D7.2

Legal Requirements

Project number:	607577
Project acronym:	ECOSSIAN
Project title:	ECOSSIAN: European Control System Security Incident Analysis Network
Start date of the project:	1st June, 2014
Duration:	36 months
Programme:	FP7/2007-2013

Deliverable type:	Report
Deliverable reference number:	ICT-607577 / D7.2/ 1.0
Work package contributing to the deliverable:	WP 7
Due date:	February 2015 – M09
Actual submission date:	02 03 2015

Responsible organisation:	KUL
Editor:	Damian Clifford
Dissemination level:	PU
Revision:	1.0

Security Sensitivity Committee Review performed on:	27 02 2015
Comments:	No

Abstract:	This deliverable focuses on legal requirements related to the treatment and sharing of data. It builds upon the work completed in D 7.1 Analysis of the applicable legal framework and provides a detailed assessment of the applicable requirements to the ECOSSIAN project.
Keywords:	Privacy, Data Protection, Critical Infrastructure Protection, Security.

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement n° 607577.

Editor

Damian Clifford (KUL)

Contributors (ordered according to beneficiary numbers)

Alessandro Spangaro (UNIBO)

Annarita Ricci (UNIBO)

Yung Shin Van Der Sype (KUL)

Executive Summary

This deliverable focuses on legal requirements related to the treatment and sharing of data. It builds upon the work completed in D7.1 ‘Analysis of the applicable legal framework’ and provides a detailed assessment of the applicable legal requirements to the ECOSSIAN project. It also highlights guidelines for the application of a privacy compliant solution and lists these and the requirements in table form.

Chapter 2 outlines the general data protection requirements derived from the research reported in D7.1 ‘Analysis of the applicable legal framework’, outlines the application of the principle of privacy by design, examines the relevant security and critical infrastructure protection requirements and indicates the potential impact of national law. The derived general legal requirements are then presented in a table.

Chapter 3 focuses on the impact of these requirements on ECOSSIAN.

Chapter 4 lists the resulting applicable guidelines for the implementation of the legal requirements.

In essence the deliverable provides insights in the form of general requirements and guidelines for the implementation of the privacy by design principle in the context of threat detection and analysis and information sharing.

Reference should be made to the specific tables provided in the deliverable. These should form the basis for the implementation of a privacy compliant ECOSSIAN solution but will also be further built upon in D7.3 ‘Information sharing policies in disaster situations - Version 1’.

Contents

List of Tables

Chapter 1 Introduction

Cyber-attacks and the disruption of critical information (CI) infrastructures have become risks of significant importance.[1] One of the key objectives of ECOSSIAN is to design and develop prevention and detection tools that facilitate preventive functions like threat monitoring, early indicator and real threat detection, alerting, support of threat mitigation and disaster management in a privacy compliant manner.

The purpose of this analysis is to outline the legal requirements relevant for ECOSSIAN. Chapter 2 outlines the general data protection requirements derived from the research reported in D7.1 'Analysis of the applicable legal framework'[2]. It also outlines the application of the principle of privacy by design. It examines the relevant security and critical infrastructure protection requirements. Finally, it indicates the potential impact of national law. The derived general legal requirements are then presented in a table. Chapter 3 focuses on the impact of these requirements on ECOSSIAN. Chapter 4 lists the resulting applicable guidelines for the implementation of the legal requirements.

Reference will also be made to the specific sub-scenarios and incidents highlighted in D1.5 'Use case scenario report' where relevant in order to stipulate the significance and application of the legal requirements. A draft version of this deliverable will be used as a point of reference in its current draft form. Importantly however, this will not provide a complete summary of the relevant scenarios and use cases as reference can be made to the specific deliverable for such insights. Instead, it will merely highlight the relevant actions from a legal requirements perspective (their use and impact is outlined further in chapter 3).

Finally, it should be noted that D7.3 'Information sharing policies in disaster situations - Version 1' will provide a deeper analysis of the international and, where relevant, national frameworks governing information sharing in disaster situations. Such distinctions are not the focus of this analysis. Instead we will focus on the general legal requirements for the implementation of a solution in compliance with the requirements for the treatment and sharing of data and the development of guidelines to aid the implementation of these derived legal requirements.

[1] World Economic Forum, *Insights Report. Global Risks 2014 (Ninth Edition)*, Switzerland, 2014, 17, http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2014.pdf.

[2] D. Clifford, A. Ricci, G.D. Finocchiaro, L. Proenca, Y.S. Van Der Sype, and K. e Silva, 'ECOSSIAN D7.1 Analysis of the applicable legal framework' (2014).

Chapter 2 General legal requirements

This section of the deliverable will outline the privacy and data protection and security law requirements relevant for ECOSSIAN. It will also provide a brief outline of the potential impact of national law. This will build upon the work completed in D7.1 'Analysis of the applicable legal framework'[3] (hereinafter D7.1) which provides an analysis of the relevant legal framework. As such the analysis should be read in conjunction with the relevant sections of the D7.1. This will be in the form of an assessment scheme and should provide initial guidance for the evaluation tasks.

2.1 Privacy and data protection requirements

The privacy and data protection requirements need to be complied with and this compliance should be integrated into the design of the architecture. Accordingly this section will first highlight the requirements and will then discuss their integration. Each of the requirements will need to be balanced in the context of the processing undertaken in (and development of) ECOSSIAN and it is thus necessary to observe their importance in relation to any particular data processing which may occur in the context of the operation of the ECOSSIAN solution. Reference will also be made to the proposed changes in the form of the draft General Data Protection Regulation (hereinafter the draft GDPR).[4]

To begin, it is perhaps prudent to first reiterate the definition of a data controller in brief as it is a key criterion for the application of the data protection requirements where personal data is processed. Article 2(d) Directive 95/46/EC defines the concept of data controller. It states that:

> "'Controller' shall mean 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…"

This consists of data controllers processing personal information of data subjects either through their own means or by contracting a third-party data processor. Accordingly in the context of ECOSSIAN, the role of each entity will need to be assessed to see if they satisfy this definition. The potential impact of this is discussed further in section 2.4. There is a distinction between 'normal' personal and 'sensitive' data (or special categories of data) and regard should be had to the definitions and increased protections required as described in D7.1.

[3] D. Clifford, A. Ricci, G.D. Finocchiaro, L. Proenca, Y.S. Van Der Sype and K. e Silva, 'ECOSSIAN D7.1 Analysis of the applicable legal framework' (2014).

[4] 'Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)' COM (2012) 11 final.

2.1.1 Data quality

As was outlined in D7.1, to process personal data certain key requirements under Directive 95/46/EC need to be complied with in order for the processing to be lawful.[5] Article 6 of Directive 95/46/EC specifies the conditions to be satisfied by the data controller in relation to data quality.

The key requirement of Directive 95/46/EC is the obligation that personal **data must be processed "fairly and lawfully"**. It is clear from the Article that processing can only take place for legitimate purposes and that it must be justified on the basis of one of the grounds for legitimate data processing contained in Article 7 of the Directive.[6] This issue was discussed in detail in D7.1 and will therefore not be repeated.

However, it is noteworthy that in the context of ECOSSIAN Articles 7 (a) (consent), 7 (c) (legal obligation – see also section 2.3 of this document), 7 (e) (public interest) and 7 (f) (legitimate interests of the data controller) may all potentially provide legal grounds for personal data processing in the context of ECOSSIAN. This is also supplemented by the exemption clause found in Article 13 of Directive 95/46/EC which provides that Member States are permitted to provide exemptions under the Directive where necessary to safeguard:

a) national security,
b) defence,
c) public security,
d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions,
e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters,
f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);
g) the protection of the data subject or of the rights and freedoms of others.

As such, this provides additional discretion to the data controller in comparison with the grounds under Article 7 as it exempts the application of particular requirements under Directive 95/46/EC.[7] These exemptions are maintained in the draft GDPR in Article 21 with the addition that any restriction must be proportionate in a democratic society. However, in order to understand the scope of this exemption reference must be made to relevant national legislation (for more see section 2.3).

[5] European Parliament and Council, Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31.

[6] For more see the general legal requirements table (section 2.4) req.s 1.5 – 1.9.

[7] In particular Articles 6 (1), 10, 11 (1), 12 and 21 Directive 95/46/EC.

The **purpose limitation principle** provided for in Article 6 (1) (b) which prohibits the processing of personal data "in a way incompatible" with the specified purposes. The principle prevents the re-use of personal data for purposes other than those originally specified. As highlighted by the Article 29 Working Party[8], specification of the purpose is a pre-requisite for applying the other data quality requirements. Thus, the purpose should be made clear before the data processing takes place and the subsequent use limited to the fulfilment of only compatible purposes. In order for personal data to be repurposed, one of the legitimate grounds for processing under Article 7 must again be satisfied. Accordingly, any personal data collected for purposes specified by ECOSSIAN cannot be later re-used for a different incompatible purpose.

