SEVENTH FRAMEWORK PROGRAMME

THEME ICT-2009.1.2

"Internet of Services, Software and Virtualization"

D6.5
Legal requirements and ethical issues

Project acronym: SocIoS

Project full title: *Exploiting Social Networks for Building the Future Internet of Services*

Contract no.: 257774

Workpackage:	WP6	Dissemination and Exploitation	
Editor:	Aleksandra Kuczerawy		KULeuven
Author(s):	Aleksandra Kuczerawy		KULeuven
Authorized by	Prof. Theodora Varvarigou		ICCS/NTUA
Doc Ref:	D6.5 Legal requirements and ethical issues		
Reviewer	Konstantinos Tserpes		NTUA
Reviewer			
Dissemination Level	PU		

The research leading to these results has received funding from the European Community's Seventh Framework Programme [FP7/2007-2011] under grant agreement no. 257774

SOCIOS CONSORTIUM

Beneficiary Number	Beneficiary name	Beneficiary short name	Country	Date enter project	Date exit project
1(coordinator)	Institute of Communication and Computer Systems/National Technical University of Athens	ICCS/NTUA	Greece	Month 1	Month 30
2	IBM Haifa Research Lab	IBM	Israel	Month 1	Month 30
3	Athens Technology Center	ATC	Greece	Month 1	Month 30
4	Google Ireland Limited	Google	Ireland	Month 1	Month 30
5	Cognium Systems	Cognium	France	Month 1	Month 30
6	Center for the Study of the Information Society, University of Haifa	HU	Israel	Month 1	Month 30
7	Deutsche Welle	DW	Germany	Month 1	Month 30
8	Stefi Productions S.A.	Stefi	Greece	Month 1	Month 30
9	Katholieke Universiteit Leuven (K.U.Leuven) – Interdisciplinary Centre for Law and ICT	KULeuven	Belgium	Month 1	Month 30

DOCUMENT HISTORY

Version	Date	Changes	Author/Affiliation
v.0.1	23-02-2011		KULeuven
v.0.2	26-02-2011		KULeuven
v.1.0	28-02-2011	Final document	KULeuven

The research leading to these results has received funding from the European Community's Seventh Framework Programme [FP7/2007-2011] under grant agreement no. 257774

Executive Summary

At month M06 in the SocIoS project a first set of legal requirements and ethical issues analysis is provided by KULeuven. As described in the SocIoS proposal, fundamental right to privacy is considered to be an ethical issue. For this reason, the whole presented deliverable is focused on the topic of privacy and data protection. The document provides an introduction to the subject, analysis of the relevant legislation and presentation of the legal requirements that will need to be adhered to throughout the design and implementation process of the SocIoS platform. It also identifies problems that could be encountered due to the current state of the privacy framework. Solutions that will be developed in cooperation with other Workpackages, are going to be presented in the future deliverables, mainly D3.5 Legal and ethical analysis.

It is a general conception that a project that interacts with individuals' profiles needs to satisfy a list of legal requirements. The legal partner KULeuven is responsible for the task of identifying the legal and ethical issues, providing the legal requirements, and ensuring that they are adhered to and that the ethical issues are tackled. This task will run for the full duration of the project and will coordinate the monitoring of the legal issues to continuously assess and ensure that the framework being proposed adheres to a minimum set of ethical and legal requirements. This task requires cooperation with WP2 and WP3 in ensuring that the technical requirements are legally compliant and adhere to the relevant legal and ethical obligations. The SocIoS platform will be assessed against the current legislative framework, including most importantly Directive 95/46/EC relating to the protection of personal data, and other relevant policy documents, recommendations and opinions, including Opinion 5/2009 on online Social Networks, June 2009 (Article 29 Working Party).

The initial findings are presented in this report: **Deliverable D6.5 Legal requirements and ethical issues**. The document provides a list of legal requirements for privacy protection to guarantee that these issues are handled ethically within the project. It also identifies the challenging areas and states the problems, which could be posed by the current shape of the privacy framework. The document describes the most important concepts of data protection that have to be taken into account in the design and implementation of the SocIoS platform. The deliverable describes:

- The relevant legislation in the area of privacy and data protection
- Basic concepts of privacy and data protection
- Legal requirements for privacy and data protection, more specifically the principles related to data processing and the rights of data subjects
- Other relevant issues that need to be taken into account like the concepts of transparency and privacy by design
- Relation between privacy protection and freedom of expression

The research leading to these results has received funding from the European Community's Seventh Framework Programme [FP7/2007-2011] under grant agreement no. 257774

- Review of the Data Protection Directive 95/46/EC and its possible impact
- Implications of the above points for the SocIoS project

The deliverable presents the requirements in one specific area, that of data protection. Other relevant areas are Intellectual Property Rights and the issue of liability for User Generated Content. These topics will be examined extensively in the future months of the project. The research in this regard will be performed throughout the project lifetime and the requirements for these areas will be presented in the deliverable D3.5 Legal and ethical analysis in month M23.

The research leading to these results has received funding from the European Community's Seventh Framework Programme [FP7/2007-2011] under grant agreement no. 257774

Abbreviations

CoE Convention 108	Council of Europe – ETS n°108 – Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1980
Data Protection Directive, DPD	Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
ECJ	European Court of Justice
WP29	Article 29 Data Protection Working Party
SNS	Social Networking Sites

The research leading to these results has received funding from the European Community's Seventh Framework Programme [FP7/2007-2011] under grant agreement no. 257774

Table of Contents

The research leading to these results has received funding from the European Community's Seventh Framework Programme [FP7/2007-2011] under grant agreement no. 257774

The research leading to these results has received funding from the European Community's Seventh Framework Programme [FP7/2007-2011] under grant agreement no. 257774

1 Introduction

The SocIoS project is aimed at exploiting the User Created Content and the Social Graph of users in Social Networks to create new services. The goal of the project is to provide developers with cross-platform tools that enable them to manage the dynamically generated content and complex social interactions by allowing them to build services that combine data and functionality from two or more different SNS, disregarding the underlying SN implementation. With such objective a number of legal questions arise. The main three areas that have to be tackled to ensure compliance with the existing law focus around privacy and data protection, intellectual property rights and issues regarding liability for the user generated content. These three topics will be analysed throughout the project lifetime.

The present deliverable is focused on the privacy and data protection issues. The document provides an introduction to the subject, analysis of the relevant legislation and presentation of the legal requirements that will need to be adhered to throughout the design process of the SocIoS platform. It also describes the current situation in the field of the European data protection regime where the review process of the Data Protection Directive is on going. The document indicates the most important research questions, which have to be tackled to ensure the legal compliance of the SocIoS project. Further analysis, as well as a revision of the requirements, if necessary after the review process is finished, will be presented in the next deliverable D3.5. Deliverable D3.5 will also address the issues of the Intellectual Property rights and liability issues for the User Generated Content. The legal requirements for these topics will be provided.

The goal of the SocIoS project is to use the vast content from SNS for new services such as news and complex media items creation. The possibilities offered by the constantly growing popularity of the SNSs are numerous. People all over the world use SNSs to connect with their friends (e.g. in Facebook, LinkedIn, NetLog), to exchange news and opinions, and to communicate to others about events they participate in (e.g. Twitter). A re-use of a content generated from these platforms presents a great risk of privacy violations. The reason for this is that many of the SNS users provide access to their personal data on their profiles. This could refer to their full names, address and telephone numbers but it could also reveal their sensitive data like political opinions, beliefs or information related to their health, or sex life. This situation requires implementation of adequate privacy safeguards in order to deliver a socially, and legally acceptable prototype. Services which are willing to use the User Generated Content from SNSs have to be aware that when they are processing personal data of individuals, they become addressees of the data protection regulations. This means that they are responsible for the compliance with the specific law for the data processing activities. The present deliverable aims to clarify the possible ambiguities that might be a result of this situation. It also provides the legal requirements for personal data processing, which need to be taken into account at the earliest stage of the design of the SocIoS platform.

2 Relevant legislation

2.1 Article 8 ECHR: the right to privacy

The right to privacy is described in Article 8 of the European Convention on Human Rights (hereinafter 'ECHR'). It ensures the respect for individual's private and family life, his home and his correspondence. The fundamental concept of Article 8 has been formulated in terms of protecting 'the individual against arbitrary interference by the public authorities in his private or family life'. The main goal of the right to respect for private life is to secure a sphere within which the individual can freely pursue the development and fulfilment of his personality[1]. But this right does not only refer to the safeguarding of a sphere of seclusion in which the individual may act autonomously, 'it also gives some protection for inter-personal relationships both inside and outside the domestic realm'[2].

