D7.6

Legal evaluation of the ECOSSIAN system and recommendations

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:	SEC-607577 / D7.6/ 1.0
Work package contributing to the deliverable:	WP7
Due date:	March 2017 – M34
Actual submission date:	28th March, 2017

Responsible organisation:	KUL
Editor:	Jessica Schroers
Dissemination level:	PU
Revision:	1.0

Security Sensitivity Committee Review performed on:	23rd March, 2017
Comments:	N/A

Abstract:	This deliverable includes a legal evaluation of the ECOSSIAN system, based upon an assessment of the compliance of the requirements as specified in D7.2, which have been updated considering the adoption of the General Data Protection Regulation. Furthermore, it provides an overview on the NIS Directive and gives recommendations for a potential future deployment of ECOSSIAN.
Keywords:	Privacy, Data Protection, Critical Infrastructure Protection, Security, ethical impact and legal compliance

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

Jessica Schroers (KUL)

Contributors (ordered according to beneficiary numbers)

Alessandra Spangaro (UNIBO)

Erik Zouave, Plixavra Vogiatzoglou, Eline Dekyvere (KUL)

Executive Summary

This deliverable provides a legal analysis of the ECOSSIAN system. As an evaluation, is it based upon the requirements as they were defined in D7.2. Of course, there is also a wider legal and ethical scope, which however will not be analysed in this deliverable. Legal aspects regarding information sharing are analysed in D7.7, regarding public private partnerships in D7.9 and D7.10 and a methodology and assessment of a combination of different legal, ethical, economic, political and societal factors is provided in D7.11.

This deliverable includes an assessment of the compliance of the requirements as specified in D7.2 and provides recommendations for a potential future deployment of ECOSSIAN. D7.2 had defined 21 general requirements and 9 implementation guidelines. In general ECOSSIAN fulfils the requirements as far as it was possible to assess this on a technical level.

Chapter 2 focuses on the general requirements. In this chapter, first the privacy and data protection requirements are outlined and it is assessed in how far they are fulfilled in the ECOSSIAN system. During project time the adoption of the GDPR took place. Since therefore a significant change has occurred, first the alignment of the previous requirements is assessed against the requirements provided by the GDPR. Afterwards, it is analysed in how far ECOSSIAN is able to fulfil these requirements, providing an overview as well as how ECOSSIAN organisationally and technically has addressed the data protection requirements, e.g. with the function of a human operator and the anonymization tool. As many requirements are only possible to be fully assessed in case of a full operation of ECOSSIAN by different entities, for these requirements only general guidelines and recommendation can be provided. Especially the use of a data protection impact assessment is recommended, and contractual safeguards for controller-controller or controller-processor relationships.

Secondly, the security and critical infrastructure requirements are shown. Here again a legal change has happened during project time as the NIS Directive has been adopted. This section provides an overview of the NIS Directive and shows that ECOSSIAN aligns well with it.

Chapter 3 gives an overview of the evaluation of the nine implementation guidelines in a table form, taking into account also the results of Work package 5 as described in D5.6.

Finally, Chapter 4 outlines the conclusion and recommendations for the potential implementation of an ECOSSIAN system. However, the analysis and recommendations can only be provided on a generic level, and will need to be elaborated and tailored in detail for every sector and CI provider when ECOSSIAN would be implemented. Considering that different sectors process different types of personal data, special focus was given in this deliverable to the requirement of a Data Protection Impact Assessment, as this will provide an indication of which type of data might be transferred if the CI operator would use the ECOSSIAN system.

Contents

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 functions such as threat monitoring, early indicator and real threat detection, alerting, support of threat mitigation and disaster management in a privacy compliant manner.