Article 6 (1) (d) of Directive 95/46/EC further requires that **personal data should be accurate and if necessary updated**. This obliges that all reasonable steps are taken in order to ensure that inaccurate and/or incomplete data are deleted or updated while remaining aware of the purposes of the processing.

Article 6 (1) (e) specifies the **limited retention principle**. This principle requires the deletion of personal data that are no longer necessary to achieve the objectives of the processing of the data. As such, it has clear relevance at the N-SOC, O-SOC and E-SOC levels as any storage of personal data resulting from the ECOSSIAN system must only be kept for a proportionate time period (i.e. one that is reasonable given the objectives of the processing and time needed to delete or anonymise the personal data).

The limited retention principle also reflects the **data minimisation principle**. This principle, is not expressly provided for in the Directive, but is implied by certain requirements in the Directive.[9] It provides that the data controller should strictly constrain the gathering of personal data to that necessary for the purpose pursued by the processing. However, the data minimisation principle has been recognised by the Court of Justice.[10] Moreover, Article 5 of the proposed GDPR provides clarification by expressly providing for the principles of transparency, data minimisation and controller liability, which are currently only implicitly recognised.[11] Despite the fact that these principles have been around for 25 years, this proposal represents the first time they have been expressly referred to in a legislative text.[12]

---

[8] Article 29 Data Protection Working Party, Opinion 3/2013 on purpose limitation, adopted on 2 April 2013 WP 203 (02.04.2013) http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf, accessed on 19/12/2014.

[9] B. van der Sloot and F.Z. Borgesius, 'Google and Personal Data Protection' in A. Lopez-Tarruella (ed.) *Google and the Law: Empirical Approaches to Legal Aspects of Knowledge-Economy Business Models* (Springer Information Technology and Law Series Vol. 22 2012) 75-111.

[10] CJEU Case-274/99 *P. Connolly v Commission*, [2001] OJ C173/13 see also more recently in CJEU Case C-131/12 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014] OJ C 212/4.

[11] A. Savin, *EU Internet Law* (Elgar European Law, Cheltenham, 2013) 190-218.

[12] L. Mitrou and M. Karyda, 'EU´s Data Protection Reform and the right to be forgotten - A legal response to a technological challenge?' (5th International Conference of Information Law and Ethics Corfu-Greece, June 2012) 1-23.

2.1.2 Data subject rights

Articles 12 and 14 of Directive 95/46/EC provide data subjects with certain rights which the data controller must respect. The data subject has the right to access the personal data being processed about her/him, to demand the modification or deletion of her/his personal data, and to object to further processing under certain specified conditions (see Article 14 (a) and (b)). In the application of these requirements to ECOSSIAN this could include the integration of a system capable of processing data subject requests within the ECOSSIAN architecture.

2.1.3 Automated individual decisions

Currently Directive 95/46/EC affords data subjects the right not to be subject to a decision that "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."[13] This is supplemented by Article 12 (a) of the Directive which provides that Member States are required to guarantee every data subject the right to obtain the "knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions" from the data controller. Thus, this supplements the data subject rights outlined *supra.* However, according to the European Commission this requirement can be circumvented quite easily by merely including formal human intervention in the decision process without this actually having an impact on the outcome of the processing.[14] Accordingly, in the context of ECOSSIAN it appears that some level of formalised human intervention will satisfy this requirement. However, the proposed changes in the draft GDPR should be considered as they represent a potential shift in requirements.

The European Commission has proposed to considerably expand these requirements in the form of increased protection against "profiling" in the new Article 20 GDPR. It is clear from the text of Article 15 of Directive 95/46/EC that it is limited in scope to an automatic "decision". This implies a degree of deliberation. In the draft Article 20 of the GDPR every "measure" producing "legal effects" or that "significantly affects" a "natural person" is within the scope of the Article. From this description it is also clear that the scope has also been expanded in relation to those who it addresses. Directive 95/46/EC only applies to data subjects and therefore is restricted to situations where personal data is processed. However, Article 20 of the draft GDPR, by referring to "natural persons" appears to indicate that the requirements will have affect irrespective of whether personal data is indeed processed. It should also be noted that in the most recent version of the draft Regulation the European Parliament has increased the data controller's obligations *vis-a-vis* accountability by inserting

[13] Article 15 (1) Directive 95/46/EC.

[14] Commission, 'Staff Working Paper Impact Assessment Accompanying the document Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) and Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data', SEC(2012) 72 final: ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_en.pdf accessed on 10/12/2014.

a requirement for a human assessment before a profiling decisions is taken. This further requires the recording of the explanation of decisions taken and represents a shift from the current passive human intervention currently required under Article 18 Directive 95/46/EC.

In addition to this Article 20 (3) of the draft GDPR provides explicitly that, "Automated processing of personal data intended to evaluate certain personal aspects relating to a natural person shall not be based solely on the special categories of personal data". Article 20 (2) of the draft GDPR stipulates the grounds upon which such profiling could be legitimised. Of particular interest in relation to ECOSSIAN are Article 20 (2) (b) and (c). The latter of these stipulates that profiling can be "based on a data subject's consent, subject to the conditions laid down in Article 7 and to suitable safeguards." However, obtaining consent in the context of ECOSSIAN may not always be possible. The former of the grounds does potentially provide some alternative by stating that the EU or Member States may expressly authorise profiling in particular contexts provided that they also lay down measures which "safeguard the data subject's legitimate interests." Accordingly, in the context of ECOSSIAN it appears that under the draft GDPR some legal grounds to process similar to that provided for in Articles 7 (c) and 7 (e) is needed to legitimise profiling. Finally, it should also be noted that the requirements in relation to profiling could be restricted in the application of Article 21 of the GDPR (i.e. the current Article 15 95/46/EC).

2.1.4 Data security

The obligations related to confidentiality and security of the personal data processing are also important. Personal data should be protected by security safeguards against risks such as loss or unauthorised access, destruction, use, modification or disclosure of the data.

According to Article 17(1) of Directive 95/46/EC the data controller must ensure that "appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing" are implemented. These measures must be appropriate with regard to the risks connected with the personal data processing, as well as with regard to the nature of the data collected. Indeed, Article 17(2) of Directive 95/46/EC goes on to provide that the necessary level of data security is ascertained by: [15]

- the state of the art in the given industry,
- the costs of implementation, and
- the sensitivity of the data being processed.

In assessing the state of the art in the given industry one must consider the work completed by the European Network and Information Security Agency (ENISA) in relation to network and information security and the recent security threats encountered and the means of

[15] European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European data protection law*, (Publication office of the EU Luxembourg 2014) 94.

dealing with them (ENISA"s opinions are discussed further in section 2.2 and the proceeding sections).[16]

2.1.5 Personal data breach notification requirements

Connected with the above discussion are the requirements specific to data breach notification. Currently in the context of data protection and privacy, notification requirements are restricted in application to the communications sector with both the E-Privacy Directive[17] and the recent Data Breach Notification Regulation[18] providing such obligations and the provision of a communications network or service to the public.[19] However, as the operations in ECOSSIAN remain outside the scope of their application (i.e. ECOSSIAN is neither a public communications network nor a service provider) these requirements appear to have no effect. However, this issue requires analysis at a national level (see more in section 2.3).

In addition it should be noted that there are some proposed changes in this regard which need to be considered. The draft GDPR proposes the introduction of an obligation to notify personal breaches in Articles 31 and 32. This establishes the requirement that personal data breaches must be notified to the relevant parties "without undue delay". Given the increased frequency of data breaches this is one of the least controversial reforms in the proposal. The requirement is further reflected in the proposed Police and Criminal Justice Data Protection Directive[20] and in the area of network and information security as discussed further *infra* (see section 2.2). Finally, from Article 30(3) of the proposed GDPR, the security of personal data appears to have been aligned with the concepts of privacy by design and by default.[21] It is with this in mind that our attention now turns to the discussion surrounding the integration of these requirements into the design of the architecture.

---

[16] *Ibid.*

[17] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector [2002] OJ L201/37.

[18] Commission Regulation (EU) No 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications [2013] OJ L173/2.

[19] Article 29 Data Protection Working Party, Opinion 03/2014 on personal data breach notification adopted on 25 March 2014 693/14/EN WP 213 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf accessed on 18/01/2015 – see: E-Privacy Directive Article 4(2) and 7(3) (in addition to the Clarification provided in Regulation No. 611/2013) and Article 13a of Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) [2002] OJ L108/33.

[20] 'Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data', COM (2012) 011 final.

[21] M. Hildebrandt and L. Tielemans, 'Data protection by design and technology neutral law' [2013] 29 Computer law and Security Review 509.