With the time it became clear that the mere recognition of the general principle of privacy is not sufficient to effectively protect this fundamental right. For this reason the European Court of Human Rights has progressively incorporated data protection within the scope of Article 8 ECHR. Such an approach was based on the principles established by the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS n°108 (hereinafter 'CoE Convention 108') (Leander, 1987; Rotaru vs. Romania, 2000). This document is considered as the first European legal framework for the fundamental right to protection of personal data. In the Marper case (2008, §67) the Court held that 'the mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8. The subsequent use of the stored information has no bearing on that finding'.

A limited number of exceptions to this right is foreseen by Article 8.2, which states that '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.'

[1] BYGRAVE L., Data protection pursuant to the right to privacy in Human Right treaties, International Journal of Law and Technology, 1998, volume 6, pp. 247-284, http://folk.uio.no/lee/oldpage/articles/Human_rights.pdf

[2] BYGRAVE L., Data protection pursuant to the right to privacy in Human Right treaties, International Journal of Law and Technology, 1998, volume 6, pp. 247-284, http://folk.uio.no/lee/oldpage/articles/Human_rights.pdf

Article 8.2 stipulates that the right to privacy is not unconditional and has to be put in balance with other interests. Derogations are therefore limited to specific situations and have to comply with the criteria defined by the ECHR.

2.2 Articles 7 and 8 of the Charter of Fundamental Rights of the European Union

The Charter of Fundamental Rights of the European Union (hereinafter 'EU Charter') was introduced in December 2000. The Charter includes the explicitly stated right to respect for privacy (Article 7) and a right to personal data protection (Article 8). Since the entry into force of the Treaty of Lisbon (1st December 2009), the provisions of the Charter became legally binding in all EU Member States (see Article 6.1 of the Treaty of the European Union). The Lisbon Treaty introduced a new horizontal approach to data protection and privacy and provided for the necessary legal basis (Art. 16 TFEU) "to get rid of the existing differences and divergences which prejudice a seamless, consistent and effective protection of all individuals"[3]. Article 16 TFEU extends the scope of the EU data protection regime to the third pillar (police and judicial cooperation in criminal matters), but also to the second pillar (common foreign and security policy), which previously was excluded. The scope of application of the EU Charter is, however, restricted solely to EU institutions processing personal data and to the implementation of EU law in Member States. The ambit of the instrument is hence not as far-reaching as the ECHR. However, coherence and continuity between the two documents is ensured. According to Article 52 (3) of the Charter, insofar as the Charter contains rights corresponding to those in the ECHR, the meaning and scope of those rights shall be the same as in the ECHR. Furthermore, whereas article 7 of the EU Charter recognises a right for private and family life, using the exact same wording as article 8.1 ECHR, it should be interpreted in the light of the ECHR case-law on Article 8. The EU Charter however, through its Article 52, allows European law to provide more extensive protection.

Article 8 of the EU Charter states that '1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority.'

The explanation to this article is very limited. It points out to Article 286 of the Treaty establishing the European Community, Article 8 of the ECHR and the CoE Convention

[3] Article 29 Working Party, The Future of Privacy, Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, WP 168, 1 December 2009, p.7

108 as the sources of its wording. Moreover, it indicates that the right to protection of personal data is to be exercised under the conditions laid down in the Data Protection Directive. The right may be limited under the conditions set out by Article 52 of the Charter. No additional information, however, is provided. For this reason it is necessary to refer to the provisions of the Data Protection Directive (infra) and where relevant of the CoE Convention 108 to specify the content of the rights.

The derogations to the right are not listed in the Article 8 of the Charter and they have to be looked for in Article 52, which defines the general conditions under which the exercise of the rights and freedoms recognised by the Charter can be limited. Such interference with the rights is possible when it is provided for by a law, and respects the essence of those rights and freedoms. The principle of proportionality should be complied with when limiting the right to privacy. Moreover, it should be done only if it is necessary and when the objective of general interest recognised by the Union or the need to protect the rights and freedoms of others is met. This means that despite the different wording of the derogation and the lack of a closed list of reasons, conditions for derogation to the right to privacy as provided for by the EU Charter are substantially similar to those listed in Article 8.2 ECHR. However, the mentioned differences might lead the European Court of Justice to come with different and innovative case law.

2.3 The European data protection framework

The Core of the European data protection legislation consists primarily of two different instruments: the Coe Convention n°108 mentioned above and the European Union's Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereafter referred to as the 'Data Protection Directive', 'Directive', or 'DPD'). The general Data Protection Directive is complemented in the area of the electronic communications by the Directive 2002/58[4] (commonly known as the ePrivacy Directive). Important provisions, to some extent, can be also found in the Directive 2000/31/EC on Electronic Commerce and the Directive 1999/93/EC on Electronic Signatures[5]. All of these instruments have influenced and inspired national legislations in the area of privacy and data protection in Member States.

[4] Directive 2002/58/EC of 12 July 2002, concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communication), O.J. L 201/37, 31 July 2002, replacing Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 on the processing of personal data and the protection of privacy in the telecommunications sector.

[5] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, Official Journal L No. 13, 19.01.2000, p. 12.

The Data Protection Directive is the most comprehensive and complex of these instruments as it provides a general framework on processing of personal data. The document establishes a set of rules capable of broad application and impact. Its objective is to ensure that the rights of the individual on his personal data have a uniform level of protection across the EU and to ensure that such data can move freely within the single market of the European Union. This means that the purpose of the Directive is twofold. "The establishment and functioning of an internal market requires that personal data should be able to flow freely from one Member State to another, while at the same time a high level of protection of fundamental rights of individuals should be safeguarded"[6]. The Directive extends and adapts the principles set out by the CoE Convention 108. However, it aims for a real harmonization of data protection rules within the European Union, which the CoE Convention did not manage, mainly because of its broad formulation. Recital 11 of the Directive links both norms and states that 'whereas the principles of the protection of the rights and freedom of individuals, notably the right to privacy, which are contained in this Directive, give substance to and amplify those contained in the Council of Europe Convention of 28 January 1981 for the protection of Individuals with regards to Automatic processing of personal data.'

The interpretation of the provisions of the EU Privacy framework is delivered by the Article 29 Working Party, an independent EU advisory body on data protection and privacy composed of representatives of national data protection authorities. It seeks to harmonize the application of data protection rules throughout the EU, and publishes opinions and recommendations on various data protection issues. These opinions indicate the trends and directions of the privacy and data protection in the EU. They provide a deep analysis of very specific issues and for this reason they will be often called upon. For the SocIoS project the most important documents include for example Opinion 1/2010 on the concepts of 'controller' and 'processor' of 16 February 2010, Opinion 5/2009 on online social networking of 12 June 2009 and Opinion 4/2007 on the concept of personal data of 20 June 2007.

In the following section an analysis of the provisions of the Data Protection Directive is presented. The basic concepts and main principles of privacy protection are provided with the indication of specific problems that might occur in the frame of the SocIoS project. The identified issues will be researched throughout the project lifetime as the technology will be developed. The research on these topics will be further developed in the future deliverable D3.5.

[6] Article 29 Working Party, The Future of Privacy, Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, WP 168, 1 December 2009, p. 6.

3 Basic concepts of privacy and data protection

The main questions that have to be answered to assess the applicability of the European Data Protection framework to the SocIoS project is whether personal data of SNS users will be processed in the project. It is important not to forget also about a special category of personal data, called sensitive data, the processing of which requires the application of a special protection regime. In order to clarify the situation it is necessary to introduce the main concepts of data processing.

3.1 Personal data

'Personal data' is defined in Article 2 (a) of the Data Protection Directive as any information relating to an identified or identifiable natural person ('data subject'). Furthermore the same Article explains that 'an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity'.

In order to assess if a person is identifiable, Recital 26 of the DPD explains that account should be taken of 'all the means likely reasonably to be used either by the data controller or by any other person to identify the said person'. It is thus considered that 'as such, identification does not require knowledge of a person's name but it does require knowledge of some unique characteristics of the person relative to a set of other persons. What is of legal importance is the capability or potentiality of identification rather than the actual achievement of identification. Hence, data will not fail to be personal merely because the data controller refrains from linking them to a particular person.'[7] The means employed by the controller to identify individuals should hence be assessed according to a proportionality criterion. In other words, data will not qualify as 'personal' if the process of identification requires the controller to deploy disproportionate efforts.