As explained in D2.2, the ECOSSIAN project developed a 3-level architecture of different SOC levels. Similarly to a CI enterprise SOC and having the same functionality is the O-SOC. The O-SOC monitors the networks and systems of the organization for intrusions and additionally provides the functionality of sharing incidents with the corresponding N-SOC and of receiving warnings.[2] In order to protect multiple CI operators against highly sophisticated attacks, the envisaged ECOSSIAN system includes a N-SOC in each of the participating countries.[3] The mission of the N-SOC is to enable trusted information exchange between the different SOC levels and to aggregate information from different O-SOCs and it is supposed to be a coordinating SOC[4]. To help operators across different countries to defend against a coordinated, large-scale, transnational attack on the infrastructure (e.g. the power grid), the E-SOC is introduced with the main purpose of delivering situational awareness on a European level and to monitor CIs and their interdependencies.[5] The ECOSSIAN project provides the technical solutions for such a system. The purpose of this deliverable is to provide an analysis of the compliance with the legal requirements as set out in D7.2.

Chapter 2 focuses on the general requirements. In this chapter, first the privacy and data protection requirements are outlined and it is assessed in how far they are fulfilled in the ECOSSIAN system. During project time the adoption of the GDPR took place which will start to apply from 2018 on. Furthermore, the Brexit decision was made. However, this deliverable focuses on the GDPR and does not assess separately the legal framework of the UK, as the UK has indicated to adhere to the GDPR.[6] Since with the adoption of the GDPR a significant change has occurred, first the alignment of the previous requirements is assessed against the requirements provided by the GDPR. Afterwards, it is analysed in how far ECOSSIAN is able to fulfil these requirements.

As many requirements can be fully assessed only in case of a full operation of ECOSSIAN by different entities, the focus is also on possible considerations in such a case. Especially the use of a data protection impact assessment is recommended. Secondly the security and critical infrastructure requirements are shown. Here again a legal change has happened during project time as the NIS Directive has been adopted. This section provides an overview of the NIS Directive and how ECOSSIAN aligns with it.

Chapter 3 gives an overview of the evaluation of the nine implementation guidelines in a table form, taking into account also the results of Work package 5 as described in D5.6.

Finally, Chapter 4 outlines the conclusion and recommendations for an ECOSSIAN system.

---

[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] D2.2., p. 42.
[3] D2.2, p.42.
[4] D2.2., p.42.
[5] D2.2, p.42.
[6] see e.g. https://www.huntonprivacyblog.com/2017/02/03/uk-government-quizzed-gdpr-implementation-post-brexit-data-protection/, furthermore will the UK in 2018 still be within the EU and is therefore obliged to adhere to the Regulation, but it is expected that the GDPR will include similar provisions to ensure an ongoing data flow between the UK and the EU.

Chapter 2 Evaluation of compliance with the requirements

2.1 Privacy and data protection requirements

2.1.1 Processing of personal data in the ECOSSIAN system

According to D2.2., the main tasks of the O-SOC are the provision of alerts and warnings, incident analysis, incident response on site, incident response support and coordination, business continuity and disaster recovery planning and security-related information dissemination.[7]

D2.2. defines certain tasks that can be fulfilled by the N-SOC. These can be for example alerts and warning services, incident response support and coordination, vulnerability analysis, artefact handling and analysis, announcement service, technology watch, security-related information dissemination, risk analysis and situational awareness.[8] For the E-SOC, less core-services are foreseen, the E-SOC in general should also provide alerts and warning services, incident response support and coordination, artefact handling, announcement services and security-related information dissemination and finally the E-SOC is in a good position to provide a situational awareness service for a bigger overview of the European cyber security & threat landscape.[9]

Most of the information containing personal data will be processed within the organizations responding to threats and incidents (O-SOC level). O-SOCs may act as responders for multiple organizations. The O-SOCs will process data relating to devices, processes, and users. The users will most likely consist of employees or customers of a service. Information from attackers will also be processed if available. In certain cases, O-SOCs might have to deal with attacks where third party personal data is compromised both by the attacker and the responders, such as attacks launched via botnets.