2.1.6 Privacy and data protection by design

It is significant to note that, from a data protection and privacy perspective, ECOSSIAN aims to implement a solution that is based on the principle of privacy and data protection by design and by default. The implementation of measures complying with this principle is a key objective of ECOSSIAN and must therefore be given particular attention. The aim of this principle is to "protect privacy by embedding it into the design specifications of information technologies, accountable business practices, and network infrastructures, right from the outset"[22]. Therefore, privacy is part of the system and integrated in a way which does not result in a loss of functionality.[23]

In addition to Article 30 (3) GDPR (discussed above) the principle has also been included in the proposed GDPR as the data protection by design and by default requirement in Article 23 (hereinafter referred to as merely privacy by design). This principle has been gaining in popularity and is symptomatic of a general move towards the development of privacy aware/enhancing technologies. In order for a true implementation of this principle the privacy requirements need to be considered at the very outset. As such, one must conclude that the existence of privacy enhancing technologies or implementations are insufficient as privacy cannot be guaranteed by technology alone. Especially if this technology merely consists of a few components embedded in a larger ICT system add words.[24] Hence, privacy by design represents a significant shift from a reactive to a proactive model for privacy[25] and is a manifestation of the response to technological development and the importance attached to privacy and data protection as fundamental rights.[26]

Furthermore, it must be understood that for a true implementation of the privacy by design principle its scope extends beyond the architecture and also includes the implementation of operating policies. Indeed, in addition to the implementation of this principle in the architecture of ECOSSIAN it must also be part of the mind-set and operation of the solution. With this in mind the proposed implementation of accountability under Article 22 of the draft

[22] A. Cavoukian, 'Privacy by design in law, policy and practice. A white paper for regulators, decision-makers and policy-makers' (Information and privacy commissioner of Ontario, Canada 2011) https://www.ipc.on.ca/images/resources/pbd-law-policy.pdf accessed on 18/02/2015.

[23] A. Cavoukian, 'Privacy by design: the 7 foundational principles' (Information and privacy commissioner of Ontario, Canada 2009) https://www.ipc.on.ca/images/resources/7foundationalprinciples.pdf accessed on 18/02/2015.

[24] G. Danezis, J. Domingo-Ferrer, M. Hansen, J-H. Hoepman, D. Le Métayer, R. Tirtea and S. Schiffner, 'The implementation of the Privacy and Data Protection by Design – from policy to engineering' (ENISA 2014) https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-and-data-protection-by-design accessed on 02//022015.

[25] A. Monreale, S. Rinzivillo, F. Pratesi, F. Giannotti, D. Pedreschi, 'Privacy-by-design in big data analytics and social mining', [2014] 3/24 EPJ Data Science Springer Open http://www.epjdatascience.com/content/3/1/10 accessed on 02/01/2014.

[26] Article 8 of the European Convention on Human Rights (the right to privacy) and Article 8 of the European Union Charter of Fundamental Rights (the right to the protection of personal data)

GDPR[27] would further enhance the privacy by design principle. Indeed if the proposal is adopted operators will be required to implement policies and implement **appropriate measures** to ensure and be able to demonstrate compliance with data protection rules (Article 22). In this regard, the draft provisions propose the following minimum measures:

- keep documentation of all processing operations (article 28),
- implement data security requirements (Article 30),
- perform data protection impact assessments (Article 33),
- comply with requirements for prior authorisation or consultation of the supervisory authority wherever relevant (Article 34(1) and (2)), and
- appoint a Data Protection Officer (Article 35(1)).

2.1.6.1 General objectives for privacy and data protection by design

In the practical implementation of the privacy by design principle several objectives will require an evaluation. Indeed, as highlighted by the Article 29 Working Party:

"In particular, when making decisions about the design of a processing system, its acquisition and the running of such a system the following general aspects / objectives should be respected:

- Data Minimisation: data processing systems are to be designed and selected in accordance with the aim of collecting, processing or using no personal data at all or as few personal data as possible.
- Controllability: an IT system should provide the data subjects with effective means of control concerning their personal data. The possibilities regarding consent and objection should be supported by technological means.
- Transparency: both developers and operators of IT systems have to ensure that the data subjects are sufficiently informed about the means of operation of the systems. Electronic access / information should be enabled.
- User Friendly Systems: privacy related functions and facilities should be user friendly, i.e. they should provide sufficient help and simple interfaces to be used also by less experienced users.
- Data Confidentiality: it is necessary to design and secure IT systems in a way that only authorised entities have access to personal data and thus that the storage and communications systems are secure.
- Data Quality: data controllers have to support data quality by technical means. Relevant data should be accessible if needed for lawful purposes.

[27] 'Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)' COM (2012) 11 final.

- Use Limitation: IT systems which can be used for different purposes or are run in a multi-user environment (i.e. virtually connected systems, such as data warehouses, cloud computing, digital identifiers) have to guarantee that data and processes serving different tasks or purposes can be segregated from each other in a secure way."[28]

Although the above objectives may be clear in a legal sense their practical application may be more difficult to incorporate. With this in mind the focus must now turn to the means of implementation and as such design strategies.

2.1.6.2 Privacy and data protection - design strategies

In an analysis of the application of the principle of privacy by design Hoepman outlines 8 privacy by design strategies. These distinguish between data orientated strategies and process orientated strategies.[29] These are represented in the following tables.

Data Oriented Strategies		
Strategy	**Description**	**Design patterns/implementation**
Minimise	Only the minimum amount of personal data should be collected.	For example "Select before you collect"[30] and "anonymisation and use pseudonyms"[31]
Hide	Personal data and their interrelationships should be hidden from plain view thereby reducing the risk of abuse (an example of such an identifier would be an IP address).	For example the encryption of data, the use of mix networks to hide traffic patterns, the use of anonymisation or techniques to unlink the relationship between related events.[32]
Separate	The processing of the personal data should be in a distributed fashion, this would prevent the completion of full profiles of individuals. Personal data should be processed in separate compartments; by separating the processing or storage of several sources of personal data that belong to the same person, complete	Currently no design patterns for this strategy are known.[33]

[28] Article 29 Data Protection 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 adopted on 1 December 2009, 02356/09/EN WP 168 http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf accessed on 20/12/2014.

[29] J.-H. Hoepman, 'Privacy design strategies – (extended abstract) In ICT Systems Security and Privacy Protection' (29th IFIP TC 11 International Conference SEC Morocco, June 2014).

[30] B. Jacobs, 'Select before you collect, [2005] 54 Ars Aequi 1006.

[31] A. Pfitzmann and M. Hansen, 'Anonymity, unlinkability, undetectability, unobserv-ability, pseudonymity, and identity management – a consolidated proposal for terminology', (version v0.34 Aug. 10, 2010) http://dud.inf.tu-dresden.de/Anon_Terminology.shtml accessed on 05/01/215.

[32] Danezis, (n 21).

[33] *Ibid.*

Data Oriented Strategies		
	profiles of one person cannot be made.	
Aggregate	The highest level of aggregation should be used including the least amount of detail as this will restrict the amount of personal data that remains.	Examples include: Dynamic location granularity, *k*-anonymity[34] and other anonymization techniques.

Table 1. Data Oriented Strategies

The four data orientated strategies discussed above primarily address the principles of necessity and data minimisation.[35]

Process Oriented Strategies		
Strategy	**Description**	**Design patterns/implementation**
Inform	Data subjects should be informed of which data is processed, the purposes of this processing and the means of this processing. This corresponds to the principle of transparency and the requirement to inform the data subject of the processing.	Data breach notification processes are an example of such an implementation.[36]
Control	Data subjects should have agency over their personal data and the data subject rights should be exercisable in order to allow the exertion of these rights.	User centric identity management and end-to-end encryption support control. Given the nature and aims of ECOSSIAN this may not be practically implementable.
Enforce	A privacy policy should be available and enforced. This draws the complementary aspect of accountability. This requires clear responsibilities and internal or external auditing.	Examples include sticky policies and access control.
Demonstrate	This is in order to show compliance with the privacy policy and the legal requirements.	For example logging and auditing.

Table 2. Process Oriented Strategies

2.1.6.3 Privacy and data protection - design requirements

In applying these general objectives and strategies certain requirements can be extrapolated. These could involve the following:

[34] L. Sweeney, '*k*-anonymity: A model for protecting privacy' [2002] 10(5) International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems 557.

[35] Danezis, (n 21).

[36] In this context is interesting to look at proposed amendments Data Protection reform packages (section 2.1) and in the draft NIS Directive (section 2.2): where such an obligation is foreseen.

