.[67]

4.4.3 Territorial Scope

Article 4 DPD provides that national provisions which are adopted pursuant to the Directive are applicable to the processing of personal data where:

(a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State;
(b) when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;
(c) the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law;
(d) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.

Concretely this means the following. When an undertaking is established in one of the 28 Member States, and the processing of personal data takes place in the context of the activities of this establishment, the national law of the Member State in which the undertaking is vested will apply. As for the requirement that the processing of personal data needs to take place 'in the context of the activities of the establishment' it needs to be kept in mind that for determining the applicable law it does not matter where the personal data is stored.[68] What is decisive here is whether the personal data is processed in the context of activities of a controller established in the European Union country (and which country).

Take for example company A which is established in Member State A and is collecting data in Member State B. In this case, data are collected in Member State B while company A is not established there, they are only located in Member State A. The data are processed in the context of the activities of the establishment in Member State A. Therefore, the applicable law is the law of Member State A.[69]

In case the undertaking has establishments in more than one Member State, it needs to be assessed in the context of the activities of which establishment the processing of the personal data is taking place. In other words: where is the data being used, by which establishment? It is possible that one or several laws apply to the different stages of processing. [70]

In order to ensure the right to the protection of personal data provided by the DPD, it is possible to trigger the applicability of a Member State's data protection law even where the controller is not established in the EU. This would be the case when the undertaking is not established on EU territory but processes data through equipment (or means)[71] located in a Member State[72].[73] Therefore, not

67 Article 2(a) DPD.
68 Opinion 08/2010 on applicable law of the Article 29 Working Party, p. 10.
69 *Ibid*, p. 12.
70 *Ibid*, p. 13.
71 The notion of "equipment" has been expressed in other EU languages by "means".
72 Article 4(1)(c) DPD.

any use of equipment within the EU/EEA leads to the application of the Directive. It presupposes some kind of activity of the controller and the clear intention of the controller to process personal data. Equipment thus includes human and/or technical intermediaries, such as in surveys or inquiries. As a consequence, it applies – amongst others – to the collection of information using questionnaires.[74]

Although less common, the applicability of a Member State's data protection law may also be triggered by virtue of international public law. This can for instance be the case where international public law or international agreements determine the law applicable in an embassy or a consulate, or the law applicable to a ship or airplane. In those cases where the controller is established in one of these specific places, the applicable national data protection law will be determined by international law. [75]

Since the controller in the REVEAL project will most likely be ATC, which is vested in Greece, **the Greek law on the Protection of Individuals with regard to the Processing of Personal Data will apply**.

4.4.4 Grounds for processing of personal data

Article 7 DPD provides for the legitimate grounds of data processing. This refers to situations in which processing of personal data is actually allowed. There are several grounds on which data processing can be based on for the process to be rendered lawful. It is recognised 'that the processing of any personal data about another is a trespass into the informational privacy of that person and must therefore either be accepted by the individual (consent) or justified on some basis'[76]. The list provided in Article 7 is exhaustive and cannot be expended upon by national law.

The first ground listed by the Directive states that data may be processed if the **data subject has unambiguously given his consent**[77]. The data subject's consent is defined as '*any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.*'[78] The key criteria for consent to be valid are that it has to be:

(a) unambiguous: the 'consent' can only be understood as the data subject's unequivocal agreement that his/her personal data will be processed. Therefore the procedure to seek and to give consent must leave no doubt as to the data subject's intention. There are in principle no limits as to the form consent can take. [79] However, for consent to be valid it should be an active indication of the user's wishes. The minimum expression of an indication could be any kind of signal, sufficiently clear to be capable of indicating a data subject's wishes, and to be understandable by the data controller. [80]

(b) specific: consent should clearly and precisely refer to the scope and consequences of the data processing. [81]

---

73 *Ibid*, p. 18.
74 Opinion 08/2010 on applicable law of the Article 29 Working Party, p. 20.
75 *Ibid*, p. 18.
76 Jay R., Angus Hamilton, Data Protection Law and Practice, Thomson, Sweet and Maxwell, 2003, 2nd edition, p. 178.
77 Article 7(a) DPD.
78 Article 2(h) DPD.
79 Opinion 15/2011 on the definition of consent of the Article 29 Working Party, p. 23.
80 *Ibid*.
81 *Ibid*, p. 17.

(c) freely given: consent needs to be a voluntary decision by an individual in possession of all of his facilities, taken in the absence of coercion of any kind, be it social, financial, psychological or other. [82]

(d) informed: consent must be based upon an appreciation and understanding of the facts and implications of an action[83]. In addition, consent can only be valid if the data subject is able to exercise a real choice, and there is no risk of deception, intimidation, coercion or significant negative consequences if no consent has been given.[84]

The Regulation provides that consent must be 'explicit'.[85] Also, further conditions for consent have been added. These clarify that implied consent does not suffice.[86] The Regulation also requires that consent given in a written declaration must be distinguishable from any other matters dealt with in the declaration.[87] This may mean that it will be no longer allowed to obtain consent – for instance via general terms and conditions – through a pre-ticked box. Also, the proposal outlines that consent to personal data processing will not be legitimate if there is *"a significant imbalance between the position of data subject and the controller"* (e.g. in the employment context).[88] Finally, the Regulation provides for the right of data subjects to withdraw their consent at any time.[89]

Next to consent, data can – under the DPD – also be processed if the processing is **necessary for the performance of a contract to which the data subject is party**[90], or in order to take steps at the request of the data subject prior to entering into a contract. This scenario applies where the data subject has entered into a contract, although it is not required that the contract is with the data controller.[91]

Moreover, personal data can be processed when it is **necessary for compliance with a legal obligation to which the controller is subject**[92]. This covers situations in which the data controller is required by law to process personal data.[93]

The data can also be processed if it is **necessary in order to protect the vital interests of the data subject**[94]. A 'vital interest' as a legal basis for lawfully processing data can only apply to a very limited number of situations. Classical examples mostly relate to the medical field. In addition, some fundamental security and financial interests with regard to housing, clothing and food might also fall in this category.[95]

The **processing of personal data is** allowed when it is **necessary for the performance of a task carried out in the public interest**[96], or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed. Processing data in the 'public interest' or in the 'exercise of official authority' must pursue a legitimate purpose and be necessary, appropriate and propor-

82 *Ibid*, p. 13.
83 *Ibid*, p. 19.
84 *Ibid*, p. 12.
85 Currently this is only required where consent is obtained to process sensitive personal data.
86 Recital 25 of the Regulation.
87 Recital 32 and Article 7(2) of the Regulation.
88 Recital 34 and Article 7(4) of the Regulation.
89 Article 7 of the Regulation.
90 Article 7(b) DPD.
91 Opinion 15/2011 on the definition of consent of the Article 29 Working Party, p. 18.
92 Article 7(c) DPD.
93 Opinion 03/2013 on purpose limitation of the Article 29 Working Party, p. 16.
94 Article 7(d) DPD.
95 Opinion 03/2013 on purpose limitation of the Article 29 Working Party. See also: A. Büllesbach, Y. Poullet, C. Prins (ed.), Concise European IT Law, Kluwer Law International, Alphen aan den Rijn, 2010, p. 57.
96 Article 7(e) DPD.

tionate to this legitimate purpose. Moreover, if these activities are being carried out by or on behalf of public authorities, they need to be foreseen in a legal provision. [97]

Finally, processing data is possible, if it is necessary for the purposes of the **legitimate interests pursued by the controller**[98] or by the third party or parties to whom the data are disclosed. This is the case, however, provided that this is not in conflict with the data subject's interests or fundamental rights and freedoms. In other words, processing on the basis of this ground is lawful, if the legitimate interests of the controller or of the third party prevails the (privacy) interests of the data subject. This requires the balancing of interests on a case-by-case basis weighing contradictory interests. The interest claimed by the controller needs to be a legitimate one, recognized by national (or EU) law.[99]

In the recent Opinion on the notion of legitimate interest of the data controller, the Article 29 Working Party provides an extensive analysis of this legal ground.[100] This group of data protection experts clarifies that "*A proper Article 7(f) assessment is not a straightforward balancing test consisting merely of weighing two easily quantifiable and comparable 'weights' against each other. Rather, the test requires full consideration of a number of factors, so as to ensure that the interests and fundamental rights of data subjects are duly taken into account*."[101] These factors include:

- the nature and source of the legitimate interest and whether the data processing is necessary for the exercise of a fundamental right, is otherwise in the public interest, or benefits from recognition in the community concerned;

- the impact on the data subject and their reasonable expectations about what will happen to their data, as well as the nature of the data and how they are processed;

- additional safeguards which could limit undue impact on the data subject, such as data minimisation, privacy-enhancing technologies; increased transparency, general and unconditional right to opt-out, and data portability.[102]

All these factors will be taken into account in REVEAL (*See Chapter 7*).

In the proposed Regulation these processing grounds have been kept.[103]

Also in the REVEAL project, a legal ground for the processing of personal data will have to be defined. At the current stage it seems that the **most appropriate legal ground for the processing of data in the REVEAL project will be either the data subject's consent or the legitimate interest of the controller (or a combination of both)**.