The personal data that may be processed within an organization is highly contextual. Anything and everything linking the human, the machine(s), and networks can give clues regarding the nature of threats and incidents. So-called “indicators of compromise” vary between sectors. The financial sector, for example, will process personal data relevant to investigations on fraud, typically information on accounts and account holders. The focus will be on the victims of fraud, such as their names, birthdates, account details, and transaction details. For e-identity providers, indicators of compromise can even be closely linked to unique identifiers. In other sectors, such as the energy sector, the attacks may target employees of the organization. The behavioral patterns of employees and documents stored on systems can become indicators of compromise.[10] However, ECOSSIAN focuses especially on the ability to monitor Industrial Control Systems (ICS)[11] and relies specifically on systems such as Honeypot and BPIDS, which capture rogue traffic, MAC addresses and IP-addresses in particular.

In a first step, data is collected. Which information can be used or is available depends on

[7] D2.2, p.27.
[8] D2.2, p.32 ff.
[9] D2.2, p.32 ff.
[10] See in this regard e.g. the DOGANA project http://www.dogana-project.eu/.
[11] D2.2., p.42.

the constituents.[12] The O-SOC typically will have access to multiple monitoring systems, which are collecting data related to various activities within an organization. This includes low-level information like network traffic, user actions, application logs, samples of executable files, documents, email messages and many others. "*In ECOSSIAN the internal source is represented in the Acquisition functional block where the ECOSSIAN sensors are placed. This includes CI system status from different sources like networks, SCADA/ICS components, external sensors and other data sources dedicated to "legacy". Additionally a set of sensors like IDS, system monitors, sensors and other security appliances are placed there. Via the Legacy Interface FB it is also possible to capture data from legacy devices if they are supported*."[13] Therefore, in principle a big amount of (possibly personal) data can be available. Personal data, as explained in D7.1 and D7.2, is data that relates to an identified or identifiable natural person. 'Identifiable' means a person who can be directly or indirectly identified, for example by a name, an identification number, location data, an online identifier or by one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. To assess whether a person is identifiable, all the likely means for identifying the person that could be used either by the controller or by another person need to be taken into account.

A special position which resulted in a legal hurdle for information sharing was the status of IP addresses, which in some countries were considered personal data while in other countries not.[14] In 2016, the Court of Justice of the European Union (CJEU) decided a case regarding the status of dynamic IP addresses which provided a certain clarification in this question. This case is commonly referred to as the Breyer case[15]. It was questioned whether the classification of IP addresses as personal data extends to dynamic IP addresses in situations where the website operator who processes the IP addresses does not have the identifying information necessary to link them to individual users. In such cases, the identifying information is instead held by a third party (i.e. the ISP) and is therefore beyond the reach of the website operator without direct cooperation between the parties. The CJEU considered that the possibility to combine a dynamic IP address with the additional data held by the internet service provider could constitute a means likely reasonably to be used to identify the data subject, as is the case in Germany where legal channels exist to obtain the information. The Advocate General had pointed out that a dynamic IP address would not be considered personal data if the identification of the data subject was prohibited by law or if it was practically impossible due to the required disproportionate effort in time, cost and man-power, resulting in an insignificant risk of identification.

This means that, considering that ISPs keep a record of the person's account to whom a dynamic IP address has been given, and in many countries where (legal) means exist to access the information, IP addresses are generally considered personal data.[16] The reasoning of the court regarding likely reasonable means can also be applied regarding other information than dynamic IP addresses. Therefore, for example MAC addresses could be considered personal data in the same way if a register or other information which links them to a natural person exists and this information is accessible by legal or other reasonable means. On the other hand, if it is known that a specific IP address does not relate to an identified or identifiable person, e.g. because it has been assigned to a machine within the company and it is not possible to deduct in any way for example that a specific person is

[12] D4.2, p.15.
[13] D4.2, p.15.
[14] also mentioned as a point of concern for information sharing between CERTs in R. Bourgue, J. Budd, H. Homola, M. Wladenko, D. Kulawik, Detect, SHARE, Protect – Solutions for Improving Threat Data Exchange among CERTs, October 2013, p.8.
[15] CJEU Judgement Case C-582/14 19 October 2016 (Breyer).
[16] Article 29 Working Party, Opinion 4/2007 on the concept of personal data, WP 136, 20 June 2007.; WP 37: Privacy on the Internet - An integrated EU Approach to On-line Data Protection- adopted on 21.11.2000. ; CJEU Judgement Case C-582/14 19 October 2016 (Breyer).