- Privacy should be proactive and not reactive and thus should be implemented as a default setting embedded into the design of the ECOSSIAN architecture. This could involve the implementation of an automated anonymisation process.
- The security of the personal data should be protected throughout the data lifecycle and this could involve encryption and also the coordination of Privacy Impact Assessments.
- Encryption should be employed throughout with the default state of data being unreadable if there is a data leak. This encryption should be applied automatically.
- Access to the personal data should be on a need-to-know basis only and should be restricted to specific employees. This could be achieved through authentication protocols with privacy features such as the Just Fast Keying protocol.[37]
- The creation of measures (technological, policy and procedural) which bar the linking of personal data thereby respecting the data minimisation and purpose limitation principles.
- All personal data should be securely disposed of at the end in compliance with the limited retention of data principle. This should leave no trace of personal data in order for the process to be truly complete and compliant with the legal requirements relating to personal data retention and deletion.

From the above it is clear that there is a clear focus on the security of the data processing and the importance of avoiding data breaches through the implementation of safeguards. In order to gain a more accurate indication of the relevant security obligations and to understand the practical implications of the "state of the art" security requirements, one must consider the particular obligations applicable in the context of critical infrastructure protection. This issue will now be discussed in detail.

2.2 Security and critical infrastructure protection requirements

The requirements imposed by the Critical Infrastructure Directive[38] and the Directive on attacks against information systems[39] are targeted towards the EU Member States and thus implementation at the national level. The framework determines that the application of cyber-security measures is largely at the discretion of the stakeholders. The responsibility for protecting European Critical Infrastructures (ECI) lies with the EU Member States and the owners or operators.[40] This section is divided into 1° the security requirements and 2° the data sharing requirements.

[37] Danezis, (n 21).

[38] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection [2008] OJ L345/75.

[39] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, [2013] OJ L218/8.

[40] Recital 6 Directive 2008/114/EC.

2.2.1 Security requirements

2.2.1.1 Current requirements

For the most part Directive 2008/114/EC focuses on the role of the Member States in relation to their communication and cooperation requirements. However, although Directive 2008/114/EC only establishes obligations for Member States, certain *de facto* requirements are established for the operators to ensure the implementation of certain security measures. Each Member State on whose territory an ECI is located is required to inform the owner/operator of the infrastructure concerning its designation as an ECI.[41] According to Directive 2008/114/EC, Member States are required to:

- ensure that ECI's possess and implement an operator security plan,[42]
- conduct a threat assessment,[43]
- ensure that a security liaison officer or equivalent is designated for each ECI,[44] and
- appoint an ECI protection contact point who shall be responsible for the coordination of ECI protection issues.[45]

From these requirements it is clear that the operators have clear obligations in aiding the successful completion of each of the requirements. Despite this, the legislation does not specify any particular information security requirements in respect of critical infrastructure protection. However in relation to ECOSSIAN the project's solution must be integrated with the already existing Operator Security Plan. As ECOSSIAN will be merely a part in the overall security plan it may have to build upon the existing safeguards or these may have to be adopted to incorporate ECOSSIAN.

However, both at an EU as at the Member State level certain industry standards and best practice documents have been developed to provide guidance to the ECI's. This practice has been encouraged by the European Commission.[46] Indeed in Directive 2008/114/EC there are mentions of the sharing and development of best practice information with the operators.[47] In addition ENISA encourages the development and sharing of best practices and is tasked

[41] Article 4(5) Directive 2008/114/EC.

[42] The operator security plan ('OSP') procedure shall identify the critical infrastructure assets of the ECI and which security solutions exist or are being implemented for their protection. The minimum content to be addressed by an ECI OSP procedure is set out in Annex II. Article 5 and Annex II Directive 2008/114/EC.

[43] Article 7 Directive 2008/114/EC.

[44] Article 6 Directive 2008/114/EC: The officer serves as the contact point between the owner/operator of the ECI and the Member State authority concerned. The purpose is to allow for the exchange of information regarding the risks and threats relating to the ECI.

[45] Article 10 Directive 2008/114/EC.

[46] High Representative of the European Union for Foreign Affairs and Security Policy, Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 'Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace' JOIN (2013) 1 final: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf accessed on 19/12/2014: With the objective of promoting a single market for cyber-security products in the EU.

[47] Article 8 and Recital 16 Directive 2008/114/EC.

with development and provision of such documentation.[48] For example, in their recent report on crisis management one of the key recommendations advocated for the supporting of activities for enhanced sharing of information, best practices and the development of cyber crisis management procedures.[49]

2.2.1.2 Proposed security reforms

The proposed Directive on Network Information Security (NIS Directive)[50] aims to foster the prevention and resilience of the information systems by expressly stating in Article 16 that Member states shall "Encourage the use of standards and/or specifications relevant to networks and information security". Under the proposed NIS Directive, Member States have several key obligations and from these certain *de facto* requirements emerge for the operators of critical infrastructures.[51] Of particular relevance to our current discussion on security and threat detection is Article 14(1) which states that:

> Market operators must "take appropriate technical and organisational measures to manage the risks posed to the security of the networks and information systems which they control and use in their operations. Having regard to the state of the art, these measures shall guarantee a level of security appropriate to the risk presented. In particular, measures shall be taken to prevent and minimise the impact of incidents affecting their network and information system on the core services they provide and thus ensure the continuity of the services underpinned by those networks and information systems."[52]

Therefore, operators are required to implement such measures in order to ensure the security of the critical infrastructure and in the context of ECOSSIAN it is required that the systems are proportionate and in line with accepted state of the art. Similar to the privacy and data protection framework, the critical infrastructure protection framework leaves the specific choices up to the operator but, as indicated *supra* references, does mention the provision of best practice documentation to the operators.

2.2.2 Data sharing requirements

2.2.2.1 Current requirements

In essence, in the context of ECOSSIAN information sharing is divided in two: 1° the positive notification requirements as imposed by law and 2° the requirements associated with the sharing functionality to be implemented as part of the project. Despite the increasing importance of the digital economy and the smooth running of critical infrastructures for the

[48] Danezis, (n 21).

[49] *Ibid.*

[50] 'Proposal of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union' COM (2013) 48 final.

[51] Article 2 (8) Proposed NIS Directive.

[52] Article 14 (1) Proposed NIS Directive.

overall benefit of society, small cyber incidents are rarely reported and often go undetected. As noted in an ENISA document on incident reporting this lack of transparency is effectively counter-productive as it makes it more difficult for policy makers to truly appreciate the scale of the problem and the potential associated threat.[53] Nevertheless, currently there is only a positive duty to inform authorities of breaches in certain clearly defined situations.

Directive 2008/114/EC states in recital 14 that:

> "[T]he efficient identification of risks, threats and vulnerabilities in the particular sectors requires communication both between owners/operators of ECIs and the Member states, and between the Member states and the Commission. Each Member states should collect information concerning ECIs located within its territory. The Commission should receive generic information from the Member states concerning risks, threats and vulnerabilities where ECIs were identified".

In addition as is further noted in recital 17 "effective protection of ECIs requires communication, coordination and cooperation at national and Community level". As a result the Directive does lay down some positive requirements with regard to notification for Member States which may be applicable. Indeed in summary Member States are required to:

- identify potential ECIs54 and inform the Commission and the owner/operator55 and the Member States (which may be significantly affected by a potential ECI) about its identity and the reasons for designating it as a potential ECI,
- participate in bi/multilateral discussion with other potentially affected MSs when identifying a potential European Critical Infrastructure56, and
- provide a report every two years to the Commission including generic data on a summary basis on the types of risks, threats and vulnerabilities encountered per ECI sector in which there is an identified and designated ECI57.

2.2.2.2 Proposed data sharing reforms

The EU legislator has seen the need for change in this regard and certain key proposals aimed at bridging this notification requirement gap. These measures focus on breach/incident notification as opposed to incident response. Incident response includes the plans and activities taken to eliminate the cause or source of an infrastructure event. As noted by ENISA, as "it comes after the fact, assesses the total impact; identifies root causes; documents the actions taken; and describes lessons learned" and is therefore of more value to mitigate the effects of an attack as it allows for the sharing of valuable information to the

[53] M. Dekker, C. Karsberg and B. Daskala, 'Cyber Incident Reporting in the EU: An overview of security articles in EU legislation' (ENISA 2012), http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/cyber-incident-reporting-in-the-eu accessed on 03/12/15.

[54] According to Article 4(6) Directive 2008/114/EC, the identification and designation process of ECIs should have been completed by 12 January 2011, and reviewed on a regular basis.

[55] Article 4 Directive 2008/114/EC.

[56] Article 4 Directive 2008/114/EC.