4.4.4.1 Grounds for processing sensitive data

As mentioned earlier, the processing of sensitive data is prohibited unless a specific exception applies (*See Chapter 4.4.1.1)*.[104] Such exception includes, notably, an explicit consent, which is freely

97 *Ibid*.
98 Article 7(f) DPD.
99 *Ibid*. See also: A. Büllesbach, Y. Poullet, C. Prins (ed.), Concise European IT Law, Kluwer Law International, Alphen aan den Rijn, 2010, p. 58.
100 Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interest of the data controller under Article 7 of the Directive 95/46/EC, WP217, 9 April 2014.
101 *Ibid*. p.3
102 *Ibid*. p.3
103 See more in Article 6(1) of the Regulation, available at: http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2014-0212
104 Article 8(2) DPD.

given[105]. This strict regime is the result of the conviction that the processing of these types of data is more privacy-invasive and presents a high risk of infringing fundamental freedoms or privacy[106]. The list is enumerative, which entails that only these types of data are considered to be sensitive. The aforementioned types of data are qualified as sensitive irrespective of the context in which they occur.[107]

As said, the processing of sensitive data is permitted in the cases when:

(a) the data subject has given his explicit consent to the processing of those data,
(b) it is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards; or
(c) it is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent.
(d) it is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects; or
(e) it relates to data which are manifestly made public by the data subject or when it is necessary for the establishment, exercise or defence of legal claims. [108]

4.4.5 Exemptions

It is worth noting that the DPD provides exceptions for a number of situations. In those situations the Directive is **not applicable**.

(a) Exception for activities not covered by Community law: the DPD does not apply to activities which are not covered by Community law. Article 95 of the Treaty establishing the European Community is the basis for the DPD. As a result, the DPD is first and foremost intended to harmonise the laws in transborder data flows in order to facilitate the internal market. These data flows are undoubtedly intertwined with internal market activities, such as movement of workers, goods and services.
(b) Exception for 'Third Pillar' data processing: the DPD also provides for an exception in case of the processing of personal data in the areas of foreign policy, security and defence, police and judicial issues.
(c) Exception for data processing related to personal or household activities: the processing of personal data for personal and household activities is exempt from the application of the DPD. As a result, it is exempt from the DPD when for instance people's names, addresses, phone numbers and email addresses are stored in diaries, on telephones or laptops[109] [110].

Exemptions for public authorities are provided under article 13.[111] Also, Article 9 provides for a possibility for Member States to introduce exceptions to some of the provisions of the Directive for the

105 Article 8(2)(a) DPD.
106 Recital 33 DPD.
107 S. SImitis., *Revisiting Sensitive Data,* 1999.
108 Article 8 DPD.
109 See recital 12 DPD.
110 Article 3(2) DPD. See also Article 3(2) of the Greek Law.
111 Obligations and rights may be restricted for safeguarding: "(a) national security; (b) defence; (c) public security; (d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of

processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression (See *Chapter 5.3*). This does not mean that processing of data for journalistic purposes are excluded from the scope of the Directive, but that EU countries can introduce more lenient rules with regard to specific obligations of the Directive (with regard to general rules of the processing, transfers of data to third countries, as well as supervisory authorities and working parties).[112] As a result, legal regime with regard to journalistic purpose may differ across the EU, depending on the exceptions introduced by each Member State.

4.5 Legal requirements for processing of personal data

As concluded in the previous section, data protection legislation is applicable to the activities conducted in the REVEAL project. As a result, the legal consequences which derive from the DPD need to be assessed. These can be divided into (a) data controller obligations and (b) data subject rights.

4.5.1 Data controller obligations

4.5.1.1 Legitimacy of Processing – transparency principle

The DPD states that processing must be fair and lawful.[113] These principles are often described as '*the essence of the right to data protection'*. According to Bygrave all '*the other provisions of the data protection Directive elaborate on these principles*'.[114] In order to fulfil this requirement, the data subject needs to reasonably know which of his personal data is processed, why and by whom. As a result, the data subject needs to be provided with certain information, which is listed in article 10 DPD, at the time of the obtaining of the data, or right after. In this way, the transparency of the data collection will be ensured. Moreover, this principle requires data controllers to comply with all types of their legal obligations, general and specific, statutory and contractual, concerning the processing of the personal data. For example the processing should be performed with respect to article 8 of the European Convention on Human Rights (which calls for respect for the private life of the individual - supra).

The concept of fair processing is linked to the reasonable expectations of the data subject. Processing of personal data is to be considered as fair if *'the collection and further processing of personal data (is) carried out in a manner that does not intrude unreasonably upon data subjects*' privacy nor interferes unreasonably with their autonomy and integrity. [115] It brings with it the requirements of balance and proportionality. On the other hand, it implies that a person is not unduly pressured into supplying data on himself to a data controller or accepting that the data are used by the latter for particular purposes.[116]

The Data Protection Directive states that processing, in order to be considered as lawful, must be carried out on one of the grounds listed by Article 7 DPD (*See Chapter 4.4.4*). As described, Article 7

---

ethics for regulated professions; (e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters; (f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e); (g) the protection of the data subject or of the rights and freedoms of others." See also Article 3(2)(b)-(c) of the Greek law.

112 See Article 9 DPD.

113 Article 6(1)(a) DPD.

114 L. A. Bygrave, Data Protection Law: approaching its rationale, logic and limits, Kluwer Law international, 2002, p.43.

115 A. Büllesbach, Y. Poullet, C. Prins (ed.), Concise European IT Law, Kluwer Law International, Alphen aan den Rijn, 2010, p. 65-66.

116 *Ibid*.

lists six legal grounds on which the processing can be based on as the 'criteria that makes the processing legitimate.'[117] This links the lawfulness of the data processing to its legitimacy. This means that any data processing needs to have a legal justification. In case of the contrary, the processing will be unlawful. Moreover, these grounds cannot be expanded by national laws.

4.5.1.2 Purpose Specification – finality principle

On the basis of Article 6(1)(b) DPD[118] personal data must be *'collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes'.* This means that a data controller needs to specify – in advance – what he plans to do with the personal data. This provision is also known as the '**principle of finality'** or 'purpose (or use-) limitation principle'. It protects data subjects by setting boundaries on how collected personal data for a given purpose may be processed by controllers and may be put to further use. The purpose(s) that is/are initially specified to justify the collection and/or further processing of the data in principle delineates its authorized usage. Processing of personal data in a way incompatible with the purposes specified at collection is against the law, and therefore prohibited. [119] Further processing for a different purpose does, however, not necessarily mean that it is incompatible with the original purpose. This needs to be assessed on a case-by-case basis. [120]

The concept of purpose limitation has two main building blocks (a) purpose specification and (b) compatible use.

(a) **'purpose specification'**: the data controller needs to determine the specific purpose for which the processing of data is needed. The purpose of processing must be:
   i. Specified: the purpose(s) needs to be clearly and specifically identified, allowing the data subject to know what kind of processing will not be included;
   ii. Explicit: the purpose(s) must be clearly revealed, explained or expressed in some intelligible form, allowing for an unambiguous identification of why the data will be processed (supra, transparency);
   iii. Legitimate: the purpose(s) must be in accordance with the law, in the broadest sense possible. [121]

It is possible that a controller fails to comply with these requirements, for example, if he does not specify the purposes of the processing accurately and in sufficient detail or in a clear and unambiguous language. Examples of purpose specifications that do not comply, because of their vagueness, are for example: 'improving users' experience' or 'for marketing purposes'.[122] It is important to emphasize that this does not mean that the data controller can process personal data for any and all purposes at its discretion. Neither the controller is free to determine the purposes based on its subjective expectations or unilateral interpretation of inconsistent information. In such cases, it will be necessary to reconstruct the purposes of the processing, keeping in mind the facts of the case.[123]

(b) **'compatible use'**: personal data collected must not be further processed in a way incompatible with those purposes. This building block calls for an assessment by the data controller. This assessment can take two different forms.[124]

---

117 Recital 30 DPD.
118 Article 4(1)(a) of the Greek Law.
119 Opinion 03/2013 on purpose limitation of the Article 29 Working Party, p. 16.
120 *Ibid*.
121 *Ibid*.
122 *Ibid*.
123 *Ibid*.
124 *Ibid*.

i. formal assessment: comparing the purpose(s) that was initially provided by the data controller with any further uses to find out whether these uses are covered.
ii. substantive assessment: identifying both the new and the original purpose, taking into account the way they are (or should be) understood, depending on the context and other factors. [125]

Processing of personal data for historical, statistical or scientific purposes, which is conducted by the same controller is expressly privileged under Article 6(1)(b) DPD. Such further use is considered as always being compatible with the initial purpose of data collection. However, appropriate safeguards against infringement of data subject rights need to be taken[126].