working at this machine, this IP address would not be considered personal data. Similarly, as soon as ISPs delete the information connecting the IP address to a specific person, and there is no other information available to connect the IP address to a person (e.g. a form where a user has filled in personal information and the IP address has been saved), the IP address will no longer be considered personal data.

This difficult assessment is the main challenge for ECOSSIAN, as in case where personal data is processed the data protection legislation applies, while it does not apply in case no personal data is processed. However, it is often difficult to assess whether personal data is processed as it will depend on the circumstances, which in case of a project cannot be assessed beforehand. In the ECOSSIAN project itself, no personal data has been processed by the system. With regard to the ECOSSIAN system, the possible compliance of system with the requirements as specified in D7.2 is analysed in this deliverable. As it is not possible to assess several requirements on a system level since it will depend on the implementation and the scope of data will depend on the company where it will be implemented, different technical and organisational solutions, mainly at the O-SOC level, have been included in the system or are recommended (e.g. a DPIA, see section 2.1.2). These are focused on the O-SOC level, since, as mentioned earlier, there the initial collection of the data takes place. Therefore, if the data minimisation principle is complied with, it is most likely that none or not much personal data will be transmitted via ECOSSIAN to the N-SOC or even E-SOC. In the next sections the compliance of ECOSSIAN with the general legal requirement as identified in D7.2 will be assessed. At the beginning of every section the requirement from D7.2 has been included:

Req. number	Description	Importance* (M/O)	Relevant for Level			Comment
			O-SOC	N-SOC	E-SOC	

*M – mandatory; O – optional

Afterwards a potential requirement change due to the introduction of the GDPR will be shown and explained. Finally, an assessment of the compliance of the ECOSSIAN system with the requirement is made.

2.1.2 Notification and authorisation requirements

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[17]	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.

[17] 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	
GDPR GReq. 1.1'	The risk of the processing operations should be determined. Considering the specific risk of the data processing, a data protection impact assessment might need to be done.	M	x	x	x	Art. 35 GDPR

GDPR changes:

One of the original requirements was that notification and authorisation requirements must be respected. Though still applicable during the project, this requirement is not applicable for an ECOSSIAN system anymore. As pressed in recital 89 of the GDPR, the general obligation to notify personal data processing to supervisory authorities did not substantially improve the protection of personal data and has therefore been abolished in the GDPR. Instead, the aim of the GDPR is to establish effective procedures and mechanisms for processing operations which could form a high risk to the rights and freedoms of natural persons. The measure of choice in those cases is a data protection impact assessment which should be carried out by the controller before the processing takes place. This is done in order to assess the particular likelihood and severity of the risk, taking into account the nature, scope, context and purposes of the processing and the sources of the risk. The measures, safeguards and mechanisms to mitigate the risk should be included in the data protection impact assessment.

The GDPR gives an indication of what type of processing operations could possibly be considered high risk and need a data protection impact assessment beforehand. These are processing operations relating to automated decision making, large scale processing of special categories of data or of personal data relating to criminal convictions and offences, or the large scale systematic monitoring of a publicly accessible area. Furthermore, if the processing operations use new technologies, or in general the nature, scope, context and purposes of the processing are likely to result in a high risk, an assessment is required. The supervisory authority can provide lists of processing operations, which do require a data protection impact assessment, as well as processing operations for which no data protection impact assessment is required.

The next section provides an overview of risk assessment and Data Protection Impact Assessment.