[57] Article 7 Directive 2008/114/EC.

relevant interested parties.[58] Of note in this regard are the specific notification requirements seen in the draft NIS Directive. As all of these legislative reforms are likely to be implemented during the lifecycle of the project it is important to weigh their impact accordingly. Some of the specific requirements, as provided for by the NIS Directive, for Member states are as follows:

- to adopt a national NIS strategy defining the objectives and the policy and regulatory measures necessary to achieve and maintain a high level of NIS,59
- to designate a national competent authority responsible for monitoring the application of the Directive at a national level,60
- to establish a Computer Emergency Response Team (CERT) to handle incidents and risks,61 and
- to cooperate within a network that enables secure and effective coordination (including coordinated information exchange, detection and response at an EU level).62

Through this network, Member States should exchange information and cooperate to counter NIS threats and incidents on the basis of the European NIS cooperation plan.[63] From these certain *de facto* requirements can be extrapolated for the operators of the critical infrastructures:

- market operators must notify the competent authority of incidents having a significant impact on the security of the core services they provide,64 and
- market operators must: "(a) provide information needed to assess the security of their networks and information systems, including documented security policies; (b) undergo a security audit carried out by a qualified independent body or national authority and make the results thereof available to the competent authority."[65]

[58] M. Dekker, C. Karsberg and B. Daskala, 'Cyber Incident Reporting in the EU: An overview of security articles in EU legislation' (ENISA 2012), http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/cyber-incident-reporting-in-the-eu accessed on 03/12/15.

[59] Article 5 Proposed NIS Directive: The strategy should include *inter alia* the following matters: (i) a definition of the objectives and priorities of the strategy based on an up-to-date risk and incident analysis; (ii) a governance framework to achieve the strategy, including a definition of the roles and responsibilities of the public bodies and relevant agents; (iii) the identification of the measures on preparedness, response and recovery, including cooperation mechanisms between public and private sectors. The national NIS strategy shall include a national NIS cooperation plan. Both, the strategy and the cooperation plan shall be communicated to the Commission

[60] Article 6 and 15 proposed NIS Directive.

[61] Article 7 proposed NIS Directive - The requirements and tasks of the CERT are included in Annex I of the proposal.

[62] Article 8 proposed NIS Directive.

[63] For more see: D. Clifford, A. Ricci, G.D. Finocchiaro, L. Proenca, Y.S. Van Der Sype, K. e Silva, 'ECOSSIAN D7.1 Analysis of the applicable legal framework' (2014), 36 – 88.

[64] Article 14(2) proposed NIS Directive.

[65] Article 15 proposed NIS Directive.

Accordingly regarding cyber-security, the draft NIS Directive proposes to establish that market operators will have to provide the necessary information for assessing the security of their networks and information systems, including documented security policies. They also have an obligation to undergo a security audit carried out by a qualified independent body or national authority and make the results thereof available to the competent authority.

Therefore, as the notification of security and personal data breaches are likely to become part of the legal framework during the project lifecycle it is important to consider sharing functionalities within the design of the ECOSSIAN solution (see also sections 2.1.5). However, as such information sharing is a key functionality of ECOSSIAN this requirement may be inherently satisfied. Nevertheless, a reporting mechanism that respects the privacy and data protection concerns is key.

2.3 Additional requirements following from national implementations of EU legislation

As was made clear in the analysis set out in D7.1 there is a degree of disparity in the application of the legal framework on privacy and data protection and security amongst the EU Member States. In addition despite compliant implementation of the legal framework on privacy and data protection, subtleties in implementation also exist at the national level as shown in D7.1. Accordingly it is important to note that certain (more restrictive) national laws may have effect in particular contexts. This has a specific impact not only on the rules for the implementation of ECOSSIAN at an O-SOC and N-SOC level but also on the selection of Member States in which the E-SOC as a potential data controller will be located. This is an issue which should be weighted carefully. However, this does raise some issues in relation to the identification of the data controller. It is possible that the ECOSSIAN solution will involve several entities (e.g. O-SOC(s), N-SOC(s) and E-SOC(s) which may be classified as data controllers). It will be a challenge to identify the data controller and to establish profound relations with the different data processing actors.

Indeed, it should be specified that the O-SOC and N-SOC may also be classified as data controllers as opposed to data processors if they are processing the data not only on behalf of the data controller but also are significant in the determining of the purposes and means of the processing. Accordingly, the O-SOC, N-SOC and E-SOC all potentially will be obligated to comply with the requirements stipulated. Given the spread of responsibilities (i.e. potential multiple data controllers) it is also significant to note that the data controllers will need to be aware of the subtleties in the relevant implementations of the legal requirements at a national level.

This is particularly significant in relation to notification and authorisation requirements (Articles 18, 19 and 20 of Directive 95/94/EC), the requirement for a legal obligation as a ground for data processing (Article 7(c) Directive 95/94/EC), the exemption from the application of the requirements at the discretion of the Member States (Article 13 Directive 95/94/EC), and technical and organisational security measures (Article 17 Directive 95/94/EC and Article 5 and Annex II Critical Infrastructure Protection Directive). Regarding the former

of these reference should be made to the first report issued by the Data Protection Coordinator for ECOSSIAN and the specific Member State requirements outlined therein.[66] However it is worth mentioning that another clear example of disparity arises in the context of data breach notification. For example in the German implementation a breach notification duty was added in section 42a of the Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG).[67] This applies in relation to sensitive personal data and personal data related to:

- secrecy,
- criminal and or administrative offices,
- bank or credit card accounts, and
- certain telecommunications and online data.

As discussed in D7.1 (and above in relation to the obligations at an EU level) this contrasts sharply with the legislation in other Member States where such notification requirements are restricted to the telecommunications sector.[68]

In relation to the use of a legal obligation as a ground for data processing and the exemption from the application of the requirements at the discretion of the Member States, reference must be made to specific national legislation. As described in D7.1, in the country level analysis it is noted that in the context of critical infrastructure protection in the UK one should consider the application of provisions such as section 17 of the Anti-Terrorism, Crime and Security Act 2001 and the Civil Contingencies Act 2004 which grant legal grounds for the processing of personal data in particular contexts.[69] This indicates the potential for national implementing measures providing legitimate grounds for personal data processing or providing exemptions from its application in certain instances and regard must therefore be given to other such national member state legislative provisions and grounds. In order to establish the correct legal basis for the processing in the context of ECOSSIAN the data protection officers of the data controllers should be consulted and contact should be made with the relevant national data protection authority by the data controller if needed in order to establish the correct legal basis for the processing of personal data.[70]

The analysis of the French legislation regarding critical infrastructure protection in D7.1 can be used as an example of national disparity as it revealed specific national requirements in relation to the creation of technical and organisational measures which also affects the requirements under the national data protection implementation if such infrastructures

[66] A. Vedder, D. Clifford, and Y.S. Van Der Sype, 'ECOSSIAN D9.3 Report from Data Protection Coordinator – Version 1', B. Nussbaumer (ed.) (2015).

[67] Bundesdatenschutzgesetz [Federal Data Protection Act], Dec. 20, 1990, BGBl. I at 2954, as amended.

[68] For more see: D. Clifford, A. Ricci, G.D. Finocchiaro, L. Proenca, Y.S. Van Der Sype and K. e Silva, 'ECOSSIAN D7.1 Analysis of the applicable legal framework' (2014), 36 – 88: For example in Ireland the DPA has adopted a best practice code of conduct in such scenarios.

[69] For more see: D. Clifford, A. Ricci, G.D. Finocchiaro, L. Proenca, Y.S. Van Der Sype and K. e Silva, 'ECOSSIAN D7.1 Analysis of the applicable legal framework' (2014), 36 – 47.

[70] For more see: A. Vedder, D. Clifford, and Y.S. Van Der Sype, 'ECOSSIAN D9.3 Report from Data Protection Coordinator – Version 1', B. Nussbaumer (ed.) (2015).

process personal data. This, as with the specific situation in France, may also affect the personal data breach notification requirements as there may be specific critical infrastructure protection related rules requiring the notification of an attack to a public authority.

It should be noted that D7.3 “Information sharing policies in disaster situations - Version 1” will provide a deeper analysis of the international and, where relevant, national frameworks governing information sharing in disaster situations and accordingly such distinctions are not the focus of this analysis. Therefore, from the above discussion it is clear that reference should be made to national laws in the noted contexts and regard should be had to the work completed in D7.1.