In the opinion of the Article 29 Working Party, a mere hypothetical possibility to single out the individual is not sufficient to meet the criteria of this provision[8]. A series of additional factors should be taken into account. The Working Party lists them as the cost of the identification, the intended purpose of the processing of this information, the way the processing is structured, the advantage expected by the controller, the interests at stake for the individuals, as well as the risks of organisation dysfunctions (such as breaches of confidentiality duties) and technical failures[9].

It is evident that this concept of personal data is rather broad. For this reason it might be hard, in some cases, to determine if a certain type of information actually allows to identify a person. Very often it might be difficult to assess whether the obtained information constitutes personal data as there is no enumerative list of such data. The concept of

[7] Bygrave L. A., Data Protection Law: approaching its rationale, logic and limits, Kluwer Law international, 2002, p.43-44.
[8] Article 29 Working Party, Opinion 4/2007 on the concept of personal data, WP136, 20 June 2007, p. 15.
[9] Article 29 Working Party, Opinion 4/2007 on the concept of personal data, WP136, 20 June 2007, p. 15.

personal data is subject to a constant transformation due to societal, cultural, technology or economical changes. This could happen for example in a situation when a certain type of data, not used before, is being introduced and commonly used to identify people. Moreover, although a singular piece of information about a person might not be enough to identify him or her, in a contextual perspective this might change. In other words a piece of information that on its own seems to be irrelevant, could in combination with other pieces of information of the same type provide sufficient knowledge about a user to identify him or her. In this situation such combination of data could be protected as well.[10] In the SocIoS environment it has to be borne in mind that the tools developed following the end user requirements (see deliverable D2.1) will possibly allow access to personal information. However, in many situations it might be difficult to assess, whether the search result constitutes personal data, as explained above. If functionalities developed in the project allow to access information about a person's full name, his current residence place and involvement in certain clubs, interests groups or events it would be considered as accessing personal information. This will, in consequence, mean that obligations from the data protection legislation will have to be adhered to. This seems to be particularly interesting question in case profiling systems will be designed. Data gathered with such methods might not always constitute personal data as the profiles are very often built basing on a great amount of non-personal data. However, the extensive range of this information will most of the time be more than enough to identify an individual. The question that will be analysed in the further stage of the project is whether such collection of non-personal data, that allows for identification of an individual, should possibly be covered by the data protection rules, foreseen for personal data in the strict understanding.

An important aspect of protection of personal data refers to a situation when this type of data is made public on the Internet. This might be seen as a permission of the data subject for others to process the data. As data subjects consciously publish their data on line, in some opinions, it is considered as their consent for further processing. This however is not the case. Even though the data is basically 'out there', and is easily available for re-use, especially for technically advanced parties, there still exist legal constraints for processing of such data. In other words, the fact that data is published on the Internet does not mean that it is freed from the protection foreseen by the law. If such data is to be used, all the rules of the data protection law apply. This means, among others, that the processing needs to be based on one of the legal grounds, and that the purpose of the processing has to be compatible with the original purpose of the processing (infra). This aspect of data protection will be referred to further on in this deliverable.

3.1.1 Anonymous data

As defined by the Data Protection Directive, anonymous data is any information relating to a natural person who is no longer identifiable (Recital 26). According to the WP29, a case-by-case analysis should be carried out to check whether identification of a person to whom it was related is no longer possible. The results of such analysis are always dependent on the circumstances of the case. Only in cases where full anonymysation is ensured, i.e. the

[10] Kuner C., European Privacy Law and Online Business, Oxford University Press 2003, p. 51

information cannot be traced back to the individual in any way, the data protection framework ceases to apply.

3.1.2 Processing of personal data

The definition of data processing, contained in Article 2(b) of the Data Protection Directive, is very broad and covers any type of activity performed upon data. According to the Directive processing of personal data means 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. This extremely broad definition makes it very difficult to argue that any type of use of personal data obtained with the help of the SocIoS platform and its specific search functionality does not constitute an act of data processing. What follows is a necessity to comply with the list of obligations imposed on data controllers (infra) by the data protection regulation.

The Directive applies 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 filling system or are intended to form part of a filing system (Art. 3 of the Data Protection Directive). According to this article, the scope of the Directive extends to manual data processing whenever data are stored in a filing system or they are intended to be stored in a filing system.

In result of such a broad definition, the mere collection of information or the process of anonymisation is qualified as processing within the meaning of the Data Protection Directive. The data protection framework will therefore apply whenever such processing activities are performed on personal data.

3.1.3 Grounds for processing of personal data

Article 7 of the DPD describes the legitimate grounds of data processing. This refers to situations when 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'[11]. 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. Consent can be manifested either implicitly or explicitly. Such consent means 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 (Article 3 (h) of the Data Protection Directive). Consent should not be 'silent', as even an implicit type of consent requires some kind of 'active' reaction. Moreover, it should

[11] Jay R., Angus Hamilton, Data Protection Law and Practice, Thomson, Sweet and Maxwell, 2003, 2nd edition, p.178.

be possible to withdraw consent at any moment, after which the processing becomes unlawful (see more in Section 4.2 on Data Subject's Rights). It should be highlighted that contrary to the German doctrine of 'information self-determination', the power of consent is not over-emphasized by the Directive. All legal grounds for the processing have the same status.

Data can be processed also if the processing is necessary for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering into a contract. This ground refers to a 'contract between the data subject and the controller which can be only fulfilled if the controller processes certain data about the data subject'. This refers to contracts the primary subject of which is not data processing, but the processing is necessary to fulfill the contract, like for example booking plane tickets. There are some similarities to the previous ground as entering into a contract could be seen as implicit consent to data processing.[12] Moreover, personal data can be processed when it is necessary for compliance with a legal obligation to which the controller is subject. The data can also be processed if it is necessary in order to protect the vital interests of the data subject. The processing can only be based on this ground whenever it is essential for the life of the data subject and it is a matter of life and death, so it should be interpreted narrowly. The processing of personal data is allowed when it is necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed. Finally, it is possible as well if it is 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, provided this is not incompatible with the interests or the fundamental rights and liberties of the data subject. In the SocIoS project the most likely legal ground for processing of personal data is the consent of the user. The reason for this is the fact that all the other legal grounds are too specific and most probably will not occur in the SocIoS case.

3.2 Sensitive data

Special attention should be paid to the concept of 'sensitive data'. According to Article 8 of the Data Protection Directive, the processing of 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 is prohibited.

This approach is a result of an opinion that the processing of these types of data is more privacy-invasive and presents a high risk of infringing fundamental freedoms or privacy (recital 33). The list is enumerative, which means 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.[13] The protective approach of the Directive prohibits the processing of sensitive data unless the controller could obtain consent of the data subject - prior to the processing and explicit. This strict regime is however softened by exemptions, foreseen in respect of specific needs. On the grounds of important public

[12] Kotschy W., in: Büllesbach A., Poullet Y., Prins C. (eds.), Concise European IT Law, Alphen aan den Rijn, 2005, p. 48.
[13] SIMITIS S., *Revisiting Sensitive Data*, 1999.

interest, Member States are therefore authorised to derogate from the prohibition, whenever they provide specific and suitable safeguards so as to protect the fundamental rights and the privacy of individuals (Recital 34). In result, the Data Protection Directive defines specifically in which cases processing of these data is allowed.

Controllers are permitted to process sensitive data when the data subject has given his explicit consent or the processing 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.
- when the processing of the data is required for the provision of care or treatment where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.
- 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 authorised by national law providing for adequate safeguards.
- the processing 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.
- the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims.

At the current stage of the project it does not seem that any of the exceptions is applicable to the data processing activities that will be performed in the SocIoS project. This means that data processing activities involving sensitive data will have to rely on the explicit consent of users.

It should be highlighted that also additional exemptions are possible, if they are introduced either by national law or by decision of the supervisory authority, whenever they provide for suitable safeguards. Moreover, national legislations may contain additional requirements for the collection and processing of sensitive data. Such is the case for example in Belgium or Spain where the written consent of the individual is required prior to the processing of sensitive data.