Risk assessment:

The GDPR requires the controller in any case of processing to make a risk assessment and to document it. This requirement can be found in article 24 GDPR, which obliges the controller to take into account the risks of varying likelihood and severity for the rights and freedoms of natural persons in order to implement appropriate technical and organisational measures. The risk assessment needs to be done every time something changes, since article 24 GDPR requires review and update of the measures when necessary, and the controller needs to ensure and be able to demonstrate that processing is performed in accordance with the GDPR. A risk assessment is also required for the implementation of data protection by design (art. 25 GDPR) and in order to ensure a level of security appropriate to the risk(article 32 GDPR).

The evaluated level of risk on the other hand has influence on the obligations of controllers. The GDPR calls for an assessment whether the data processing operations involve a risk or a high risk (recital 76). However, also the existence of no or minimal risk (defined as

processing operations which are unlikely to result in a risk) could have influence on the obligations of the controller.

Therefore three levels can be distinguished:

"**unlikely to result in a risk**": The obligation to designate a representative in the Union does not apply in case of "*processing which is occasional, does not include, on a large scale, processing of special categories of data […] or processing of personal data relating to criminal convictions and offences […], and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing*."[18] Furthermore, if a data breach occurs, but if the controller can demonstrate that the breach is unlikely to result in a risk to the rights and freedoms of natural persons, the controller is exempted from the requirement to notify the data breach [recital 85 and art. 33].

"**risk**": Throughout the Regulation, obligations are enshrined which require controllers to employ technical and organisational measures to ensure a level of security appropriate to the risk. While the fact that processing is unlikely to result in a risk relieves the burden on the controller, in case the processing is likely to result in a risk the burden can be increased. For example in article 30 (5) GDPR, the exemption from the record keeping obligation for enterprises or organisations employing fewer than 250 persons cannot be invoked if the organisation's processing activities might result in a risk for the rights and freedoms of data subjects. The European Data Protection Board may issue guidelines regarding which processing operations are considered to be unlikely to result in a high risk and which measures may be sufficient to address the risk.[19]

"**high risk**": Prior to high risk processing the controller needs to do a data protection impact assessment (art. 35 GDPR), and if this assessment confirms the high risk, he or she needs to consult the supervisory authority prior to processing.[20] Three examples that might constitute high risk are listed in art. 35 (3) GDPR : systematic and extensive evaluation of personal aspects, based on automated processing (including profiling) on which decisions are based that produce legal effects or similarly significantly affect the natural person; large scale processing of special categories of data or data relating to criminal convictions and offences; or systematically large scale monitoring of public places. In case a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller is additionally obliged to inform the data subject of the breach without undue delay.[21] This can only be avoided if certain risk reducing measures are taken, in particular measures that render the personal data unintelligible to any person who is not authorised to access it.[22]

1) Which risk needs to be assessed?

Risk is usually assessed in terms of likelihood and severity/seriousness. However, a risk assessment in the field of data protection should not be confused with the general procedure of risk management, which normally addresses risks for organizations and their activities.[23] Also, the assessment in numerical values given for the likelihood and severity is criticized, as

[18] article 27 2 (a) GDPR.
[19] Recital (77) GDPR
[20] art. 36 GDPR
[21] art. 34 GDPR.
[22] art. 34 (3) (a) GDPR.
[23] Felix Bieker et al., "A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation," in *Privacy Technologies and Policy*, vol. 9857, Lecture Notes in Computer Science (Cham: Springer International Publishing, 2016), 24, http://link.springer.com/10.1007/978-3-319-44760-5.

for example the severity of an impact on data subjects cannot be measured in numbers.[24] Currently no general agreed way to assess risk in the field of privacy and data protection exists, even though several guidance documents are available. Within the ECOSSIAN project, an evaluation methodology has been developed to evaluate not specifically privacy and data protection risks, but general legal, ethical, economic, political and societal risks (see D7.11).