The analysis in this sub-section demonstrates the **importance to specify explicit and legitimate purposes before starting to processes personal data.**

4.5.1.3 Data minimisation

Pursuant to Article 6(1)(c) DPD data minimisation is required, meaning that the processing of personal data should be limited to data that are adequate, relevant and not excessive. As a result, data controllers are obliged to store only a minimum of data necessary to run their services. [127] The purpose of this principle is to prevent the collection of data which is not strictly necessary for the purpose in question. The principle therefore acts as a barrier in order to limit the collection of data. Once the data collected does not serve the purpose it was collected for anymore, the controller either has to anonymize the data or erase it. When assessing the scope of the purpose, it is also important to take into account the data subject's reasonable expectations. [128]

4.5.1.4 Data quality

Article 6(1)(d) DPD[129] provides that all personal data should be accurate and, where necessary, kept up to date. As a result, data controllers need to take every reasonable step to ensure that data which are inaccurate or incomplete are either erased or rectified, having regard to the purposes, for which they were collected. A creation of an appropriate mechanism to allow data subjects updating their personal data or notifying the data controller about the incorrect information is often suggested in this context.[130] Such a solution would reduce the risk of complaints of breach of this principle, in case of harm caused by inaccurate data.[131]

4.5.1.5 Data conservation

Article 6(1)(e) DPD requires that personal data shall not be kept for longer than necessary for the purposes for which it was collected. When the purpose for which the data was gathered has been achieved, the data should either be rendered anonymous or destroyed.[132]

125 *Ibid*.
126 Article 6(1)(b) and Recital 29 DPD.
127 Opinion 03/2013 on purpose limitation of the Article 29 Working Party, p. 13.
128 *Ibid*.
129 Article 4(1)(b) of the Greek Law.
130 A. Büllesbach, Y. Poullet, C. Prins (ed.), Concise European IT Law, Kluwer Law International, Alphen aan den Rijn, 2010, p. 53.
131 *Ibid*.
132 Article 6(1)(e) DPD.

4.5.1.6 Data security

The DPD imposes a duty of security. As a result, the data controller is required to take appropriate technical and organisational measures that *'protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.*'[133]

4.5.1.7 Notification to the competent DPA

Every controller of personal data has the obligation to inform the relevant Data Protection Authority (DPA)[134]. This notification needs to be made *before* the controller will start its processing activities.[135] The Directive provides Member States the possibility to simplify the notification procedure or to waive it in certain situations. However, for the majority of entities engaged in processing of personal data, notification is obligatory.

According to Article 19 DPD the notification to a national data protection authority needs to include at least the following information:

(a) the (trade) name and address of the controller (and of his representative, if any);
(b) the purpose(s) of the processing;
(c) a description of the category or categories of data subject and of the data or categories of data relating to them;
(d) the recipients or categories of recipient to whom the data might be disclosed;
(e) proposed transfers of data to third countries;
(f) a general description allowing a preliminary assessment to be made of the appropriateness of the measures taken to ensure security of processing.[136]

When a controller stops (or adjusts) its data processing activities, the Directive also requires a notification to the DPA.

The Greek data protection legislation specifies the following information that needs to be included in the notification to the DPA:

(g) the address where the file(s) or the main hardware supporting the data processing are established;
(h) the time period during which the controller intends to carry out data processing or preserve the file(s);
(i) the basic characteristics of the system and the safety measures taken for the protection of the file(s) or data processing.[137]

The General Data Protection Regulation introduces the obligation for controllers and processors to maintain documentation of the processing operations under their responsibility[138], instead of the general notification to the supervisory authority currently required. This means that the earlier mentioned notification to the DPA could in a later stage of the project no longer be obligatory. It is how-

133 Article 17(1) DPD. Article 10(3) of the Greek Law.
134 Article 18(1) DPD. Article 6 of the Greek Law.
135 *Ibid.*
136 Article 19(1) DPD.
137 Article 6(2) of the Greek Law.
138 Article 28 of the Regulation.

ever not definite yet that this element will be kept in the final Regulation. Also, at this point we need to comply with present legislation.

The Regulation does however introduce a breach notification: controllers will be obliged to notify data protection authorities of personal data breaches[139].

4.5.2 Data subject rights

The goal of Data Protection legislation is to protect the data subject against the illegitimate processing of his or her personal data. As a result, the data subject is provided with a number of rights that he or she can exercise against the data controller and that need to provide for a correct processing of the personal data.

It is worth mentioning that the Regulation proposes an expansion of the information[140] which a data subject can demand from a controller. Also, controllers must have procedures in place to deal with the exercise of data subjects' rights.[141]

4.5.2.1 Right to information

Before collecting personal data, the data subject concerned must be supplied with certain information. The purpose of the right is to ensure the transparency of the processing. Article 10 DPD[142] provides that the controller must inform the individual whose data is collected of the following details:

(a) his or her identity (and the identity of his or her representative, if any);
(b) the purpose of data processing;
(c) any further information insofar it is necessary having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject, such as:
    a. the recipients or the categories of recipients of such data
    b. whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply
    c. the existence of a right to access and the right to rectify the data concerning him.

The proposed Regulation extends the scope of information that would need to be provided to the data subjects.[143]

In situations where the data have not been obtained from the data subject directly, it is required to assess in which cases and at what time the information should be given to the data subject.[144]

Article 11 DPD states that the information should be provided at the time of the recording of personal data or, if a disclosure to a third party is foreseen, no later than the time when the data are first disclosed. The second paragraph, however, provides that this obligation does not apply *'where the provision of such information proves **impossible** or would involve a **disproportionate effort**'*.

139 Article 31 of the Regulation.
140 Article 13 of the Regulation.
141 Article 12 of the Regulation.
142 Article 11 of the Greek Law.
143 Article 14 of the Regulation.
144 A. Büllesbach, Y. Poullet, C. Prins (ed.), Concise European IT Law, Kluwer Law International, Alphen aan den Rijn, 2010, p. 66.

No requirement may be imposed on a controller which he would be unable to fulfil. As a result, a controller cannot be obliged to provide information if this is proven to be impossible. This impossibility needs to be evident at the moment when the information should have been provided. It could, for instance, be impossible to provide information to the data subject when the controller is not able to contact the data subject.[145] This could be the case when the controller does not have the postal or email address of the data subject at his disposal and he was not able to find this information after reasonable effort with resources available.[146]

The controller is also lifted from his obligation to provide the data subject with the information required by Article 10 DPD in case this would involve a disproportionate effort. Here the effort is balanced against the interests of the data subject. [147] When assessing the disproportionate effort the costs, time, and ease of providing the information should be weighed against the benefit to the individual of receiving the information. However, when it would be more likely that the rights of the data subject will be infringed, a higher degree of effort is deemed appropriate. [148]

Article 11(2) provides that the provision of information could in particular be disproportionate when processing for statistical purposes or for the purposes of historical or scientific research. In this regard, the number of data subjects, the age of the data, and any compensatory measures adopted may be taken into consideration.[149] A question whether this exception could be relied upon in REVEAL will be further investigated in the project (*See Chapter 7*).

4.5.2.2 Right to object

Data subjects have the right to object to certain types of processing of their personal data.[150] This requirement needs to be evaluated on a case-by-case basis. The main condition is that the data subject can call upon compelling legitimate grounds relating to his particular situation. The data subject will have to establish that the processing might affect him negatively and/or the processing does not have a legitimate basis (anymore).[151]

As an example, the DPD mentions the *"processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority and processing necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed*" as possible cases in which a right to object can be granted.[152] When his personal data is processed by a data controller who anticipates direct marketing purposes, the data subject may object to this processing.[153] He must also be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing. In such cases the data subject should be expressly offered the right to object, free of charge, to such disclosures or uses.

Requests do not have to be motivated by data subjects when objecting to the processing of their data for direct marketing purposes. In any situation, the data subject will have to fulfil certain formal requirements when exercising its right to object which requirements can vary from Member State to

145 *Ibid*, p. 71.
146 *Ibid*.
147 *Ibid*.
148 *Ibid*.
149 Recital 40 DPD.
150 Article 14 DPD.
151 A. Büllesbach, Y. Poullet, C. Prins (ed.), Concise European IT Law, Kluwer Law International, Alphen aan den Rijn, 2010, p. 82.
152 Article 14(a) DPD.
153 Article 14(b) DPD.

Member State. The request should at least be submitted – signed and dated – to the controller. The latter will have – on the basis of Greek law – 15 days[154] (starting from the submission of the request) to inform the data subject that it has complied with the request.

If the controller does not respond within the specified time limit or his or her reply is unsatisfactory, then the data subject has the right to appeal before the DPA and request that his or her objections are examined. The DPA then analyses whether such objections are reasonable and furthermore if there is a risk of serious damage being caused to the data subject as a result of the processing. If this is the case, the DPA may order the immediate suspension of the processing until a final decision on the objections is issued.[155]

4.5.2.3 Right of access

The data controller has to provide certain information to data subjects. While the right to information provides the data subject with the basic information about the processing of his personal data, he or she also holds the right to receive more information about the data that is processed:

(a) Information on whether or not data relating to him is being processed, as well as information regarding the purposes of the processing, the categories of data the processing relates to, and the categories of recipients the data is disclosed to;
(b) Communication of the data being processed in an intelligible form, as well as of any available source information;
(c) Information about the basic logic involved in any automatic processing of data relating to him in case of automated decision making.[156]

The Greek Law provides that the data subject is entitled to request and obtain from the controller the following information:

(a) All the personal data relating to him as well as their source;
(b) The purposes of data processing, the recipient or the categories of recipients;
(c) Any developments as to such processing for the period since he or she was last notified or advised;
(d) The logic involved in the automated data processing;
(e) The correction, deletion or locking of data, the processing of which is not in accordance with the provisions of the law, especially due to the incomplete or inaccurate nature of data;
(f) The notification to third parties, to whom the data have been announced, of any correction, deletion or locking which is carried out in accordance with (e), taken that the notification is not impossible or does not demand disproportionate efforts.[157]

The Regulation introduces a right to access and to obtain data for the data subject.[158] In addition to the current information that needs to be provided, the Regulation specifies additional information that will have to be provided by the controller to the data subject[159]

154 Article 13(1) of the Greek Law.
155 Article 13(2) of the Greek Law.
156 Article 12(a) DPD.
157 Article 12 of the Greek Law.
158 Article 15 of the Regulation.
159 Article 15 of the Regulation.