In the light of the SocIoS project it is very likely that processing of sensitive data, which could reveal political opinions, religious or philosophical beliefs, trade-union memberships or even racial of ethnic origin, will occur. Such question should be always tackled on a case-by-case basis, nevertheless general guidelines will be provided in the context of this project.

SocIoS data processing activities involving the processing of sensitive data should be based on prior consent. The manner in which the prior consent of the individual should be obtained is an issue that a solution will have to be found for. This may become problematic,

especially when national laws require the gathering of written consent. Also, a question how to prove that consent has been given will have to be answered. This will usually depend on whether national legislation acknowledges digital documents as written documents. Solutions which have been proposed in other fields such as in e-banking will be explored.

3.3 Data controller and processor

The Data Protection Directive defines two main roles in data processing activities, that of data controller and data processor. This distinction shapes the legal obligations that the entity processing the data should comply with. According to Article 6 (2) the controller should ensure compliance with the main principles of data processing. This means in practice that the responsibility for compliance with the conditions for lawful processing is assigned to the controller.

A data controller, according to the Data Protection Directive, is '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'. The SocIoS end-users will most likely be in the position of a data controller as they are the party taking a decision about the purposes and means of the processing of personal data – so what for the data is used and how.

The processor is 'the natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller'. The role usually played by the processors could be described as sub-contractors who perform particular processing tasks on behalf of the controlling entity and according to the given instructions. Moreover, the task of the processor is also to ensure the security of the personal data they processed.

The core criterion to distinguish controllers from processors is the actual possibility to decide upon the purpose and the means of the processing. This analysis however needs to be performed on a case-by-case basis. Rapid technological development entails that the boundaries delineated for the traditional roles of the controller and processor become blurry. Due to arising difficulties in assigning roles in a data processing operation, a helpful hand came in a form of a recent opinion of the Article 29 Working Party. The document provided extensive explanation of the old terms and clarified the criteria for interpretation.[14] More specifically, the Article 29 WP points out several elements, like for example the degree of actual control exercised by a party, to facilitate the whole process.

The clear division of the roles of parties involved in the processing is an activity necessary for the correct allocation of the responsibility for the compliance with data protection rules. As was stated above, it is the controller who is the main responsible actor in the data processing with the processor's role being rather secondary – he processes the data on behalf of the controller. This means that he is not determining the purposes and means of the processing, he merely follows the instructions. Here it should be mentioned that apart from the difficulties with clear distinction between a controller and a processor even more

[14] Article 29 Working Party, Opinion 1/2010 on the concepts of 'controller' and 'processor', WP166, 16 February 2010.

complications are possible, in a form of a joint controllership. Such a situation occurs when several parties together define the purposes and means for the processing. In this case the responsibility falls on all of the entities involved. It is also possible that various controllers will be liable for the processing of personal data at different stages of the processing and to different degrees. This means that it is possible to allocate compliance with data protection rules and responsibilities for breach of these rules to entities performing specific tasks. It is then crucial to provide the data subject with information about which entity is responsible in each case, especially for the exercise of their rights (access, rectification, objection, deletion).

In the framework of the SocIoS project the likelihood of this situation will be analysed as there will be many parties involved in the process and their roles have to be described to ensure compliance with the existing law. An extra factor of complexity is caused by the fact that partners are based in different Member States. According to Article 4 of the Data Protection Directive (see below in section 3.7), each Member State shall apply its Data Protection Act where the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State. In other words, specific national laws are applicable to the collection and processing of personal data carried out by controllers established within their territories.

The controllership of each partner of SocIoS will have to be described carefully on a case-by-case basis. Partners that are involved in determination of purposes and means of processing, on different stages of the process, like in collection and storage of the data, will need to comply with different national legislations due to their different locations. This means that these partners will be obliged to comply with data protection legislation of the countries of their establishment (see more on the applicable law below, Section 3.7). They will be also responsible for the notification to the data protection authority of their country. It is advised that the collected personal data would then only be shared with other partners, if required, after being anonymised. Such anonymisation is meant to enhance the privacy and reduce the risk of the confidentiality breach.

It has to be also emphasized that solely in case of true anonymisation, so when i.e. the information cannot be traced back to the individual in any way, the data protection framework cease to apply.

3.4 Exemptions

The Data Protection Directive excludes from its scope of application the processing of personal data in two cases. First, if the processing is performed by a natural person in the course of a purely personal or household activity. According to Recital 12 of the Directive the processing of data carried out by a natural person should be excluded, if it is done in the exercise of activities which are exclusively personal or domestic, such as correspondence and the holding of records of addresses. However, the application of this rule seems to be problematic as there are many uncertainties about what constitutes ‘personal use’. In the constantly developing information society, where everything is connected to everything else, the boundaries between personal use and commercial services tend to blur. The reason

for this is that there are more and more services, which enable people to store their personal details, and other type of information online, to make it reachable everywhere.[15] In the ECJ ruling Bodil Lindqvist[16], the Court held that this exception could only apply to activities which are carried out in the course of private or family life of individuals, excluding the publication of personal data on the Internet 'so that those data are made accessible to an indefinite number of people'.[17] This exclusion will not be applicable to SocIoS data processing activities as they will not be carried out in the course of private or family life of individuals.

The second exemption occurs in the course of an activity which falls outside the scope of Community law. This provision refers to activities such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defense, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law. With regard to this exception some questions have been asked about further transfer of personal data for purposes falling outside the scope of application of the Directive. In the Passenger Name Records (PNR) Case[18] where the ECJ examined the legitimacy of transfers of passengers' information to law enforcement authorities, the Court ruled that the application of the Directive to the processing will be determined by the purpose of such processing. In this case, the personal data collected and processed with commercial purposes by air companies were falling under the scope of the Directive. However, their further transfer to law enforcement authorities for national security purposes was deemed to fall outside the provisions of the Directive. This exemption is also unlikely to apply to SocIoS activities.

Since the entry into force of the Lisbon Treaty, which eliminated a division into three pillars, the data protection regulation of the EU is extended to the area of police and judicial cooperation and common foreign and security policy (the former third and second pillar). Currently, the situation in the former third pillar 'can be described as a patchwork of data protection regimes, which are applicable in different situations'[19]. The Commission addresses this issue in the on-going review of the Data Protection Directive. As mentioned above, the activities from the area of the former second and third pillar should not be in the scope of the SocIoS project.

[15] Terstegge J., in: Büllesbach A., Poullet Y., Prins C. (eds.), Concise European IT Law, Alphen aan den Rijn, 2005, p. 38.
[16] ECJ, Bodil Lindqvist, C 101/01, E.U.O.J. C 7 of 10 January 2004, p. 3. For an analysis of this case see e.g. VAN ALSENOY B., BALLET J., KUCZERAWY A., DUMORTIER J., *Social networks and web 2.0: are users also bound by data protection regulations?*, Identity in the Information Society, Volume 2, Number 1 / December 2009, pp.65-79.
[17] Terstegge J., in: Büllesbach A., Poullet Y., Prins C. (eds.), Concise European IT Law, Alphen aan den Rijn, 2005, p.38
[18] Judgment of the Court of Justice in Joined Cases C-317/04 and C-318/04 (30 May 2006).
[19] Article 29 Working Party, The Future of Privacy, Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, WP 168, 1 December 2009, p. 7.

3.5 Applicable law

The applicability of specific national laws on data protection is regulated in Article 4 of the Directive. According to the provision national regulation on data protection of a Member State applies in three cases. First of all, it applies if the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State. This means that the data controller has to comply with the national law of the country where it has its main place of establishment. 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 applicable national law. The second part of Article 4.1 (a) requires the data controllers to comply with all the laws of countries, in the territory of the EU, where they conduct their business, with regard to the data processing activities taking place in these countries. This is a strict employment of the 'country of origin' principle in the area of data processing. As explained in Recital 19, 'when a single controller is established on the territory of several Member States, particularly by means of subsidiaries, he must ensure, in order to avoid any circumvention of national rules, that each of the establishments fulfils the obligations imposed by the national law applicable to its activities'.

The national law applies also when 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. This provision refers to situations when the controller is based on the territory of an embassy or a consulate of a Member State. This case will most likely not occur in the SocIoS project.