The GDPR defines that the risk that needs to be assessed is the risk to the rights and freedoms of natural persons [art. 35 (1) GDPR, recital 77]. It is further mentioned in the GDPR that this risk may result from personal data processing, which could lead to physical, material or non-material damage.[25] The recital also includes a non-exhaustive list of possible harms resulting from processing:

- discrimination,
- identity theft or fraud,
- financial loss,
- damage to the reputation,
- loss of confidentiality of personal data protected by professional secrecy,
- unauthorised reversal of pseudonymisation,
- any other significant economic or social disadvantage;
- where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data;
- where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures;
- where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles;
- where personal data of vulnerable natural persons, in particular of children, are processed;
- where processing involves a large amount of personal data and affects a large number of data subjects.

Security risks, which are only a part of the risk addressed in a DPIA, also need to be assessed. Moreover, the controller needs to take measures to mitigate those risks in order to ensure an appropriate level of security [rec 83]. For an appropriate level of security, including confidentiality, the state of the art and the costs of implementation should be weighted with the risks and the nature of the personal data to be protected [rec 83]. Specific risks mentioned are “accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to, personal data transmitted, stored or otherwise processed” which may in particular lead to physical, material or non-material damage [rec 83]. [26]

2) How should the risk be assessed?

The GDPR does not define a specific model, but states that in order to evaluate whether processing operations involve a risk or a high risk, an objective assessment should be made

[24] Felix Bieker, Marit Hansen, and Michael Friedewald, “Die Grundrechtskonforme Ausgestaltung Der Datenschutz-Folgeabschätzung Nach Der Neuen Europäischen Datenschutz-Grundverordnung,” Zeitschrift für Datenschutz-, Informations- und Kommunikationsrecht, no. 4 (2016): 193.
[25] recital 75 GDPR.
[26] art. 32 (2) GDPR.

of the severity and likelihood of the risk to the rights and freedoms of the data subject, which is determined by looking at the nature, scope, context and purposes of the processing.[27]

Therefore, currently only indications exist on how to assess the risk. Indications pointing towards a high risk that needs to be assessed in a DPIA are specified below.

Data Protection Impact Assessment (DPIA)

1) When is a DPIA required?

The GDPR lists certain types of processing operations, which are likely to constitute a high risk and where a DPIA might be required. These are for example:

- processing operations relating to automated decision making,
- large scale processing of special categories of data or of personal data relating to criminal convictions and offences, or
- the large scale systematic monitoring of a publicly accessible area.[28]

An assessment is also required if the processing operations use new technologies, or in general the nature, scope, context and purposes of the processing are likely to result in a high risk.[29] The supervisory authority shall provide a list of processing operations, which do require a data protection impact assessment, as well as processing operations for which no data protection impact assessment is required.[30] The aim of the DPIA is not only to identify the high risks, but even more so to mitigate them.

2) How is a DPIA done?

There is currently no European wide standard risk assessment. As noted by Bieker et al., various approaches existed to adapt an impact assessment model for the area of privacy and data protection, but the attempts had a wide range, as there was no obligation for controllers to do such an assessment.[31] Most likely, this will change with the GDPR coming into force.[32] Therefore, in future more guidance might become available.[33] The Data protection authorities can be seen as the best source for a future DPIA model.[34] Furthermore, approved codes of conduct, certifications, guidelines provided by the European Data Protection Board as introduced by the GDPR or indications provided by a data protection officer[35] could be possible sources of guidance regarding the "identification of the risk related to the processing, their assessment in terms of origin, nature, likelihood and severity and the identification of best practices to mitigate the risk "[36].

[27] recital 76 GDPR.
[28] art. 35 (3) GDPR.
[29] art. 35 (1) GDPR.
[30] art. 35 (4) and (5) GDPR.
[31] Felix Bieker et al., "A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation," 22.
[32] Ibid.
[33] See for example the work on a DPIA for smart grids: https://ec.europa.eu/energy/en/test-phase-data-protection-impact-assessment-dpia-template-smart-grid-and-smart-metering-systems
[34] Ibid.
[35] When a data protection officer is designated, the controller is anyway obliged to seek the advice, see art. 35 (2) GDPR.
[36] Recital 77 GDPR.