4.5.2.4 Right to erase

Data subjects also have the right to have their personal data erased, free of charge. This right can, however, only be invoked **when the data is incomplete/irrelevant to the purpose(s) of processing, when the processing is prohibited or when the data is stored longer than originally agreed.** So, when a data subject has successfully exercised its right to object, the data controller can also be asked to erase the data subject's personal data.[160] As to the formalities, the same ones apply as with regard to the exercise of the right to correction. The Regulation specifies the grounds for erasure in Article 17. For example, it provides that data should be erased when a court or regulatory authority based in the EU has ruled as final and absolute that the data concerned must be erased. [161]

4.5.2.5 Right to Correct

On the basis of the DPD, data subjects have the right to ask for the correction of their personal data, free of charge.[162] This is the result of the data controller's obligation to keep personal data accurate and up-to-date. In order to exercise this right, the same formalities have to be fulfilled as with regard to the right to object. The controller will have to communicate any rectifications made within one month after submission, not just to the data subject but also to all known recipients of the information.

4.5.2.6 Right not to be a subject to an automated decision

Article 15 DPD grants data subjects the right not to be subject to an automated decision which produces legal effects concerning him or significantly affects him. The right refers to a decision, which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him. This could be his performance at work, creditworthiness, reliability, conduct, etc.[163] Statutory exceptions related to this right arise in cases where the decision is either:

(a) taken in the course of the entering into or performance of a contract, provided that the request (for the entering or the performance of the contract) has been launched by the data subject and there are suitable measures to safeguard the data subject's legitimate interests; or
(b) authorised by a law that also lays down measures to safeguard the data subject's legitimate interests.[164]

4.5.2.7 Right to seek legal relief

Pursuant to Article 22 DPD every person has the right to a judicial remedy for any breach of the rights guaranteed to him by the national law applicable to the processing in question. Further, Article 23 DPD provides that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to the Directive is entitled to receive compensation for the damage suffered from the controller.

160 Article 12(b) DPD.
161 Article 17 of the Regulation.
162 Recital 25 DPD.
163 A. Büllesbach, Y. Poullet, C. Prins (ed.), Concise European IT Law, Kluwer Law International, Alphen aan den Rijn, 2010, p. 84.
164 *Ibid*.

4.6 Sanctions

The DPD requires that Member States provide suitable measures to ensure compliance with the Directive. This includes sanctions for the breach of national legislation.[165] There is a wide range of sanctions that can be imposed for breach of data protection legislation.

Monitoring of the application of the national rules is bestowed upon supervisory authority of each Member State. These data protection authorities have investigative powers as well as effective powers of intervention. The latter include delivering opinions before processing operations are carried out, ensuring appropriate publication of such opinions, and ordering the blocking, erasure or destruction of data, imposing a temporary or definitive ban on processing, warning or admonishing the controller, and referring the matter to national parliaments or other political institutions.[166] Moreover, data protection authorities have the power to engage in legal proceedings where the national provisions transposing the Directive have been violated or to bring these violations to the attention of the judicial authorities.[167]

The Greek data protection law provides for the right for supervisory authorities to impose administrative and criminal sanctions as well as civil liability.[168] The former amount to warning, fines on data controllers, temporary or definitive ban on processing or a combination of all.[169] Also a variety of criminal sanctions can result from a breach of data protection legislation. For instance, data controllers who have not (correctly) notified the Greek DPA of their processing activities risk imprisonment for up to three years and a large fine.[170] Moreover, breach of the data protection rules can result in liability for damages or compensation.[171]

Under the proposed Regulation, a breach of protection rules could result in a fine of up to EUR 100 million or 5% of the global annual turnover. [172]

165 Article 24 DPD.
166 Article 28(3) DPD.
167 *Ibid*.
168 See Section E of the Greek Law.
169 Article 21 of the Greek Law.
170 Article 22(1) of the Greek Law.
171 Article 23 of the Greek Law.
172 Article 79 of the Regulation.

5 Other relevant concepts of data protection

5.1 Privacy by design

The Concept of Privacy by Design (PbD) was developed in the nineties by Ann Cavoukian, the Information and Privacy Commissioner of Ontario, Canada. It addresses the ever-growing and systemic effects of Information and Communication Technologies, and of large-scale networked data systems. Privacy-by-design relies on the design and implementation of procedures and systems in accordance with privacy and data protection, already at the planning stage right through to its ultimate deployment.[173] Privacy by Design advances the view that the future of privacy cannot be assured solely by compliance with regulatory frameworks. Rather, privacy assurance must ideally become an organization's default mode of operation. Initially, deploying Privacy-Enhancing Technologies (PETs) were seen as the solution. In literature, however, there now seems to be agreement on the fact that a more substantial approach is required.[174]

The objectives of Privacy by Design consist of ensuring privacy and gaining personal control over one's information. For organizations, it consists of gaining a sustainable competitive advantage.[175] These goals may, in Cavoukian's view, be accomplished by practicing the following seven principles:

(a) Proactive not Reactive; PbD is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events before they happen. [176]

(b) Privacy as the Default Setting; PbD seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given system. If an individual does nothing, their privacy still remains intact. [177]

(c) Privacy Embedded into Design; PbD is embedded into the design and architecture of IT systems and business practices. [178]

(d) Full Functionality; Privacy by Design avoids the pretence of false dichotomies, such as privacy vs. security, demonstrating that it is possible to have both. [179]

(e) End-to-End Security; Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved. [180]

(f) Visibility and Transparency; Privacy by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to users and providers alike. [181]

(g) Respect for User Privacy; PbD requires to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options.[182]

---

173 Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling, p. 3.
174 *Ibid*.
175 See: http://www.privacybydesign.ca/
176 *Ibid*.
177 *Ibid*.
178 *Ibid*.
179 *Ibid*.
180 *Ibid*.
181 *Ibid*.
182 *Ibid*.

According to the **General Data Protection Regulation,** having regard to the state of the art, current technical knowledge, international best practices and the risks represented by the data processing, the controller and the processor, need to at the time of the determination of the purposes and means for processing and at the time of the processing itself, implement appropriate and proportionate technical and organisational measures and procedures in such a way that the processing will meet the requirements of the Regulation and ensure the protection of the rights of the data subject.[183]

5.2 Transfer of personal data to third countries

Personal data which is processed may only be transferred to a third country under certain conditions, namely if that country can guarantee an adequate level of data protection. A third country is defined as a state to which the DPD is not addressed and thus does not apply (non-EU countries).[184] This adequacy is assessed in the light of all the circumstances surrounding a data transfer operation. In particular it refers to *"the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country*."[185] This assessment is performed by the Commission.

Article 26 DPD does however provide for a number of exceptions[186]. These exceptions are formulated in the same line as the exceptions to the principal prohibition of processing special categories of data (*See Chapter 4.4.4.1)*.

5.3 Processing of personal data versus freedom of expression

As stated earlier, Member States can introduce exemptions or derogations in their national laws for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression. [187] However, such derogations are only allowed if they are necessary to reconcile the right to privacy with the rules governing freedom of expression. The said exemptions can refer solely to certain parts of the DPD, mainly chapters on the general measures on the legitimacy of data processing, on the transfer of data to third countries and the power of the supervisory authority. [188] The exemptions are, however, not allowed to derogate from measures to ensure security of

183 Article 23(1) of the Regulation.
184 Article 25(1) DPD.
185 Article 25(2) DPD.
186 Article 26(1) DPD provides that that transfering personal data to a third country which does not ensure an adequate level of protection may take place on condition that: (a) the data subject has given his (unambiguous) consent to the proposed transfer; or (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or (d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or (e) the transfer is necessary in order to protect the vital interests of the data subject; or (f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.
187 Büllesbach A., in: Büllesbach A., Poullet Y., Prins C. (eds.), Concise European IT Law, Alphen aan den Rijn, 2005, p. 55.
188 *Ibid*.

processing. Such balancing between the fundamental rights of privacy and freedom of speech and expression is necessary as very often these two rights might be in a clear conflict. [189]

The fundamental right of freedom of speech is guaranteed in particular in Article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms, and Article 11 of the Charter of Fundamental Rights. It includes the freedom to hold opinions and to receive and impart information and ideas without interference by public authorities and regardless of borders. This right can sometimes prevail over the right to privacy as a legitimate interest, also for opinions voiced on the Internet.[190] To solve this conflict, the Directive allows Member States to introduce specific derogations to their laws. This leads to great divergence between specific national regulations. The situation ranges from stipulation of the overall primacy of freedom to expression, through wide exemptions for the press, to a system that is equivalent to imposing prior restraint on the publication of certain information by the press.[191] For example in German constitutional law a differentiation is made between opinions and facts. Voicing facts is usually lawful. Voicing opinions is usually lawful, as long as these opinions are not offensive or abusive.[192] In Sweden the exemption is not limited only to the professions listed (journalists, authors of literary works), since according to interpretation of the Swedish Supreme Court, Article 10 of the ECHR and Article 11 of the Charter of Fundament Rights provide everyone with the right to freedom of speech.[193] Greek data protection law[194] provides that data pertaining to public figures is considered sensitive data. The processing of such data is permitted, provided that such data are in connection with the holding of public office or the management of third parties' interests, and is carried out solely for journalistic purposes. The Greek Data Protection Authority may grant a permit only if such processing is absolutely necessary in order to ensure the right to information on matters of public interest, as well as within the framework of literary expression and provided that the right to protection of private and family life is not violated in any way whatsoever. [195]

In majority of the countries a balancing exercise between the conflicting principles of Article 8 ECHR (right to privacy) and Article 10 ECHR (right to freedom of expression) must be performed by courts on case-to-case basis. In order to have a full picture of the regulatory situation in Europe a further analysis of this issue will be conducted in the future deliverable D1.2 a.