The national law of the Member States applies as well if 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. This however is not the case if such equipment is used only for purposes of transit through the territory of the Community. This provision makes the controllers from outside of the EU compliant to the law of the Members States on the territory of which they use equipment for the processing purposes. Here, the opinion of the Working Party 29 should be recalled stating that 'cookies' constitute a type of equipment the use of which results in the application of the national law of the country where the user's personal computer is located[20]. This is a complex problem, which will not be extensively analysed here.

The relevance of the issue of controllers based outside of the EU, for the SocIoS project, is significant as there are two consortium partners based in Israel. However, the processing in which these two partners will be possibly involved, will not take place on the territory of the EU. Most likely, these partners will be performing data processing activities on personal data

[20] Art. 29 Data Protection Working Party, Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites, WP 56, adopted on 30 May 2002, p. 9; Art. 29 Data Protection Working Party, Opinion 1/2008 on data protection issues related to search engines, WP 148, adopted on 4 April 2008; Art. 29 Data Protection Working Party, Opinion 5/2009 on online social networking, WP 163, adopted on 12 June 2009;

of the data subjects from their country, on its territory. In case personal data of data subjects from the EU, where other partners are established, will be sent for processing in Israel, the rules on data transfers have to be presented.

It needs to be stated that even though the rules of Article 4 are often considered as leaving room for different interpretations[21], especially in more complex situations, the applicability of the EU data protection regime in SocIoS project is clear. The provision of Article 4.1 (a) bears significance for the project as it allows to establish, that each partner of the consortium will be responsible for legal compliance with its own national data protection regulation for the processing activities it might perform, on personal data collected from data subjects in its country. Transfer of these data for further processing in other Member States does not seem to be problematic, from the legal perspective. In order to enhance the level of protection for the data subjects, however, anonymisation of data sets collected by each partner before forwarding it to other partners would be advisable.

3.6 Transfer of personal data to third countries

The transfer of personal data is one of the processing activities listed by Article 2.b of the Directive. For this reason it should be compliant with all the data processing principles introduced by the Data Protection Directive.

Transfers of personal data to third countries are prohibited by the DPD unless these countries provide an adequate level of protection. Such prohibition aims to guarantee that personal data, which is protected on the same level in the EU, is not sent outside to countries where the given protection would be weaker, in order to circumvent the strict rules of the Community. The formal qualification of a country's level of granted protection is done by the European Commission, after a thorough assessment of its data protection regulation. Such an assessment should be done on a case by case basis, 'in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations'. The aspects that are taken into account include the nature of the data, the purpose and duration of the proposed processing operation, 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 (Article 25.2 DPD). Currently the list of countries consists of: Andorra, Argentina, Australia, Canada, Switzerland, Guernesey, Jersey, Island of Man and Feroe Islands, State of Israel, Eastern Republic of Uruguay, and the United States for companies that have joined the Safe Harbour programme[22].

[21] Article 29 Working Party, The Future of Privacy, Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, WP 168, 1 December 2009, p. 9.

[22] The Safe Harbor program was developed by the US Department of Commerce in consultation with the European Commission to allow transfer of personal data from the EU to the US based companies, under a presumption of adequacy of protection of the data. Such a possibility has been introduced in art. 25.6 of the Directive. The transfer is only possible under the condition that the companies commit themselves to a set of privacy principles negotiated by the Commission. See more at: Safe Harbor, U.S. Department of Commerce, http://www.export.gov/safeharbor/index.asp;

A series of derogations are foreseen where the data are transferred to a third country which does not provide for an adequate level of protection but:

a) the data subject has given his consent unambiguously to the proposed transfer

b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken in response to the data subject's request

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

d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims

e) the transfer is necessary in order to protect the vital interests of the data subject

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.

3.6.1 International transfers of data in the environment of cloud computing

The data processing performed in the SocIoS prototype will be performed either in Europe or exceptionally in Israel. In case personal data are transferred outside the European borders, the legitimacy of such transfer will be assessed. However, transferring data to Israel should be not a problematic issue since Israel has been declared by the EU Commission as a country with adequate level of protection.

More complex issues may, nevertheless, arise from the use of cloud computing technology. Article 4 of Directive 95/46/EC defines its own choice of law rule mainly based on the location of the data controllers' premises or, when established outside the European Union, on the location of the equipment this data controller makes use of when they are located in a member State's territory (unless this equipment is solely used for transit purposes). The practical applicability of this rule is challenged by the fact that Service-Oriented Architectures increasingly rely on 'Cloud Computing', a new and most efficient technology in terms of information management that is based on GRID technology.

Cloud computing is a style of computing in which dynamically scalable and often virtualised resources are provided as a service over the Internet. This technology thus relies on users storing all their information on the Internet and not on their computer anymore. Information is directly managed from the 'cloud'. One of the most difficult questions arise with regard to the ubiquitous nature of the storage and thus on the multiplicity of privacy laws that could apply to such online services. The diffuse and uncertain application of domestic legislations to platforms making use of cloud computing will be analysed.

Recommendations will be formulated in order to come with an acceptable solution that would ensure legal certainty to both users and service providers.

4 Legal requirements for data processing

4.1 Principles of data processing

Principles of data processing are considered to be the bedrock of the European Data Protection law. As stated by Bygrave 'they constitute the essence of the right to data protection. The other provisions of the Data Protection Directive elaborate on these principles.'[23] The principles are a set of rules, which every entity processing personal data has to comply with. The principles are considered to be the necessary requirements for the processing of personal data. They are based mainly on the provision of Article 6 of the Data Protection Directive.

4.1.1 Principle of fair and lawful processing

The first principle (art. 6(1)(a) Data Protection Directive) states that processing must be fair and lawful. In order to fulfil this requirement, the data subject has to be provided with certain information, (listed in article 10 of the Data Protection Directive), at the time of the obtaining of the data, or right after. This means that the transparency of the data collection needs to be ensured. Moreover, this principle requires the data controllers to stay in line 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 Data Protection Directive states that a processing, to be considered lawful, must be carried out on one of the grounds listed by Article 7. As described above (section 3.2), Article 7 lists legal grounds that the processing can be based on as the 'criteria that makes the processing legitimate' (Recital 30), linking 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.

The concept of fair processing is related to the reasonable expectations of the data subject. There are several aspects of this notion that can be found in the literature. Processing of personal data is 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. 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

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

the data are used by the latter for particular purposes.'[24] Further, the notion is interpreted in a way that requires the processing to be transparent for the data subject.[25] According to recital 38 'if the processing of data is fair, the data subject must be in position to learn of the existence of a processing operation and; where data are collected from him, must be given accurate and full information, bearing in mind the circumstances of the collection. This requirement is fulfilled by the information of the data subject.' Fair processing also means that when the personal data are used for another purpose which the data subject would not reasonably expect, the data controller should base this new processing on any of the legal grounds listed in Article 7 DPD[26]. This could mean that the data controller should in such a case obtain the data subject's consent to the new use. This requirement is directly linked to the compatibility of further uses with the original one.

4.1.2 Principle of finality/ purpose limitation

According to Article 6(1)(b) DPD data controllers must collect data only as far as it is necessary in order to achieve the specified and legitimate purpose. Moreover, no further processing can be carried out that is incompatible with those purposes. This can be translated into a rule that the data subject must be specifically informed about the purpose of the data collection and that such data cannot be used later for further purposes that are different than the original ones. The finality principle requires in particular that, without a legitimate reason, personal data may not be used and the individual concerned must remain anonymous.

4.1.3 Principle of data minimisation

The third principle is expressed in Article 6(1)(c) Data and it requires data minimisation. The rule states that the processing of personal data should be limited to data that are adequate, relevant and not excessive. This means that data controllers are obliged to store only a minimum of data necessary to run their services. The purpose of this principle is to prevent the collection of data' which would not be strictly necessary for the provision of the service. In other words, the principle acts as a barrier in order to limit the collection of data. The processing of data extracted from social networks, could lead to the archiving of every user's activities and opinions providing a significant source of information for profiling. This could pose a high risk for individual liberties. This principle will play an important role in the definition of which personal data is necessary for the achievement of the purpose of the processing.