2.4 General legal requirements table

Req. number	Description	Importance* (M/O)	Relevant for Level			Comment
			O-SOC	N-SOC	E-SOC	
GReq. 1.1	As described in the Data Protection Coordinator’s Report notification and authorisation requirements must be respected[71]	M	X	X	X	Articles 18, 19 and 20 Directive 95/46/EC and their national MS equivalents as stipulated by the national law of the competent Member State.
GReq. 1.2	If sensitive data is processed the specific restrictions should be complied with	M	X	X	X	The more stringent national laws applicable for the processing of sensitive data and the requirements of Art. 8 Directive 95/46/EC (including export restrictions) must be complied with if these special categories of data are being processed.
GReq. 1.3	The data controller is required to have a legal ground in order to process the personal data as specified further in req.s 1.4 – 1.9 with emphasis on req.s 1.4, 1.6, 1.8 and 1.9. Regard should also be had to any potential exemption in national law to the application of the legal requirements.	M	X	X	X	Article 7 Directive 95/46/EC, and in the case of the exemption Article 13 and the relevant national legislation justifying this exemption.
GReq. 1.4	If ECOSSIAN relies on consent as a grounds for processing this must be legally and validly obtained	M	X	X	X	Article 7(a) Directive 95/46/EC
GReq. 1.5	If the performance of a contract is the legal ground for data processing the data controller must only act within the boundaries of this contract. The extent of data	M	X	X	X	Article 7(b) Directive 95/46/EC. This could happen if an external entity is used to process personal data.

[71] A. Vedder, D. Clifford, and Y.S. Van Der Sype, 'ECOSSIAN D9.3 Report from Data Protection Coordinator – Version 1', B. Nussbaumer (ed.) (2015).

Req. number	Description	Importance* (M/O)	Relevant for Level			Comment
			O-SOC	N-SOC	E-SOC	
	processing must be necessary to fulfil the contract.					
GReq. 1.6	If the existence of a legal obligation is the legal ground for the data processing, the data controller must only act in accordance with and within the boundaries of the legal obligation. The extent of data processing must be necessary to fulfil the legal obligation.	M	X	X	X	Article 7(c) Directive 95/46/EC.
GReq. 1.7	If the legal ground for data processing is the vital interest of the data subject, the data controller must only act to protect these vital interests and the extent of data processing must be necessary.	M	X	X	X	Article 7(d) Directive 95/46/EC. This could be potentially used in a disaster situation where the processing could be legitimised, however in the day to day operation of ECOSSIAN it is unlikely to have an impact and there are more viable grounds to be relied upon.
GReq. 1.8	If the legal ground for data processing is the Performance of a public interest task or in the exercise of official authority, the data controller must only act in the furtherance of this task.	M	X	X	X	Article 7(e) Directive 95/46/EC
GReq. 1.9	If the legitimate interest of the data controller is used as the legal ground for data processing, the controller is required to have a legitimate interest in the data processing.	M	X	X	X	Article 7(f) Directive 95/46/EC
GReq. 1.10	ECOSSIAN must respect the Data quality principles as specified further in req.s 1.11 – 1.15.	M	X	X	X	Article 6 Directive 95/46/EC
GReq. 1.11	All processing operations involving personal data in ECOSSIAN must be completed fairly and lawfully and cannot contravene the protections afforded under the Data Protection Framework.	M	X	X	X	Article 6(a) Directive 95/46/EC
GReq. 1.12	The personal must only be processed for specified explicit and legitimate purposes and not further processed in a way incompatible with those purposes.	M	X	X	X	Article 6(b) Directive 95/46/EC
GReq. 1.13	The personal data processing must be necessary and adequate for the purpose specified i.e. in the context of ECOSSIAN the protection of Critical Infrastructures.	M	X	X	X	Article 6(c) Directive 95/46/EC
GReq. 1.14	In order to ensure that the personal data is accurate and up to date the responsible data controller MUST	M	X	X	X	Article 6(d) Directive 95/46/EC

Req. number	Description	Importance* (M/O)	Relevant for Level			Comment
			O-SOC	N-SOC	E-SOC	
	take every reasonable step. As such the accuracy of personal data stored should be constantly assessed an inaccurate data should be deleted.					
GReq. 1.15	Personal data MUST be deleted or anonymised when no longer necessary for the specified purpose. Therefore ECOSSIAN is required to implement a means for arranging the deletion of the unnecessary personal data.	M	X	X	X	Article 6(d) Directive 95/46/EC
GReq. 1.16	ECOSSIAN should not make automated individual decisions regarding the data subject, unless authorised by law.	M	X	X	X	Article 15 Directive 95/46/EC
GReq. 1.17	The data controller (as well as the ECOSSIAN infrastructure) must ensure the easy operation of the data subject's rights. This could include the integration of a system capable of processing data subject requests within the ECOSSIAN architecture.	M	X	X	X	Article 14 Directive 95/46/EC
GReq. 1.18	Data controller and processor must ensure the implementation of appropriate state of the art technical and organisational measures to ensure security and confidentiality.	M	X	X	X	Article 17 Directive 95/46/EC
GReq. 1.19	The ECOSSIAN solution must be able to be integrated with the already existing Operator Security Plan.	M	X	X	X	Article 5 and Annex II Critical Infrastructure Protection Directive
GReq. 1.20	National implementations of Directive 2008/114/EC must be consulted as they may (for example France) have specific requirements on the security architecture implementation.	M	X	X	X	
GReq. 1.21[72]	National requirements on the requirements in relation to security breach notification must be consulted.	M	X	X	X	

*M – mandatory; O – optional

** Work Packages where this requirement should be implemented

Table 3. General Requirements Table

[72] For more detailed information about the national law, see D7.1.

Chapter 3 Impact on ECOSSIAN

The purpose of this section of the analysis is to apply the requirements outlined above to the context of ECOSSIAN. This will be done through the lens of implementing the principle of privacy by design and thus each section will provide an analysis of the potential impact of such an implementation on ECOSSIAN. It will involve an application of the identified requirements to the use cases outlined in Task 1.2 'Use case definitions' (D1.5 'Use case scenario report') in WP1. A preliminary draft of these use cases has been developed in advance of the deadline (not due until month 12) as agreed by the partners for their use in deliverables such as this one (submitted in month 9). Accordingly, this chapter will analyse the use cases identified under the three classes noted in D1.5 'Use Case Scenario Report' namely:

- Threat Detection,
- Analysis Aggregation and Correlation, and
- Threat Mitigation and Incident Management.

For the purposes of the legal requirements these classes will be discussed under two categories namely: 1° Threat detection and analysis 2° and Information sharing. Hence, the analysis will be divided accordingly with particular reference to the specific issues relevant to critical infrastructure protection and privacy and data protection in the given context. This division has be drawn as the specific purpose of this deliverable as noted in the description of work is to provide an overview of the legal requirements governing the ECOSSIAN system, related to the treatment and sharing of data.

As figured out in D1.5 (preliminary version) we assume that the functionality of the ECOSSIAN system will be separated in a modular way into the following components:

- Threat Detection Module (TDM),
- Aggregation Analysis Correlation Module (AACM),
- Visualisation Module (VM),
- Threat Mitigation Module (TMM),
- Incident Management Module (IMM); and
- Reporting System (RS).

Specific reference to these components and the operations occurring will be made to highlight the requirements as applied to ECOSSIAN.

3.1 Threat detection and analysis

In the context of the threat detection and analysis aspects of ECOSSIAN the implementation of certain features should be considered. One must consider how the strategic recommendations could be achieved in practical terms for the ECOSSIAN system.

The ECOSSIAN solution will monitor for anomalies in the normal processing of components through the TDM and report upon potential threats to the AACM. It is clear from the above discussion that such a data gathering exercise obliges compliance with the data protection requirements if personal data is processed. ENISA in its recent report on the implementation of the privacy and data protection by design highlights certain privacy techniques which should be examined.[73] Of particular significance to the threat detection and analysis privacy considerations are ENISA's recommendations on privacy in databases, storage privacy, and privacy preserving computations. The report splits database privacy in three categories: 1° "Respondent privacy" (preventing the re-identification of the respondents), 2° "Owner Privacy" (this relates to two or more autonomous entities being able to compute queries across their databases) and 3° "User privacy" (guaranteeing the privacy of queries to interactive databases to prevent profiling and re-identification).[74]

As the first of these, "respondent privacy" relates more to the disclosure of data to third parties, like the general public, its impact is perhaps not as high in relation to ECOSSIAN. Regarding "owner privacy" this may have applicability if the O-SOC, N-SOC and E-SOC databases are shared. ENISA highlights the importance of privacy-preserving data mining and its benefits for data and knowledge hiding and such technologies should be examined in the context of ECOSSIAN.[75] In relation to user privacy issues the solutions surrounding private information retrieval are mainly based on cryptography.

ENISA's recommendation in relation to "storage privacy" are of clear significance as a major challenge in implementation is to prevent unauthorised access.[76] Given that the ECOSSIAN solution will be connected to a network localised storage is out of the question. The ENISA report outlines the following storage mechanisms for consideration:

- local encrypted storage,
- format preserving encryption,
- stenographic storage; and
- secure remote storage.

Regarding privacy-preserving computations the ENISA report highlights the benefits of homomorphic encryption and secure multi-party computation.[77] These recommendations should be considered in the assessment of the appropriate implementation of ECOSSIAN and the evaluation of the state of the art.