For the purpose of REVEAL a very relevant provision is provided for in Article 9 of the DPD. As discussed earlier, Article 9 provides for a possibility for Member States to introduce exceptions to some of the rules for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression. In result, regimes on processing of personal data for journalistic purposes may differ across the EU, depending on the position taken by each Member State. This possibility is, however, the case only if such exceptions are necessary to reconcile the right to privacy with the rules governing freedom of expression. [196] The provision aims to ensure that journalists can collect and process personal data to fulfil their duties. Article 1 DPD provides that Member States should, while permitting the free flow of personal data, protect the fundamental rights and freedoms of natural persons and, in particular, their right to privacy, with respect to processing of their personal data. That objective can only be pursued by reconciling those fundamental rights with the fundamental right to freedom of expression. It is exactly this purpose that Article 9 pursues: to

189 *Ibid*.
190 *Ibid*.
191 *Ibid*.
192 *Ibid*.
193 Ramsbro v Riksåklagaren, Swedish Supreme Court of 12 June 2001.
194 Article 7 of the Greek Law.
195 Article 7 of the Greek Law.
196 A. Büllesbach, Y. Poullet, C. Prins (ed.), Concise European IT Law, Kluwer Law International, Alphen aan den Rijn, 2010, p. 65-66.

reconcile the two rights. [197] Processing for journalistic purposes is typically done by the press, radio or film media enterprises or individual journalists. However, Article 9 also applies to the provision of information by specialised media archives and the exchange of information in the course of co-operation between media enterprises.[198] In order to benefit from this exception, the processing of personal data should only take place for journalistic purposes. If a differing processing purpose should be added, the overall processing may no longer be privileged.[199] The fact that a publication is done for profit making purposes does on the other hand not preclude publication from being considered as "solely for journalistic purposes." [200] As a result, journalistic activities include activities carried out by individuals without making a profit (e.g. bloggers).[201] Also the medium used is not determinative. Therefore, activities may be classified as "journalistic" if their sole object is the disclosure to the public of information, opinions or ideas, irrespective of the medium used to transmit them.[202]

The implementation of Article 9 DPD concerning journalism in national legislation is highly divergent and in some cases very restrictive. [203] Meanwhile, with online activities, the difficulty arises of determining which national law is applicable to concrete online activities. And, at least as currently drafted, legislation in this area will not become any clearer after the adaptation of the Regulation[204] [205].

5.4 Processing of personal data from social networks

One of the most significant developments in the online environment over the last few years has been the rise of social media.[206] More and more individuals are making use of Social Networking Sites (SNS) to stay in touch with family and friends, to engage in professional networking or to connect around shared interests and ideas. But users are not the only ones who are interested in SNSs. SNSs have come to attract a wide range of actors, which include application developers, web trackers, third-party websites, data brokers and other observers.

As the number of actors engaging with SNSs and SNS data increases, so does the risk for potential privacy infringements. This paragraph will analyze how the current data protection framework relates to the context of SNSs.

It should first be noted that different categories of data are disclosed via SNSs. Take for instance:

(a) *Disclosed data*: data that is posted by SNS users on their own profile pages (e.g., blog entry, picture, video);
(b) *Entrusted data*: data that is posted by SNS users on the profile pages of other SNS users (e.g., a wall post, comment);
(c) *Derived data*: data which is inferred from (other) SNS data (e.g., membership of group X implies attribute Y);

197 *Ibid*.
198 *Ibid*.
199 *Ibid*.
200 European Court of Justice C-73/07, Tietosuojavaltuutettu [Finnish data protection ombudsman] v. Satakunnan Markkinaporssi Oy and Satamedia Oy, 16.12.2008.
201 See: http://ico.org.uk/news/events/~/media/documents/future_of_dp_in_europe_2012/ico_event_future_of_dp_in_europe_2012_Chris_Kuner_article.ashx
202 *Ibid*.
203 See: http://ec.europa.eu/justice/news/consulting_public/0006/contributions/citizens/dp_at_csls_study_group_en.pdf
204 See Article 80 of the Regulation.
205 See: http://freespeechdebate.com/en/discuss/confused-the-tension-between-data-protection-freedom-of-expression/
206 O. Tene, 'Privacy: the new generations', *International Data Privacy Law* 2011, Vol. 1, No. 1, p. 22.

(d) *Incidental data*: data about an SNS user which has been uploaded by another SNS user (e.g., a picture);
(e) *Behavioural data*: data regarding the activities of SNS users within the SNS (e.g., who they interact with and how).[207]

Each of these social networking data will qualify as personal data insofar as they relate to an identified or identifiable individual.[208] It is not required that the individual in question be identified by his or her full name. Even where individuals do not appear to be directly identified (e.g., when a pseudonym is used), they may be indirectly identifiable through (a combination of) other data, such as the personal attributes listed in their profile (e.g., age, residence, etc.), their list of friends, traffic data (e.g. IP-addresses) or cookie data. As a result, a combination of such data on **SNS profiles are considered personal data**. [209]

Although (personal) data from social networks is public, it is crucial to bear in mind that this fact does not deprive it from the protection offered by the data protection regime (be it the Directive or the future Regulation). The processing of such data still needs to be fair and lawful. As a result, firstly, there needs to be a legitimate ground on the basis of which the data could be processed (*See Chapter 4.4.4*). This has also been made clear by the Court of Justice . The CJEU replied that even if data have previously been made public (and are being reproduced in 'unaltered form'), this does not preclude applicability of the DPD. To hold otherwise could lead to a situation where there would be no limits to the further processing of personal data once it has been made public. This holding implies that data subjects remain protected by the DPD even if their personal data has previously been made public.[210] In practice, this means that obtaining personal data from social networks is not considered to be a 'special case'. To the contrary, it is subject to all the standard rules described above. Hence, no exceptions can be inferred from the fact that personal data is publically available.[211] For this reason, in REVEAL the entities involved in processing personal data obtained from social networks will need to ensure compliance with the applicable laws on data protection.

Second, as earlier explained, personal data must be processed for a specified, explicit and legitimate purpose. We should, however, differentiate between the purpose of the social network provider and the purpose of any third party re-using the posted personal data. These two might coincide but they might as well have nothing to do with each other. Any further processing of personal data by third parties requires a legitimate reason for it as well as a clearly defined purpose. This purpose of third parties is not the same as the purpose of the SNS provider. Moreover, we should also take into account the original purpose that users have for interacting on social networks. It has to be kept in mind that the original purposes of users posting the data on SNSs like Facebook or Twitter differ. At the beginning it was solely to interact with friends and develop one's identity. Nowadays, however, there are multiple types of users active on social networks whose purposes range from business and marketing, to political reasons, advocacy and watchdogs as well as individuals interested in opinion mak-

207 B. Van Alsenoy, Rights and obligations of actors in social networking sites, Deliverable 6.2 of the SPION project, p. 20.

208 According to the Article 29 Working Party, data relates to an individual '*if it refers to the identity, characteristics or behavior of an individual, or if such information is used to determine or influence the way in which that person is treated or evaluated*' (Article 29 Data Protection Working Party, 'Opinion 4/2007 on the concept of personal data', WP 136, 20 June 2007, p. 10.)

209 B. Van Alsenoy, Rights and obligations of actors in social networking sites, Deliverable 6.2 of the SPION project, p. 20.

210 Court of Justice of the European Union, Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy, C73/07, 16 December 2008, in particular paragraph 50 et seq. See also A. Scheuer and S. Schweda, 'The Protection of Personal Data and the Media', Iris Plus 2011, vol. 6, p. 8 et seq.

211 See more in: B. Van Alsenoy, A. Kuczerawy, Aleksandra, J. Ausloos, Search Engines after 'Google Spain': Internet@Liberty or Privacy@Peril?, ICRI Working Paper Series, 15/2013, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2321494, pp. 5- 57.

ing and steering discussions on topics of interest. These latter groups have one common characteristic, namely, they all want to 'be heard'. Social networks, through democratization of the web and empowerment, offer a great tool to achieve this goal. There is, hence, a difference between such profiles and those of people who only want to stay in touch with their friends. Even though, in both cases these profiles contain personal data of individuals, the reasonable expectation of privacy is different.[212] This is a matter of context, which can greatly influence the level of acceptance for further processing of such data. It is crucial to highlight that in REVEAL we are primarily interested in those individuals who wish to broadcast themselves and contribute to the public discussion.

Moreover, the minimisation principle will have to be satisfied. This means that processing of personal data from SNSs should not include more data than necessary to achieve the legitimate purpose. Of course the difficulty here is to decide what constitutes a minimum. This might be a challenging task when dealing with numerous profiles, on different social networks, filled with different types of data. For this reason REVEAL should specify, for each social network, the types of data that need to be collected. This delineation should be then followed and no excessive data should be collected.