Two concepts, of 'data avoidance' and 'privacy by design', are often related to this principle. The first one requires that the technical devices and designs use either a limited amount of personal data or no personal data at all. The latter calls for attention to the privacy and data

[24] Bygrave L. A., Data Protection Law: approaching its rationale, logic and limits, Kluwer Law international, 2002, p.58
[25] Bygrave L. A., Data Protection Law: approaching its rationale, logic and limits, Kluwer Law international, 2002, p.58
[26] Bygrave L. A., Data Protection Law: approaching its rationale, logic and limits, Kluwer Law international, 2002, p.58

protection issues, which should be implemented from the earliest stage of design of any data processing systems.

4.1.4 Principle of data quality

The next principle is derived from Article 6(1)(d) DPD. It provides that all personal data should be accurate and, where necessary, kept up to date. The data controllers are obliged to take every reasonable step to ensure that data which are inaccurate or incomplete, having regard to the purposes, for which they were collected, are either erased or rectified. 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. Such a solution would reduce the risk of complaints of breach of this principle, in case of harm caused by inaccurate data.

4.1.5 Principle of data conservation

Article 6(1)(e) Data Protection Directive introduces a requirement that personal data shall not be kept for longer than necessary for the purposes for which it was collected. After achieving the purpose for which the data was gathered, it should be rendered anonymous or destroyed. It should be highlighted that the processing of personal data for the purpose of anonymisation falls within the scope of the Directive. Since the definition of "processing" is very broad, it also covers the process of anonymisation.

The Article 29 Working Party addressed the issue of data conservation in its Opinion 1/2008 on data protection issues related to search engines. In the document the Working Party stated that 'search engine providers must delete or irreversibly anonymise personal data once they no longer serve the specified and legitimate purpose they were collected for and be capable of justifying retention and the longevity of cookies deployed at all times'[27]. A retention period that in the opinion of the Working Party was sufficient in this case was estimated at 6 months. In this opinion search engine companies were also encouraged to implement privacy by design solutions that would limit the period of retention.

4.1.6 Principle of data quality

The principle of security is presented in Article 17 DPD. The provision requires that controllers implement security measures which are appropriate to the risks presented for personal data in storage or transmission, with a view to protecting personal data against accidental loss, alteration, unauthorised access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. This includes the prevention of occurrences such as the dissemination of information that may be helpful to protect a right of the data subject, a third party or the data controller himself – also with a view to preventing manipulation, alteration or destruction of data and related items of evidence. Specific attention should be paid to the persons entitled to access the images and to process them, particularly when the controller opts for sub-contracting

[27] Article 29 Data protection Working Party, Opinion 1/2008 on data protection issues related to search engines, WP148, 4 April 2008.

part of or the whole processing to a processor. Any person acting under the authority of the controller or of the processor, including the processor himself who has access to personal data must not process them except on instructions from the controller, unless he is required to do so by law. Recital 46 of the Directive emphasises the importance of taking appropriate technical and organisational measures both at the time of the design of the processing system, and at the time of the processing itself, in order to maintain security and to prevent an unauthorised processing. Such measures must ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks inherent in the processing and the nature of the data to be processed.

Moreover, it should be kept in mind that specific requirements in terms of security measures may be defined by national laws. Some data protection authorities, like for example the DPA of Belgium or Spain, have issued specific norms to guide the level of security required for processing of personal data As far as possible, functionalities tending to ensure the security of the data stored should be integrated into the platform.

4.1.7 Principle of notification to the Supervisory Authority

The data controller must also notify the respective national data protection authority before any data processing operation is carried out (Article 18 Data Protection Directive). The Directive leaves to the Member States the possibility to simplify the notification procedure or to waive it altogether in certain situations. However, for the majority of entities engaged in processing of personal data the notification is obligatory. According to Article 19 of the Data Protection Directive notification to a national data protection authority must include at least: the name and address of the controller and of his representative; the purpose of the processing; description of the categories of data subjects and of the data or categories of data relating to them; the recipients or categories of recipients to whom the data might be disclosed; proposed transfers of data to third countries; and a general description allowing a preliminary assessment to be made of the appropriateness of the measures taken pursuant to Article 17 to ensure security of processing.

4.2 Data subjects' rights

Apart from the obligations put on data controllers the Data Protection Directive introduces also a set of corresponding rights of the data subjects. The rights are aimed to reinforce the fundamental right to privacy described in Article 8 ECHR. The overall intention of granting the rights is to guarantee that the data subjects remain the ultimate controllers of their data, even though some of these rights are recognised only implicitly. 'A core principle of data protection laws is that persons should be able to participate in, and have a measure of influence over, the processing of data on them by other individuals or organisations'[28]. In order to achieve this goal, transparency of the processing should be ensured – and this is the main objective of these rights. The introduced rights correspond to the obligations of the data controllers. These rights should be taken into account during the design and

[28] Bygrave L. A., Data Protection Law: approaching its rationale, logic and limits, Kluwer Law international, 2002, p. 63

implementation phase of the data processing systems. Moreover, the processing activities should be carried out in respect with the rights of the data subjects.

4.2.1 Right to information

Any collection of personal data requires a prior supply of certain information to the individual concerned. This is aimed at 'making people aware of basic details of the processing of personal data on themselves'[29]. The purpose of the right is to ensure the transparency of the processing. As prescribed by Article 10 Data Protection Directive, the person whose data is collected must be provided with the information about:

• the identity of the controller and of his representative, if any

• the purposes of the processing for which the data are intended

• 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:

  • the recipients or categories of recipients of the data

  • whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply

  • the existence of the right of access to and the right to rectify the data concerning him.

In situations where the data have not been obtained from the data subject, it is required to assess in which cases and at what time the information should be given to the data subject. Article 11 of the directive 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 data subject should in such a situation be informed about the categories of data concerned. Within the SocIoS project, the data will usually be collected directly from the data subject.

4.2.2 Right to object

The right to object to the processing of data relating to a data subject, at any time, on compelling legitimate grounds, is granted by Article 14(a) Data Protection Directive. This right must at least cover the cases where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority and where processing is necessary for the purposes of the legitimate interests pursued by the controller (Article 7(e) and (f)). The controller should then erase or block these data.

Article 14(b) of the Directive refers specifically to the processing of personal data for the purposes of direct marketing. The Directive leaves to the Member States a choice between two models. They can either grant the data subject the right: (i) to object, on request and

[29] Bygrave L. A., Data Protection Law: approaching its rationale, logic and limits, Kluwer Law international, 2002, p. 63

free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing, or (ii) to 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, and to be expressly offered the right to object free of charge to such disclosures or uses. The specific procedure and time limitations is a matter of transposition of the Directive into national law.

4.2.3 Right of access

According to Article 12 Data Protection Directive, every data subject whose personal data are processed should obtain from the controller the confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned and the recipients or categories of recipients to whom the data are disclosed. A data subject should be able to exercise these rights both at the physical address of the controller and on-line. Naturally, adequate security measures should be taken to guarantee that solely the data subject has on-line access to information that concerns him. Moreover, data subjects have also a right to know the source of the data, if this information is available. In case of automated individual decisions, the data subject is also entitled to be informed about the logic involved in any automatic processing of his data. All this information must be available to the data subject 'without constraint at reasonable intervals and without excessive delay or expense' (Article 12 (a) Data Protection Directive).

4.2.4 Right to erase, rectify or block

The right of access also consists of a right to rectify, erase or block the data, in cases where its processing does not comply with the requirements of the data protection directive. This could be the case, for example, if the data controller's collection of personal data is disproportionate to his purposes. This provision applies in particular when the data at issue are incomplete or inaccurate (Article 12 (b) Data Protection Directive).

4.2.5 Right not to be a subject to an automated decision

Data subjects are also granted, in Article 15 DPD, a right not to be a 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, such as his performance at work, creditworthiness, reliability, conduct, etc. There are statutory exceptions attached to this right in cases where the decision is either: 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 authorised by a law that also lays down measures to safeguard the data subject's legitimate interests.

4.2.6 Right to seek legal relief

Article 22 of the Data Protection Directive embodies the right of every person to a judicial remedy for any breach of the rights guaranteed to him by the national law applicable to the

processing in question. Further, in Article 23 the Directive states 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 from the controller for the damage suffered.