[73] Danezis, (n 21).

[74] *Ibid.*

[75] *Ibid.*

[76] *Ibid.*

[77] *Ibid.*

Given the intention of the ECOSSIAN system to store the collected data for analysis purposes (i.e. the analysis of a potential threat), national provisions relating to the security of this storage are significant (as indicated in section 2.3). However, as per section 2.1, there are general data protection obligations that require compliance. As such, the data processing for the specified purpose must comply with the data quality principles, enable the exercising of data subject rights and ensure the security of the personal data in order for the ECOSSIAN system to be legally compliant. The requirement to delete or anonymise data no longer necessary for the specified purpose could potentially raise an issue as data will be stored by the ECOSSIAN system in order to monitor and compare future incidents thereby detecting trends in future attacks and recognising false positives and non-attack anomalies. Where possible the ECOSSIAN solution should anonymise or securely delete personal data that is not necessary for the purpose of protecting the critical infrastructure through the identification of an attack or that is no longer accurate. In relation to the accuracy of the data the implementation of a system which automatically and systematically deletes unnecessary data could help ensure accurate personal data storage. It must be understood that implementation of such reasonable steps is required to satisfy this requirement under Article 6 (1) (d) of Directive 95/46/EC.

As noted above for a privacy by design implementation it is recommended that personal data and their interrelationships should be hidden from plain view in order to ensure a privacy by design implementation. This, as described *supra* in the discussion of the design strategies (2.1.4.2), could be achieved through the encryption of data, the use of mix networks to hide traffic patterns, the use of anonymisation techniques such as techniques to unlink the relationship between related events. However, in the context of ECOSSIAN this may be difficult to implement fully as part of the systems functionality will focus on the mining of connections and interdependencies of reported events and the detection of one attack from multiple non-connected attacks. As a result, part of the ECOSSIAN solution may concentrate on the finding of interrelationships between personal data. It should be noted however, that this is a best practice recommendation and not a legal requirements *per se* (i.e. there is no legal obligation but such an implementation is encouraged by ENISA for a privacy by design implementation), nevertheless the linking of events should avoid the use of personal data in the process where possible and should only process personal data where necessary for ECOSSIAN's purpose. This difficulty is also evidenced regarding the visualisation and correlation of results where the VM will have access to all reported events in the data bank.

With this in mind the following table presents a few examples of applied requirements in the ECOSSIAN project.

Applied Req.	Description	Relevant general req.	Design strategy
AReq. 1.1	The TDM should only collect personal data that relates to an anomaly and for the purpose of identifying a threat	GReq. 1.12, GReq. 1.13	Minimise strategy
AReq. 1.2	The AACM should only store personal data for the time necessary for the objective and should securely delete/anonymise all personal data no longer required	GReq. 1.15	Minimise strategy and aggregate strategy
AReq. 1.3	The VM should hide interconnections between personal where possible unless	GReq. 1.13	Hide strategy

Applied Req.	Description	Relevant general req.	Design strategy
	such connections are required for ECOSSIAN's purpose		

Table 4. Applied Requierments Table

Having analysed the threat detection and security requirements in the context of ECOSSIAN it is now necessary to analyse the information sharing processing and the associated requirements following an attack in addition to the more general notification requirements.

3.2 Data sharing requirements

From a practical perspective, in the context of ECOSSIAN one must consider certain key issues regarding the security of communications and the state of the art in this regard. As both the positive notification requirements and the sharing functionality of ECOSSIAN will have to guarantee the secure transfer of data this analysis is important. However, these are rather legalistic concepts and the practical solution for the project must consider the implementation of a sharing functionality that respects the privacy by design model. Hence, the effective security measures must once again consider the state of the art regarding the security of these transfers and the implementation of any such functionality in a manner respecting the privacy by design principle.

In relation to data transfer ENISA makes certain recommendations vis-à-vis the implementation of secure private communications and highlights basic encryption models such as Transport Layer Security protocol as well as the Secure Shell protocol.[78] Certain end-to-end encryption technologies such as The Pretty Good Privacy software which would be capable of protecting messaging are also discussed.[79] In relation to the protection of the meta-data left exposed by end-to-end encryption certain anonymous communications are highlighted by ENISA namely: single proxies and VPNs, Onion Routing, Mix-networks and Broadcast schemes.[80] Such implementations should be considered.

As noted *supra* there are clear requirements for the processing of personal data under the privacy and data protection framework. Given that ECOSSIAN aims to share information one must also consider the effect of these requirements if it involves personal data. However, as the transfers in question are due to occur within the EU, restrictions or prohibitions on the free flow of data between Member States for data protection reasons are prohibited by Article 1(2) of Directive 95/46/EC. Moreover, the complex debates surrounding transfers to third party countries does not fall within the scope of the project. Nevertheless, there are still positive requirements at the O-SOC, N-SOC and E-SOC level. Similar to the above the data protection principles and grounds for processing must be satisfied. The additional concerns relate predominantly to the security of the processing itself and the requirements provided for

[78] *Ibid.*

[79] *Ibid.*

[80] *Ibid.*

under Article 17(1). These requirements are further supplemented by the obligation for confidentiality as found in Article 16 of Directive 95/46/EC, which concerns any controller processor relationship. Accordingly, in addition to the security requirements discussed *supra,* the confidentiality requirement extends to the N-SOC and E-SOC levels in addition to any third party processor that may be involved.

In the generic use case descriptions it is noted that following the detection of the threat by the TDM the information on the attack will be sent to the AACM. In this module the examination and designation of the anomaly as a threat will occur and a generated report will be sent to all local TDM. These processes are however within the general operation of the ECOSSIAN solution at a local level and the key concern relates more to the TMM and the RS modules. In the application of the generic issue warning scenarios the RS identifies the vulnerable components and those critical infrastructures employing similar modules and issues a warning relating to the attack. This will result in a decision to send a report to the relevant N-SOC (and in a similar fashion following analysis to the E-SOC) so that the information can be sent to the relevant parties employing the specific component.

Thus in the practical application of the data sharing requirements highlighted *supra* it must be understood that they should be assessed at each particular level (i.e. to the relevant authority or within the O-SOC, N-SOC and E-SOC levels). In addition; in relation to transfers, given the nature of the data flow each O-SOC, N-SOC and the E-SOC should consider filtering at each stage both in the flow of the information up the chain to the E-SOC and the distribution back out to the relevant N-SOCs and O-SOCs. This would ensure that only the relevant parties receive the information without any superfluous personal data. This would thus be a move towards compliance with req. 1.12 (necessary and adequate for the purpose) and req. 1.15 (Deletion). Accordingly, in the implementation of a sharing functionality the creation of a sharing mechanism capable of filtering and selecting recipients of the data would be beneficial. Furthermore, any such sharing mechanisms are required to respect req. 1.18 regarding the security of the ECOSSIAN solution. This also reflects the privacy by design recommendation for the encryption of all communications. Thus it is key for the purpose of ECOSSIAN that the following operation requirements are implemented in order to guarantee a privacy by design implementation. The applied requirements derived as examples from this analysis are highlighted in the following table:

Applied Req.	Description	Relevant general req.	Design strategy
AReq. 1.4	All communications should be encrypted	GReq. 1.18, GReq. 1.20, GReq. 1.21	Hide strategy and aggregate strategy
AReq. 1.5	Personal data are only transmitted as frequently as necessary for the system to operate and any such transfer should be encrypted and anonymised	GReq. 1.18, GReq. 1.20, GReq. 1.21	Hide strategy and aggregate strategy
AReq. 1.6	Systems should be designed to ensure that even where personal data are transmitted, any data elements which are not necessary to fulfil the purpose of the transmission are filtered out or removed.	GReq. 1.12, GReq. 1.13	Minimise strategy
AReq. 1.7	Systems should be designed so as to allow access to the transferred personal data only to the extent necessary for the role	GReq. 1.13	Minimise strategy

Applied Req.	Description	Relevant general req.	Design strategy
	being performed.		
AReq. 1.8	If possible, systems should be designed in separate compartments; this strategy calls for distributed processing instead of centralised solutions; in particular the ENISA suggests to store data in separate database, and these databases should not been linked.	GReq. 1.12, GReq. 1.13	Minimise strategy

Table 5. Applied Requirements Table II

Chapter 4 Implementation guidelines

Following the above discussion the table provided *infra* indicates some key recommendations for the implementation of the legal requirements in the ECOSSIAN solution. These implementation guidelines have been deciphered from the analysis provided.