Additionally, the question has to be tackled of ensuring data subjects' rights with regard to processing of their personal data . This means guaranteeing the transparency of the whole process so as to provide the necessary information to the user, and allowing him access to data related to him. As discussed earlier, there are exceptions to this right.[213] For example, when compliance with this right (and obligation) proves impossible or would involve a disproportionate effort. The data subject should moreover be able to object to processing of his personal data if he wishes to do so. The system should also allow the user to correct any erroneous information or delete his data completely.

Moreover, attention should be paid to the special regime for the processing of sensitive data. It has to be kept in mind that any type of data that is qualified as sensitive (racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health or sex life) cannot be processed unless one of the permitting conditions is satisfied (*See Chapter 4.4.4.1*).. As was indicated above, such permitting condition occurs when sensitive data is made manifestly public by the data subject. In such cases, the general prohibition to process sensitive data is lifted.[214] This does not mean, however, that no rules apply anymore. Rather, such publicized sensitive data enters the 'standard' regime foreseen for personal data.[215] This is relevant for REVEAL, where sensitive personal data from social networks might be collected. There is no intention to target sensitive personal data but there is a strong chance that this type of data will be accidentally included. This is because some types of sensitive data can be easily implied from the information made public (e.g. racial or ethnic origin could be inferred from a profile picture).

Finally, there is another aspect of processing personal data from social networks namely, compliance with the Terms & Conditions for developers using social networks' API. This is a particularly problematic issue as such Terms& Conditions can pose great limitations to re-use of data from social networks. This topic will be further analysed at the later stage of the project and will be reported on in the next legal deliverables. Here, we should only briefly indicate one important aspect of this issue. The rules created by social network providers in their Terms& Conditions create a legally binding contract between such provider and developers using the SN API. These rules, however, do not negate the data protection obligations of application developers. In other words, the fact that SN

212 Article 29 WP Opinion 06/2014 on the notion of legitimate interest of the data controller under Article 7 of Directive 95/46/EC, p. 40.

213 See Article 11(2) DPD.

214 Greek Data Protection Authority, "protection of personal data in the frame of the European project COCKPIT", 22.02.2012, Reg.Nr. Γ/ΕΞ/1335/22-02-2012, p. 2 (in Greek).

215 A. Kuczerawy, SocIoS Deliverable D6.6, Legal evaluation and recommendations, 2013, p. 11.

providers allow developers to re-use certain data (including personal data of their users) in no way exempts the developers from compliance with the rules stated in the Directive and the national data protection laws.[216]

6 Reform of Directive 95/46/EC

Rapid technological developments and globalisation have brought new challenges to the protection of personal data[217]. Through social network sites, cloud computing, location-based services and smart cards, the scale of data sharing and collecting increased dramatically. Such types of technology allow private companies as well as public authorities to use personal data on an unprecedented scale in order to pursue their activities. All this has transformed both the economic and social life of individuals. In this 'brave new data world' we need a robust set of rules.[218] As a result, at the beginning of 2012 the European Commission proposed a comprehensive reform of the DPD of 1995. The **reform package** consists of two legislative proposals for a more comprehensive and coherent policy on the fundamental right to personal data protection in the European Union:

- a proposal for a **Regulation** on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation, referred to as the 'Regulation');[219]
- a proposal for a **Directive** on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data.[220]

6.1 Next steps in the legislative process

The Regulation has been accepted by the European Parliament on 12.03.2014. In order to become a law it still has to be adopted by the Council of Ministers. Such acceptance will be a subject to negotiations between Parliament and the Council.[221] The Council will meet in June 2014 to establish its position. However, there will also be a change of the European Parliament, due to the elections of May 2014. For these reasons the actual entry into force of the new Regulation will most likely not happen before the end of 2015.

---

216 See more in A. Kuczerawy, SocIoS Deliverable D3.5 Legal and ethical analysis, 2012, pp. 20 – 27.

217 Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions 'A Comprehensive approach on personal data protection in the European Union', Brussels, 4.11.2010, p.2.

218 Explanatory memorandum to the original proposal for a Regulation of January 2012.

219 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 (further referred to as GDPS or Data Protection Regulation), adopted on 25 January 2012, COM(2012) 11 final, 2012/0011 (COD), Brussels, http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

220 Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, adopted on 25 January 2012, COM(2012), 10 final, 2012/0010 (COD), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0010:FIN:EN:PDF.

221 Progress on EU data protection reform now irreversible following European Parliament vote, see more at: http://europa.eu/rapid/press-release_MEMO-14-186_en.htm.

6.2 Overview of the proposed Regulation

The proposed General Data Protection Regulation was introduced to initiate far-reaching changes to the existing legal framework on data protection in Europe. Below some of the most striking expected changes are listed[222], some of which have already been discussed in more detail in the previous sections:

- **One continent, one law**: the Regulation will largely harmonize data protection law among Member States;
- **Regulation instead of a Directive**: The data protection reform aims to set up a regulation instead of a directive. In this way there will be only one single piece of legislation on data protection applicable across the whole European Union. In contrast to a directive, a regulation is a binding legislative act. Therefore it must be applied in its entirety by all EU Member States. A directive, on the other hand, only sets out a goal that the EU Member States must achieve, whilst letting the Member States choose how. A regulation provides therefore more certainty and aims for more harmonisation than a directive and hence may be regarded as more desirable for the regulation of data protection in Europe.
- **One-stop-shop**: companies with operations in multiple EU Member States will be subject to the jurisdiction of only one single data protection authority; and citizens will only have to deal with the data protection authority in their Member State, in their own language;
- **Same rules for all companies, regardless of their establishment**: the same rules will apply for all companies doing business in the EU, even if the companies are based outside Europe;
- **Putting data subjects in control**: the use of consent for legitimizing data processing will be significantly restricted and the information obligation for data breaches strengthened. The Regulation states that whenever consent is required for the processing of personal data, this consent will have to be given explicitly, rather than only be assumed.[223] Where processing is based on the data subject's consent, the burden of proof rests on the controller. He will need to be able to prove that the data subject has given consent to the processing operation.[224]
- **Transparency**: The Regulation aims to provide more transparency about how personal data is handled, with easy-to-understand information, especially for children.[225]
- **A right to be forgotten**: in order to empower data subjects, they will be able to request the deletion of their personal information if there is no legitimate grounds for retaining the information;
- **Easier access to personal data**: a right to data portability will ease the transfer of personal data between service providers;
- **Data protection first**: principles as 'privacy by design' and 'privacy by default' will become essential ground rules in EU Data Protection;
- **Lower administrative burden**: certain bureaucratic requirements, such as the notification of data processing to the data protection authorities (DPAs) will be eliminated;

222 According to the EC press release "Why do we need an EU data protection reform?", http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/1_en.pdf
223 Article 4(8) of the Regulation.
224 Article 7(1) of the Regulation.
225 Recital 38 of the Regulation.

- **One single national data protection authority**: The Regulation states that companies will only have to deal with a single national data protection authority (single point of contact), even when their personal data is processed outside their home country. This means that only one single data protection authority will be responsible for a company, even when this company is operating in several countries (one-stop-shop). This will be the data protection authority where the company has its main base.[226]
- **Data Protection Officer**: companies with more than 250 employees or companies with data processing as their core business activity, will have to appoint a data protection officer;
- **Cooperation between authorities**: The Regulation aims for an enhanced cooperation between data protection authorities on cases with a wider European impact, to ensure the consistent application of rules across the European Union.[227]
- **Effective sanctions**: administrative fines for data protection violations could range up to 5 percent of a company's annual worldwide turnover.

Also, the Regulation provides clear rules on when EU law applies to data controllers outside the EU. This means that the EU regulation may also apply to companies not established in the EU, if they offer goods and services in the European Union or monitor the online behaviour of citizens.[228]

The Regulation aims to increase the responsibility and accountability for those processing personal data. Therefore the proposal requires that companies processing personal data which relates to more than 5.000 data subjects (during any consecutive 12-month period) should be proactive and take measures to ensure compliance with the data protection law by appointing a data protection officer.[229]

The Regulation also introduces the principles of 'privacy by default' and 'privacy by design' to ensure that individuals are informed in an easy and understandable way about how their data will be processed.[230]

The Regulation states that unnecessary formalities and other administrative and/or bureaucratic burdens and requirements, such as the notification requirements for companies processing personal data, will be removed (simplification of the regulatory environment).[231]

Finally, the Regulation states that transfers of data outside the EU should be simplified, while ensuring the protection of personal data.[232]

[226] Recital 97 of the Regulation.
[227] Recital 111 of the Regulation.
[228] Recital 84 of the Regulation.
[229] Article 25(2)(b) of the Regulation.
[230] Article 23(1) of the Regulation.
[231] Recital 97 of the Regulation.
[232] Recital 121 of the Regulation.

7 Application to REVEAL

The previous chapters of this deliverable provided a description and analysis of the existing (and future) legal framework with regard to privacy protection and processing of personal data of individuals. This is one of the crucial legal aspects in REVEAL, which will influence the further developments in the project. This is why it is tackled as a first topic in the series of legal deliverables.

In the next step, the presented legal framework must now be applied to REVEAL. The following section provides a short summary of the most important lessons learned from the previous chapters. They are presented as a short list of interim conclusions that will guide the REVEAL Consortium in future actions. They should be read together with the previous chapters as without them these conclusions might seem as a simplification of the issues at stake.