5 Other relevant concepts of data protection

5.1 Transparency of data processing

One of the challenges of the SocIoS project will be to ensure the transparency of the data processing involved. The majority of the rights described above, and particularly the right to information, aims to guarantee that the data is processed in a transparent way. It is considered that transparency is a 'pre-condition to fair processing'[30]. The reason for this opinion is that "it gives the data subject a say in the processing of personal data, 'ex ante', prior to processing. Profiling, data mining, and technological developments which ease the exchangeability of personal data make it even more important for the data subject to be aware by whom, on what grounds, from where, for what purposes and with what technical means data are being processed. It is important that this information is understandable"[31]. This means that information, in order to be transparent, should be provided in a clear and comprehensible way, taking into account the final recipient of the information. The provision of clear and understandable information in social networks is a difficult issue to solve as shown, e.g. by the numerous policy changes operated by Facebook trying to satisfy its users' expectations in terms of clarity of privacy settings. Privacy information notices are usually created for legal purposes, not to inform users. As can be seen in the Facebook Privacy Policy, which is longer in the amount of words than the US Constitution, long privacy policies are written with the clear aim of protecting the company against potential lawsuits, rather than with the intention of providing clear and readable information to the data subject.[32] Several initiatives go towards greater readability (see e.g. the layered information notice of Microsoft) but the challenge remains intact. This issue should be dealt with within the SocIoS project. It is indispensable to ensure that the data subjects whose data will be processed in the framework of the SocIoS project are provided with all the necessary information, in a clear and understandable way. Several Opinions issued by the WP29 will be taken into account, namely Recommendation 2/2001 on certain minimum requirements for collecting personal data on-line in the European Union and Opinion 10/2004 on More Harmonised Information Provisions.

[30] Article 29 Working Party, The Future of Privacy, Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, WP 168, 1 December 2009, p. 8

[31] Article 29 Working Party, The Future of Privacy, Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, WP 168, 1 December 2009, p. 16

[32] Kuczerawy A., Coudert F., Privacy Settings in Social Networking Sites: is it fair?, in: Duquenoy P., Fischer-Hübner S., Hansen M. (eds.), Post-Summer School Proceedings of the IFIP/PrimeLife Summer School on —Privacy and Identity Management for Life, Helsingborg, Sweden, Springer-Verlag (2011, forthcoming); Rosen, J., The Web Mean the End of Forgetting, New York Times, 19 July 2010, http://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html?_r=3&pagewanted=1&hp

5.2 Privacy by design

As mentioned above, the principle of privacy by design plays an important role in the fulfilment of the data controllers' obligations. The reason for this is the great potential of this concept to enhance the privacy of individuals on a practical level, rather than on the regulatory one. The concept basically requires embedding of the data protection mechanisms and privacy principles into developed technologies. It is therefore addressed mainly to the IT sector. In the Data Protection Directive it is brought up at several points, mainly in Article 6 in reference to data quality, Article 17 which lays down the data controllers' obligation to implement appropriate technical and organizational measures, and in Article 16, which establishes the confidentiality of processing. The concept is also referred to in Recital 46, which calls for the technical and organizational measures to be taken at the time of the design of the processing system and at the time of the processing itself. Even though these provisions undeniably promote Privacy by Design, it has been discovered that they are not sufficient in ensuring the privacy embedding in ICT. For this reason a new provision translating the current punctual requirements into a consistent principle is being proposed within the review of the Directive, which is happening at the moment. The main aim of such an approach is to influence the design of future services and technologies with privacy by default settings. According to the Article 29 Working Party, this principle should be binding for technology designers and producers as well as for data controllers who have to decide on the acquisition and use of ICT. This means an obligation to take technological data protection into account already at the planning stage of information-technological procedures and systems, so as early as possible. Moreover, providers of such systems or services, as well as controllers, should demonstrate that they have taken all measures required to comply with these requirements.[33] The principle should, therefore, "convey the requirement that ICT should not only maintain security but also should be designed and constructed in a way to avoid or minimize the amount of personal data processed"[34].

The strong position of the European Commission on the concept of privacy by design requires that it is adhered to by the SocIoS project. In practice, this means that technological standards implementing the legal requirements have to be developed and taken into account already in the phase of system analysis done by the engineers. The implementation of the principle requires a careful evaluation of the main aspects of data processing, particularly: data minimization, controllability, transparency, user friendly systems, data confidentiality, data quality, and use limitations. All these concepts will have to be implemented into the SocIoS system by the technical partners involved.

[33] Article 29 Working Party, The Future of Privacy, Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, WP 168, 1 December 2009, p. 13

[34] Article 29 Working Party, The Future of Privacy, Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, WP 168, 1 December 2009, p. 13

6 Processing of personal data versus freedom of expression

For the purpose of the SocIoS project a very relevant provision is provided for in Article 9 of the Data Protection Directive. As stated, 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. 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. The exemptions are, however, not allowed to derogate from measures to ensure security of 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. 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. 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.[35] 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. 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.[36]

In majority of the countries a balancing exercise between the conflicting principles of Art. 8 ECHR (right to privacy) and Art. 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 D3.5.

7 Review of the Data Protection Directive

The Data Protection Directive is a document that was introduced in 1995. Its twofold objective is the protection of fundamental rights and freedoms of individuals and in particular the fundamental right to data protection and the achievement of the internal market through the free flow of personal data. This remains intact; however, rapid

[35] Büllesbach A., in: Büllesbach A., Poullet Y., Prins C. (eds.), Concise European IT Law, Alphen aan den Rijn, 2005, p.55
[36] Ramsbro v Riksåklagaren, Swedish Supreme Court of 12 June 2001.

technological developments and globalisation have brought new challenges to the protection of personal data[37]. Social networking or cloud computing are just two examples of developments that challenge the old regulatory framework and questions arise whether the existing EU data protection legislation can still fully and effectively cope with them. The EU Commission, aware of this growing doubt, launched a review of the current legal framework. According to the findings of this long review process the core principles of the Directive are still valid. There however were a number of problematic issues discovered like the impact of new technologies, or lack of sufficient harmonisation between member countries. Other problematic items that should be clarified are: addressing globalisation and improving international data transfers, providing a stronger institutional arrangement for the effective enforcement of data protection rules, and improving the coherence of the data protection legal framework. All the findings were described in the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions on 'A Comprehensive approach on personal data protection in the European Union'.[38] In conclusion, the Commission calls for modernisation of the EU personal data protection system in all areas of the Union's activities. Moreover, the entry into force of the Lisbon Treaty provided the EU with additional means to achieve this: the EU Charter of Fundamental Rights - with Article 8 recognising an autonomous right to the protection of personal data - has become legally binding. A new legal basis has been introduced (Article 16 TFEU) allowing for the establishment of comprehensive and coherent Union legislation on the protection of individuals with regard to the processing of their personal data and on the free movement of such data[39].

The review process revealed that all the stakeholders in the privacy and data protection field would welcome a more comprehensive approach on data protection. One of the main points of such an approach, that the Commission focuses on, refers to strengthening individuals' rights. This is to be achieved by ensuring appropriate protection for individuals in all circumstances, increasing transparency for data subjects, especially with regard to children, or by enhancing control over one's own data. The list of the necessary improvements contains also raising awareness, ensuring informed and free consent through clarification and strengthening of the rules on consent, protecting sensitive data as well as making remedies and sanctions more effective.

The Commission plans to propose new legislation in the course of 2011. The rules of the Directive, however, will not dramatically change. The proposed changes will rather aim to improve, clarify and enhance the existing solutions. Strong trends towards enhancing data controllers' responsibility and better enforcement of data protection rules can be seen. This

[37] 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.
[38] 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.
[39] 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.4.

is a clear signal for all the stakeholders that the issues of privacy and data protection should not be taken lightly and that the minimalistic approach will not be easily accepted. This requires a diligent consideration of the presented requirements and a thorough implementation.

8 Implications for the SocIoS project

To conclude, it should be said that the current legal framework in the area of privacy and data protection poses quite a few challenges for the SocIoS project. First of all it should be, one more time, highlighted that the activities planned for the platform will almost undoubtedly be covered by the definition of processing. Moreover, the data that will be used from different SNSs most of the time can be linked to either an identified or identifiable natural person. In the first case a person can be 'distinguished' from all other members of the group and in the latter, although the person has not been identified yet, it is possible to do it. These two aspects result in the conclusion that the data protection framework will be applicable to the SocIoS platform.

Next question that has to be asked is about the role of each partner in the data processing activities. As described above, the main factor is the determination of purposes and means of the processing. As each partner might play a different role, their tasks have to be clearly defined to ensure that the responsible parties fulfil the obligation of their national legislations, with regard to the personal data of the users collected and stored on their territory. This refers also to the obligation of notification to the supervisory authorities.