Guide. No.	Description	WP**	Associated Req.	Comment
Guid. 3.1	Only the minimum amount of personal data should be collected and this needs to be taken into account in the TDM.	2, 3	GReq. 1.3	The highest level of aggregation should be used including the least amount of detail as this will restrict the amount of personal data that remains.
Guid. 3.2	Personal data and their interrelationships should be hidden from plain view. This is particularly relevant for the AACM and VM.	2, 3	GReq. 1.12, GReq. 1.13	There are a variety of means of implementing this strategy namely: the encryption of data, the use of mix networks to hide traffic patterns, the use of anonymisation or techniques to unlink the relationship between related events.
Guid. 3.3	The processing of the personal data should be in a distributed fashion to prevent the completion of full profiles of individuals. This is particularly relevant for the AACM and VM.	2, 3	GReq. 1.12, GReq. 1.13	Currently no design patterns for this strategy are known.
Guid. 3.4	Authentication protocols with privacy features should be implemented.	1	GReq. 1.18, GReq. 1.20, GReq. 1.21	
Guid. 3.5	The security of the personal data should be protected throughout the data lifecycle	1	GReq. 1.18, GReq. 1.20, GReq. 1.21	Encryption should be employed throughout with the default state of data being unreadable if there is a data leak
Guid. 3.6	Personal data should be securely disposed of at the end of its life-cycle or anonymised in compliance with the limited retention and data minimisation principles.	1	GReq. 1.12, GReq. 1.13, GReq. 1.15	
Guid. 3.7	All communications should be encrypted (i.e. significant for the RS implementation)	3	GReq. 1.18, GReq. 1.20, GReq. 1.21	
Guid. 3.8	Systems should be designed to ensure that even where personal data are transmitted, any data elements	3	GReq. 1.12, GReq.	

Guide. No.	Description	WP**	Associated Req.	Comment
	which are not necessary to fulfil the purpose of the transmission are filtered out or removed.		1.13	
Guid. 3.9	Systems should be designed so as to allow access to the transferred personal data only to the extent necessary for the role being performed.	3	GReq. 1.18, GReq. 1.20, GReq. 1.21	

*M – mandatory; O – optional

** Work Packages where this requirement should be implemented

Table 6. Legal Requierments Table

Chapter 5 Conclusion

To conclude, this deliverable has outlined the requirements and guidelines for the implementation of the ECOSSIAN solution. It has built upon the work completed in D7.1 and has provided insights in the application of the general requirements provided for by the legislation. Furthermore, it has also provided insights in the form of requirements and guidelines for the implementation of the privacy by design principle in the context of threat detection and analysis and information sharing. Reference should be made to the specific tables provided in the deliverable. These should form the basis for the implementation of a privacy compliant ECOSSIAN solution but will also be further built upon in D7.3 “Information sharing policies in disaster situations - Version 1”.

Chapter 6 List of Abbreviations

AACM	Aggregation Analysis Correlation Module
CERT	Computer Emergency Response Team
CI	Critical Infrastructure
CII	Critical Information Infrastructure
CIP	Critical Infrastructure Protection
CIIP	Critical Information Infrastructure Protection
CIWN	Critical Infrastructure Warning Information Network
DAE	Digital Agenda For Europe
DPA	Data Protection Act/Authority
ECI	European Critical Infrastructure
ECHR	European Convention of Human Rights
EPCIP	European Programme for Critical Infrastructure Protection
ENISA	European Network and Information Security Agency
IMM	Incident Management Module
NIS	Network Information Security
RS	Reporting System
TDM	Threat Detection Module
TMM	Threat Mitigation Module
VM	Visualisation Module

Chapter 7 Bibliography

7.1 Primary Sources

European Convention of Human Rights

Charter of Fundamental Freedoms of the European Union

European Parliament and Council, Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector [2002] OJ L201/37.

Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) [2002] OJ L108/33.

Commission Regulation (EU) No 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications [2013] OJ L173/2.

Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection [2008] OJ L345/75.

Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, [2013] OJ L218/8.

'Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)' COM (2012) 11 final.

'Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data', COM (2012) 011 final.

'Proposal of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union' COM (2013) 48 final.

ECJ Case‑274/99 *P. Connolly v Commission*, [2001] OJ C173/13.

CJEU Case C-131/12 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014] OJ C 212/4.

Law No. 78 17 of 6 January 1978 on "Information Technology, Data Files and Civil Liberty" ("Law") -The Directive 95/46/EC 95/46/EC was implemented via Law No. 2004-801 of 6 August 2004.

Bundesdatenschutzgesetz [Federal Data Protection Act], Dec. 20, 1990, BGBl. I at 2954, as amended: http://www.gesetze-im-internet.de/englisch_bdsg/federal_data_protection_act.pdf.

7.2 Secondary Sources

Article 29 Data Protection Working Party, Opinion 3/2013 on purpose limitation, adopted on 2 April 2013 WP 203 (02.04.2013) http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf accessed on 19/12/2014.

Article 29 Data Protection Working Party, Opinion 03/2014 on personal data breach notification adopted on 25 March 2014 693/14/EN WP 213 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf accessed on 18/01/2015.

Article 29 Data Protection 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 adopted on 1 December 2009, 02356/09/EN WP 168 http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf accessed on 20/12/2014.

Cavoukian A., 'Privacy by design in law, policy and practice. A white paper for regulators, decision-makers and policy-makers' (Information and privacy commissioner of Ontario, Canada 2011) https://www.ipc.on.ca/images/resources/pbd-law-policy.pdf accessed on 18/02/2015.

Cavoukian A., 'Privacy by design: the 7 foundational principles' (Information and privacy commissioner of Ontario, Canada 2009) https://www.ipc.on.ca/images/resources/7foundationalprinciples.pdf accessed on 18/02/2015.

Clifford D., Ricci A., Finocchiaro G.D., Proenca L., Van Der Sype YS and e Silva K., 'ECOSSIAN D7.1 Analysis of the applicable legal framework' (2014), 36 – 47.

Commission, 'Staff Working Paper Impact Assessment Accompanying the document Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) and Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data', SEC(2012) 72 final: http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_en.pdf.

Danezis G., Domingo-Ferrer J., Hansen M., Hoepman J-H., Le Métayer D., Tirtea R. and Schiffner S., 'The implementation of the Privacy and Data Protection by Design – from policy to engineering' (ENISA 2014) https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-and-data-protection-by-design accessed on 02//022015.

Dekker M., Karsberg C. and Daskala B., 'Cyber Incident Reporting in the EU: An overview of security articles in EU legislation' (ENISA 2012), http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/cyber-incident-reporting-in-the-eu accessed on 03/12/15.

European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European data protection law*, (Publication office of the EU Luxembourg 2014) 94.

Hildebrandt M. and Tielemans L., 'Data protection by design and technology neutral law' [2013] 29 Computer law and Security Review 509.

High Representative of the European Union for Foreign Affairs and Security Policy, Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 'Cybersecurity Strategy of the European

Union: An Open, Safe and Secure Cyberspace' JOIN (2013) 1 final: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf accessed on 19/12/2014.

Hoepman J-H, 'Privacy design strategies – (extended abstract) In ICT Systems Security and Privacy Protection' (29th IFIP TC 11 International Conference SEC Morocco, June 2014).

Jacobs B., 'Select before you collect' [2005] 54 Ars Aequi 1006.

Mitrou L. and Karyda M., 'EU´s Data Protection Reform and the right to be forgotten - A legal response to a technological challenge?' (5th International Conference of Information Law and Ethics Corfu-Greece, June 2012) 1-23.

Monreale A., Rinzivillo S., Pratesi F., Giannotti F., and Pedreschi D., 'Privacy-by-design in big data analytics and social mining', [2014] 3/24 EPJ Data Science Springer Open http://www.epjdatascience.com/content/3/1/10 accessed on 02/01/2014.

Pfitzmann A. and Hansen M., 'Anonymity, unlinkability, undetectability, unobserv-ability, pseudonymity, and identity management – a consolidated proposal for terminology', (version v0.34 Aug. 10, 2010) http://dud.inf.tu-dresden.de/Anon_Terminology.shtml accessed on 05/01/2015.

Savin A., *EU Internet Law* (Elgar European Law, Cheltenham, 2013) 190-218.

Sweeney L., '*k*-anonymity: A model for protecting privacy' [2002] 10(5) International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems 557.

van der Sloot B. and Borgesius F.Z., "Google and Personal Data Protection" in A. Lopez-Tarruella (ed.) *Google and the Law: Empirical Approaches to Legal Aspects of Knowledge-Economy Business Models* (Springer Information Technology and Law Series Vol. 22 2012) 75-111.

Vedder A., Clifford D., and Van Der Sype Y.S., 'ECOSSIAN D9.3 Report from Data Protection Coordinator – Version 1', B. Nussbaumer (ed.) (2015).

World Economic Forum, *Insights Report. Global Risks 2014 (Ninth Edition)*, Switzerland, 2014, 17, http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2014.pdf accessed on 08/01/2015.