- REVEAL partly aims at obtaining personal data of individuals for analysis purposes. This could be either the real identity of individuals or metadata which could indirectly lead to the identification of individuals. This is the case in both, the news and enterprise scenario, in which the end users want to know the identity of the sources/contributors and possibly create their profiles;

- According to the broad definition, the activities that will be undertaken in REVEAL with regard to personal data are considered 'processing' of personal data;

- The majority of this personal data will be obtained from social media networks. The fact that personal data was made public on social media networks (or anywhere else) does not mean that the data protection regime stops applying. Particularly, the principles of personal data processing, the obligations of data controllers as well as the rights of data subjects stay in tact and need to be given full attention;

- One of the main points to determine at this stage of the project is the legal ground for processing personal data in REVEAL. Due to the nature of the project, it seems at this stage that the only options we can rely on are: a) consent, and b) legitimate interest of the controller. Currently, it seems that we will use a combination of these two grounds, depending on the scenario. This however posts several research questions that will have to be addressed in the project. Mainly, in the planned environment: 1) how do we request consent that will be valid, 2) how do we comply with the obligation to inform data subjects about the processing of their personal data when this data is not collected directly from them;

- Currently, it is foreseen that the position of the data controller with regard to the REVEAL platform will be played by ATC. This is because the platform will be integrated and implemented in Greece. For this reason the applicable law is the one of Greece.

It should be clarified that the presented conclusions refer solely to REVEAL as a research project. In the exploitation phase, these formal settings will have to be re-evaluated, taking into account an entity that would be deploying the platform, its location, purpose, etc.

Apart from the rules on privacy and data protection, the results of REVEAL will also depend on other legal aspects. Specifically, we will need to take into account rules on intermediary liability, media law and copyright law. Moreover, in the design process we will need to consult the Terms & Conditions for social networks' APIs. These rules, set up entirely by social media providers, create additional limitations that cannot be ignored in REVEAL. These aspects will be further analysed and presented through internal project reports and in the next legal deliverables.

7.1 Legal evaluation of the user requirements

The following section provides an initial legal analysis of the REVEAL user requirements presented extensively in deliverable D1.1. The conducted evaluation focuses on the provided user scenarios, rather than specific requirements. This is because at the current stage of the research the requirements are presented more in a form of ideas or concepts. Additionally, not every single requirement triggers legal consequences. Moreover, an indication of a bare user requirement might not be sufficient for a detailed legal analysis. In order to properly assess the legal impact of the requirements a specific description is required of a technology that will be used to achieve the desired goal. For these reasons the legal evaluation points out the possible legal issues that need to be taken into account in relation to each scenario. These scenarios, together with the identified user requirements will evolve during the project lifetime. A more in-depth examination of the legal issues involved will, therefore, be conducted at a later stage of the project.

The indicated legal issues will inevitably appear whatever form the requirements will take. They involve mainly the issues of privacy and data protection, media law, intermediary liability and intellectual property law. Privacy and data protection law was explained in the presented deliverable. Other issues, mentioned above, will be in the focus of the next legal deliverables. In order to ensure that the end result of REVEAL is legally compliant and does not infringe any rights it is necessary to ensure that these aspects are taken into account from the very beginning of the project's developments.

7.2 News scenario

Section 3.1 of deliverable D1.1 provides an extensive presentation of the news scenario. It was split into a series of mini scenarios that are tightly focused on specific end user challenges and that can be seen as typical journalistic workflows. These mini scenarios focus on: newsgathering support, revealing the contributor, and revealing multi-media content (e.g. picture and text), as well as revealing locations (mapping workbench and trending workbench). For each mini scenario a number of user requirements were provided.

As indicated above, there are several areas of law that need to be taken into consideration in the news scenario. Legislation specific for each area will influence the further development of user requirements, scenarios and ultimately the REVEAL platform. The most relevant areas of law include privacy and data protection law, copyright law, intermediary liability, and media law. Moreover, compliance with the social networks' Terms & Conditions for API developers is an important aspect that might shape the final outcome of REVEAL.

Privacy and data protection issues are considered to be one of the crucial aspects in this project. This is because they are most likely to affect the fundamental human rights of individuals. In order to deliver a legally compliant platform the rules described in chapter 4 of the present deliverable must be adhered to. Respect for the applicable data protection law is the best method of mitigating risks of data protection breach. Apart from the described principles, obligations and rights, the REVEAL Consortium will need to pay close attention to the following issues.

As was indicated above, some of the activities taking place at the REVEAL platform will constitute the processing of personal data. Some of this data will be obtained indirectly from the data subjects, specifically, from their social networks' profiles. We need to ensure, hence, that the REVEAL platform has a legitimate legal ground for such processing. In the news scenario, REVEAL will mainly

target individuals who want their views and comments to be known by a broader public, often as large as possible (see for this also the concept of citizen journalism or user-generated content as a news source or alternative information channel). Therefore, we need to take into account their reasonable expectation of privacy. This is not the same as the expectation of people who use social networks only to stay in touch with their friends, or for exchanges of a more private nature. For these reasons, it seems likely and advisable that we will base the activities described in the news scenario on the legitimate interest of the controller. This legitimate interest should be further specified, for example as delivering a platform for innovative media production that would provide a voice to the numerous sources of information by avoiding the traditional information gatekeepers.

Collecting personal data indirectly from the data subjects is linked to an obligation to provide the affected individuals with specific information. In REVEAL, we will investigate to what extent we can rely on the exception from this rule. Compliance with this obligation is not required if it proves to be impossible or would involve a disproportionate effort. Contacting every individual whose profile shows up in the search, for example, constitutes such disproportionate effort in our opinion.. This could be compared to the situation of search engines, that are generally not expected to inform every person indexed by them.

Additionally, we need to make a distinction between searching for contributors and contributors' messages with the use of REVEAL and actually using the found information about specific individuals. In the latter case, interference with this individuals' privacy is greater. This activity, however, should be attributed to a journalist who makes such a decision and not to the provider of the REVEAL platform. The role of the data controller, therefore, is played by a different entity than in case of searching for contributors. When deciding to use personal data of an individual, the journalist become a separate data controller. In such a position, he should base the intended processing on a separate legal ground. The data controller's obligations of a journalist might depend on several issues, such as nature of the news material (e.g. investigative journalism, matters of public interest, celebrity news etc.), type of event (e.g. war, conflict, urgent matter) and the specific regulations for journalists in the data protection law. [233] Pursuant to the latter, he might be exempt of some of the data processing obligations (or have to comply with additional ones). This is, however, a matter of national legislation transposing article 9 of the Data Protection Directive (see section 4.4.5 and section 5.3). This national legislation will be further examined in the project's lifetime. In order to have a full picture of the situation we will additionally examine sources in the area of media law, such as policy documents, internal rules and guidelines, press code, code of ethics etc.

Due to all the issues related to the privacy protection and processing of personal data, it is advisable for REVEAL to establish its own Privacy Policy. In such a policy, all the relevant information should be provided to the data subjects and other interested parties in a clear and transparent manner.

The news scenario also creates certain challenges in the area of copyright. Finding content available online does not mean that such content can be freely (re-)used by third parties. This is especially the case when the re-use is not for private purposes. Copyright holders should almost always be asked for permission to re-use their content (unless overruling situations apply, e.g. matters of security, risk and danger avoidance etc.). This can be omitted only in some specific cases (see above), when the content is in the public domain (the copyright protection expired or there never was one) or when a license is attached to the content specifying conditions for re-use. (e.g. one of the Creative Commons licences).

[233] See more in: Mosley v United Kingdom, ECtHR Judgement, Strasbourg, 10 May 2011, available at: http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-104712#{"itemid":["001-104712"]}

Another obstacle can be posed by thea fact that identifying an individual who posted certain content items does not mean that we identified the author. It will be the case in some of the situations but it is also possible that the content is posted by a person who holds no rights to the content. There is no method offered by the technology that could be used to clarify the authorship therefore it will not be dealt with in REVEAL.

These challenges, related to copyright law, will have to be taken into account by journalists in the news scenario. These issues might be particularly difficult to solve as this area of law is not fully harmonized across the EU. However, these challenges are faced by journalists in their normal work-flow already and cannot be attributed specifically to REVEAL.

Intermediary liability is another area of law that must be taken into consideration in REVEAL. An intermediary constitutes a party in-between that facilitates the provision of certain services. In this case, the services offered by REVEAL are placed between social media networks and their users on one hand, and journalists and their audience on the other. Such position could lead to a liability for third parties' content that is illegal in nature or infringes subjective rights of individuals. The European legislation on this matter has been provided in the E-Commerce Directive 2000/31/EC. This instrument offers liability exemptions to certain types of intermediaries, upon specific conditions. Depending on the implementation of the REVEAL platform, different requirements will have to be fulfilled by REVEAL to avoid possible liability for third parties' content. The main difference will be whether REVEAL will store the content found through its services or whether it will only link to it.

Social media provide application developers with free access to their data through their APIs. This access, however, comes with a number of rules and limitations, described in the API's Terms & Conditions. These Terms & Conditions might be particularly difficult to comply with because they change very frequently. Moreover, they don't guarantee any minimum access. This means that a compliant application could become inacceptable within mere months. In REVEAL, it is crucial to monitor the Terms & Conditions for the social media platforms relevant in the project. This exercise will have to be performed constantly throughout the project lifetime. It is possible that certain requirements might become difficult to realize if the access conditions change. To avoid this problem, in the exploitation phase of the project, a strategic partnership with these social networks should be considered. Such partnership provides a broader access to the social network data and a more stable business environment. However, to achieve such an upgrade a considerable fee is likely to be paid.