Next, a legal ground for the processing will have to be defined. At the current stage it seems that the most appropriate legal ground for the processing in the SocIoS project is the data subject's consent. This however does not mean that this solution is easy. The consent mechanism will have to be carefully designed to make sure that the obtained consent is freely given, specific and informed. The form of the consent will have to be decided upon as in some countries a written consent might be required.

Further on, a whole list of data processing requirements will have to be fulfilled. Starting from the question whether the proposed mechanism is fair, to more specific ones on how to define the purpose and how to make sure that the data is not processed contrary to the purpose agreed upon. In the context of SocIoS, it has to be kept in mind that any personal data found through the search on online platforms cannot be used for any other purpose than the one that the user had in mind when he provided the data, without the user's permission. This would be considered as counter to the purpose specification principle (supra). After all, in most of the cases the original purpose of posting the data on SNS like Facebook is to interact with friends and not to participate in news creation or reporting. Such use of the found data would constitute a secondary use for which a new notification and consent of the data subject would be required. In case of Twitter such distinction is less obvious, users in this medium usually want their posts to reach a vast amount of readers. This idea is related to a more open attitude of the users towards their personal data. However, whether such use of their data constitutes a compatible purpose to the original

one requires a further analysis. Due to such differences, a case-to-case approach to different social media is necessary.

Moreover, the minimisation principle will have to be satisfied by constructing the system in a way that would exclude processing of more data than necessary. Of course the difficulty here will be to decide what constitutes a minimum. When dealing with numerous profiles, on different social networks, filled with different types of data that will be finally used for different reasons, this task might be challenging. The question whether the data collected is adequate with regard to the purposes of the processing will have to be answered.

The next issue that has to be addressed is how long will the data be stored for. After all, achieving the purpose for which the data was gathered is the point after which the data should be rendered anonymous or destroyed.

Further, the question of ensuring data subjects' right has to be tackled. This means guaranteeing the transparency of the whole process so providing the necessary information to the user, and allowing him access to data related to him. He should moreover be able to object to processing of his 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. In the case of SocIoS project, this most likely will be a requirement to obtain the data subject's explicit consent.

Other aspect of the data processing that will have to be considered is the anonymisation of personal data collected by different partners of the project. It is advisable that the data sets is anonymised before sending them to other partners for further processing. It should however be remembered that only a full anonymisation, so when the data will be no longer linkable to the individuals, puts a stop to the applicability of the data protection legislations.

Another particularly important question is whether the data will be sent outside of the European Union. In such situations the Data Protection Directive provides a special regime, which allows transfers of data only to countries whose data protection laws have been announced as adequate by the European Commission. This term means that the data protection law of the said country must provide the same level of protection as the one guaranteed in the EU. In the context of the SocIoS project it has to be remembered that there are two project partners that are based outside of the EU territory, namely in Israel. However, in the EU Commission's decision[40] of 1.12.2009 Israel has been declared as a country with an adequate level of protection. This implies that the transfer of data into this country is allowed and should not be seen as problematic.

[40] Opinion 6/2009 on the level of protection of personal data in Israel, WP 166, 1.12.2009, available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp165_en.pdf

Another important aspect is the fact that the desired search can only be performed on publicly available profiles or accounts, unless otherwise agreed by the interested users. Whichever platforms are subject to the search, private profiles should be considered as a restricted area where users deliberately limited visibility to a selected group of contacts. Regarding the rest of the profiles, so those that can be accessed by the broad public, the situation is not straightforward either. First of all, it should be emphasized that even though information, and often personal data, is made public, this does not mean that such data is not protected by the data protection regulation. Despite the fact that some of the data is made public deliberately while other is made public incidentally, without the user being aware that his information is available to everybody, the protection that this data receives is the same as the protection of personal data that is kept private. It is considered that 'under existing European data protection law, users who publish their personal data on the Internet are entitled to the same level of fair processing and data protection than users that take care to keep their personal data private'.[41] Naturally, a 'reasonable expectation of privacy' might be different in these cases, as users who consciously publish their data are mostly aware that other Internet users can see it. The level of such awareness might be different in case of data subjects whose data is published by, for example, their friends. These differences, however, do not influence the fact that the obligations of the data controller stay the same.

9 Conclusions

All of the legal requirements presented above have to be taken into account by the SocIoS project. Fulfilment of these requirements is necessary to ensure legal compliance of the platform with the EU data protection regime and would greatly benefit the exploitation potential of SocIoS.

Attention should also be paid to the on going review of the Data Protection Directive. Once the legislation is proposed, the requirements presented in this document will be revised in case a new approach is necessary.

Considering all the difficulties, which could be encountered from the legal point of view, it seems that the safest option would be to design the platform in the form of a voluntary service where users would join freely and/or upon invitation. In such service the users would be clearly informed about the purpose of possible data collection, and means of the processing. That way they could express their consent, which would greatly limit a possible danger of infringing any regulation in this matter. Whereas such a solution might be seen as limiting the scope and coverage of the SocIoS platform, however, a strong reduction of the legal risk involved will guarantee a successful implementation of the platform in practice.

[41] User-Created-Content: Supporting a participative Information Society, Final Report, Florence Le Borgne-Bachschmidt (project manager), Sophie Girieud, Marc Leiba, Silvain de Munck, Sander Limonard, Martijn Poel, Linda Kool, Natali Helberger, Lucie Guibault, Esther Janssen, Nico van Eijk, Christina Angelopoulos, Joris van Hoboken, Ewout Swart, SMART 2007/2008, p.57.

10 References

Art. 29 Data Protection Working Party, Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites, WP 56, adopted on 30 May 2002

Art. 29 Data Protection Working Party, Opinion 1/2008 on data protection issues related to search engines, WP 148, adopted on 4 April 2008

Art. 29 Data Protection Working Party, Opinion 5/2009 on online social networking, WP 163, adopted on 12 June 2009

Art. 29 Working Party, The Future of Privacy, Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, WP 168, 1 December 2009

Art. 29 Working Party, Opinion 1/2010 on the concepts of 'controller' and 'processor', WP166, 16 February 2010

Art. 29 Working Party, Opinion 4/2007 on the concept of personal data, WP136, 20 June 2007

Büllesbach A., Poullet Y., Prins C. (eds.), Concise European IT Law, Alphen aan den Rijn, 2005

Bygrave L., Data protection pursuant to the right to privacy in Human Right treaties, International Journal of Law and Technology, 1998, volume 6, pp. 247-284, http://folk.uio.no/lee/oldpage/articles/Human_rights.pdf

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

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

Directive 2002/58/EC of 12 July 2002, concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communication), O.J. L 201/37, 31 July 2002, replacing Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 on the processing of personal data and the protection of privacy in the telecommunications sector

Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, Official Journal L No. 13, 19.01.2000

Jay R., Angus Hamilton, Data Protection Law and Practice, Thomson, Sweet and Maxwell, 2003, 2nd edition

Kuczerawy A., Coudert F., Privacy Settings in Social Networking Sites: is it fair?, in: Duquenoy P., Fischer-Hübner S., Hansen M. (eds.), Post-Summer School Proceedings of the

IFIP/PrimeLife Summer School on —Privacy and Identity Management for Life, Helsingborg, Sweden, Springer-Verlag (2011, forthcoming)

Kuner C., European Privacy Law and Online Business, Oxford University Press 2003

Opinion 6/2009 on the level of protection of personal data in Israel, WP 166, 1.12.2009, available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp165_en.pdf

Rosen, J., The Web Means the End of Forgetting, New York Times, 19 July 2010, http://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html?_r=3&pagewanted=1&hpSIMITIS S., Revisiting Sensitive Data, 1999

User-Created-Content: Supporting a participative Information Society, Final Report, Florence Le Borgne-Bachschmidt (project manager), Sophie Girieud, Marc Leiba, Silvain de Munck, Sander Limonard, Martijn Poel, Linda Kool, Natali Helberger, Lucie Guibault, Esther Janssen, Nico van Eijk, Christina Angelopoulos, Joris van Hoboken, Ewout Swart, SMART 2007/2008

VAN ALSENOY B., BALLET J., KUCZERAWY A., DUMORTIER J., Social networks and web 2.0: are users also bound by data protection regulations?, Identity in the Information Society, Volume 2, Number 1 / December 2009