7.3 Enterprise scenario

The enterprise scenario is described in section 3.2 of deliverable D1.1. It consist of a number of mini scenarios related to: 'newbies', customer relation, support, analysts, positive or negative discussions, event: Innovation World, and innovation gathering.

The enterprise scenario differs significantly from the news scenario. This is because it operates in a B2B environment. This means that there is a smaller chance of involving unaware private individuals. The specific services offered by Software AG guarantee that those involved in the TECH Community or specialized social media channels are there for a very specific purpose. Moreover, the majority of them are professionals acting to realize their business goals. For this reason there are less legal challenges.

In relation to privacy and data protection, the rules described in chapter 4 of the present deliverable will have to be taken into account in the design process. However, there is no re-publishing aspect,

which makes this scenario less complicated from a legal point of view. Also, personal data that will be processed in this scenario, in most cases, will come directly from the data subjects.

Similar as in the case of the news scenario, the legal ground for processing personal data of contributors will have to be established. Similarly, it could be either the legitimate interest of the controller or consent. It seems that in the enterprise scenario the role of consent will be larger. This is especially the case when a contributor joins a community by signing up to it. At this stage, usually, these data subjects (contributors) have to accept certain rules by agreeing to the community's Terms of Service. This step offers a great opportunity to ask for consent to process personal data and provide all the necessary information. Additional section could be therefore added to the ToS to obtain consent without unreasonable burden.

In the research phase of REVEAL, the data used for the enterprise scenario is provided by the technical partner Software AG. This data has been previously collected by this partner directly from its customers. The further use of this data for the scientific research has been accepted by the Software AG's data protection officer and is conducted in accordance with the applicable German data protection law.

Despite the fact that the processing of personal data is more straightforward, REVEAL should nevertheless provide a privacy policy for this scenario, too. As in the news scenario, it should contain all the relevant information presented to the data subjects in a transparent manner.

The role of REVEAL as an intermediary will lead to the same issue as in the case of the news scenario. This is, namely, the possibility of liability for third parties' content. In order to avoid such risk, the rules of the E-Commerce Directive will be have to be taken into account. Depending on the type of service provided by REVEAL, conditions for liability exoneration will be different. This legal aspect of REVEAL will be extensively analysed in the next legal deliverables.

Similarly as in the news scenario, we will have to closely follow the Terms & Conditions for API developers. It could pose the same problems as in the news scenario. A business model for the exploitation phase of REVEAL will be developed at a later stage of the project. According to this model, a strategic partnership with some of the social networks' providers will be considered.

8 Conclusion

The presented deliverable is a first one in the series of legal deliverables in REVEAL. It provides an extensive analysis of the issues related to privacy and data protection. The relevant legislation is presented for the European Union as well as Greece, were the project will be implemented.

Deliverable D1.2 explains the basic concepts of privacy and data protection such as the notions of personal data, processing, data controller and data processor. It also discusses the principles of personal data processing, which should be treated as legal requirements. These legal requirements have to be taken into account by REVEAL from the earliest stage of development. Adhering to them is crucial to ensure legal compliance of the project with the EU and national data protection regimes. It would moreover greatly benefit the exploitation potential of REVEAL.

It should also be pointed out that the EU data protection regime is currently under revision. The proposed text of the future Regulation has recently been accepted by the European Parliament. The most relevant provisions of the Regulation have been presented in this deliverable. A more in-depth analysis will be conducted in the next legal deliverable.

Deliverable D1.2 also provided a legal evaluation of the user scenarios. Possible legal issues have been identified in the areas such as privacy and data protection, media law, intermediary liability and intellectual property. These aspects will have to be taken into account at further stages of development in order to provide a tool that is not infringing any rights.

The main focus of this deliverable is to provide explanations of the principles of privacy and data protection regulation in the European Union. Other areas of law, relevant for REVEAL, like media law and intermediary liability will be addressed immediate after the provision of this documentation.

References

Legislation

[1] Universal Declaration of Human Rights, 1948, http://www.un.org/rights/50/decla.htm.
[2] European Convention on Human Rights, 1950, http://www.echr.coe.int/Documents/Convention_ENG.pdf
[3] OECD guidelines governing the protection of privacy and transborder flows of personal data; http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf
[4] Council of Europe – ETS n°108 – Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1980, http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm
[5] Directive 95/46/EC of the European Parliament and of the Council of 24.10.1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML
[6] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (e- Privacy Directive), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML
[7] 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), http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2014-0212
[8] Law 3471, Greek law on the Protection of Individuals with regard to the Processing of Personal Data, http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/ENGLISH_INDEX/LEGAL%20FRAMEWORK/LAW_%203471_06EN.PDF
[9] Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling, https://wcd.coe.int/ViewDoc.jsp?id=1710949.

Case Law

[10] European Court of Human Rights, decision Burghartz v. Switzerland of 22 February 1994, http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-57865#{"itemid":["001-57865"]}.
[11] European Court of Human Rights, decision *Friedl v. Austria* of 31 January 1995, http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-57917
[12] European Court of Human Rights, decision Peck v. United Kingdom of 28 January 2003, http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-60898.
[13] European Court of Human Rights, decision Odièvre v. France of 13 February 2003, http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-60935.
[14] European Court of Human Rights, decision *Mosley v United Kingdom* of 10 May 2011 , http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-104712.
[15] European Court of Justice Case 29/69, Erich Stauder v. City of Ulm, 12 November 1969, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:61969CJ0029.
[16] European Court of Justice C-73/07, Tietosuojavaltuutettu [Finnish data protection ombudsman] v. Satakunnan Markkinaporssi Oy and Satamedia Oy, 16 December 2008, http://curia.europa.eu/juris/document/document.jsf?docid=76075&doclang=EN.
[17] Swedish Supreme Court, decision Ramsbro v Riksåklagaren of 12 June 2001 Ramsbro v Riksåklagaren.

Opinions

[18] Article 29 Working Party, Opinion 1/2010 on the concepts of "controller" and "processor", WP 166, 16 February 2010, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf.
[19] Article 29 Data Protection Working Party, Opinion 5/2009 on online social networking, WP 163, 12 June 2009, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf.
[20] Article 29 Data Protection Working Party, Opinion 4/2007 on concept of personal data, WP 136, 20 June 2007, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf.
[21] Article 29 Data Protection Working Party, Opinion 08/2010 on applicable law, WP 179, 16 December 2010, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_en.pdf.
[22] Article 29 Data Protection Working Party, Opinion 15/2011 on the definition of consent, WP 187, 13 July 2011, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf.
[23] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, WP 203, 2 April 2013, http://idpc.gov.mt/dbfile.aspx/Opinion3_2013.pdf.
[24] Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interest of the data controller under Article 7 of the Directive 95/46/EC, WP 217, 9 April 2014, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf.
[25] Greek Data Protection Authority, “protection of personal data in the frame of the European project COCKPIT”, 22.02.2012, Reg.Nr. Γ/ΕΞ/1335/22-02-2012, p. 2 (in Greek).

Publications

[26] L. A. Bygrave, Data Protection Law: approaching its rationale, logic and limits, Kluwer Law international, 2002
[27] A. Büllesbach, Y. Poullet, C. Prins (ed.), Concise European IT Law, Kluwer Law International, Alphen aan den Rijn, 2010
[28] R. Jay, Angus Hamilton, Data Protection Law and Practice, Thomson, Sweet and Maxwell, 2003, 2nd edition.
[29] A.Kuczerawy, SocIoS Deliverable D6.6, Legal evaluation and recommendations, 2013.
[30] A. Kuczerawy, SocIoS Deliverable D3.5 Legal and ethical analysis, 2012
[31] P. Ohm, ‘Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization’, (13 August 2009) University of Colorado Law Legal Studies Research Paper, http://ssrn.com/abstract=1450006.
[32] T. Olsen, T. Mahler, Identity management and data protection law Identity management and data protection law: Risk, responsibility and compliance in ‘Circles of Trust’ – Part II, computer law & security report 23 (2007)
[33] R. Singel, ‘NetFlix Cancels Recommendation Contest After Privacy Lawsuit’ (Wired, 12 March 2010) <www.wired.com/threatlevel/2010/03/netflix-cancels-contest>.
[34] S. Simitis, *Revisiting Sensitive Data*, 1999 (http://www.coe.int/T/E/Legal%5Faffairs/Legal%5Fco%2Doperation/ Data%5Fprotection/Documents/Reports/W-Report%20Simitis.asp#TopOfPage).
[35] Scheuer and S. Schweda, ‘The Protection of Personal Data and the Media’, Iris Plus 2011, vol. 6.
[36] O. Tene, ‘Privacy: the new generations’, *International Data Privacy Law* 2011, Vol. 1.
[37] B. Van Alsenoy, Rights and obligations of actors in social networking sites, Deliverable 6.2 of the SPION project.
[38] Alsenoy, A. Kuczerawy, Aleksandra, J. Ausloos, Search Engines after 'Google Spain': Internet@Liberty or Privacy@Peril?, ICRI Working Paper Series, 15/2013, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2321494