The GDPR does not refer to a specific model for a DPIA, but states the minimum requirements for carrying out a DPIA.[37] Therefore, a data protection impact assessment contains at least:

1) a systematic description of the envisaged processing operations and the purposes of the processing, and in case the legitimate interest of the controller is considered the legal ground for processing, it also includes the legitimate interest;

2) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

3) an assessment of the risks to the rights and freedoms of data subjects; and

4) the measures envisaged to address the risks (e.g. safeguards and security measures).

Two approaches

Two interesting recent approaches come from the French DPA called CNIL[38] and the German DPA[3940]. The German approach is partially based on the German standardized data protection model[41], which, in its turn, is based on the methodology of the IT Baseline Protection from the German Federal Office for Information Security, implementing the ISO 27000 international standard series.[42] It is currently still under development.

The French approach has been developed before the GDPR was published and is divided in four stages: the context stage, controls stage, risks stage and decision stage.

Both approaches will be compared below along the 4 steps above, in order to analyse which basic requirements for the DPIA can be established. However, it is recommended that for example the CI provider when doing a DPIA also for a full analysis considers set methodology of the local DPA or for the specific sector/technologies, e.g. the DPIA for smart grids.

1) <u>A systematic description of the envisaged processing operations and the purposes of the processing, and in case the legitimate interest of the controller is considered the legal ground for processing, it also includes the legitimate interest</u>

Both approaches require in a first step a systematic description of the envisaged processing operations as described in the GDPR.

The German process focuses in the first stage on the description of the data and their formats, the used IT-Systems and their interfaces and the process and functions, and requires at the same time to specify the purpose of the described processing operations, to identify the actors and concerned parties and to identify the relevant legal requirements.

[37] art. 35 (7) GDPR.

[38] CNIL (Commission Nationale de l'Informatique et des Libertés, "Privacy Impact Assessment: Methodology (How to Carry out a PIA)," 2015.

[39] Felix Bieker et al., "A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation."

[40] Marit Hansen, "Datenschutz-Folgenabschätzung–gerüstet Für Datenschutzvorsorge?," *Datenschutz Und Datensicherheit-DuD* 40, no. 9 (2016): 587–591.

[41] Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, "Das Standard-Datenschutzmodell - Konzept Zur Datenschutzberatung Und -Prüfung Auf Der Basis Einheitlicher Gewährleistungsziele, V.0.9," 2015.

[42] M. Hansen, M. Jensen, and M. Rost, "Protection Goals for Privacy Engineering" (2015 IEEE CS Security and Privacy Workshops, IEEE, 2015), 164.

The French approach refers to the first step as the definition and description of the context of the processing and requires the description of the processing, the purpose, the identification of data controller and processor. They add the requirement of a description of the stakes (the benefits for the organisation, data subject or society in general) and require for a description of the scope, a detailed description of the concerned personal data, their recipients and retention periods and the description of the processes and personal data supporting assets for the entire personal data life cycle.

Both approaches seem similar in this regard, as they require in accordance with the GDPR a detailed description of the processing. Small differences are found in that the French approach includes the stakes and points in their description during the personal data lifecycle, while the German approach puts attention to the technical implementation of the processing and require the identification of actors and concerned parties, which is wider than the requirement of the French approach to identify data controller and processors. The German approach requires already in the first step the identification of the relevant legal requirements, while the French approach in its second step, the controls step, specifies a list of legal requirements and requests the definition of controls to comply with them. Both approaches require a definition of the purposes of the processing as defined in the GDPR, however, in contrast to the GDPR, none of them explicitly refers in the first stage to the definition of the legitimate interest of the controller in case it is used as a legal ground.

In general, the description should include:

- personal data concerned (and their formats)
- the IT systems and interfaces
- process and functions

→ all the above for the entire personal data life cycle (from collection to erasure)

- recipients
- retention periods
- the actors and concerned parties
- purpose of the data processing

2) An assessment of the necessity and proportionality of the processing operations in relation to the purposes

The GDPR requires an assessment of the necessity and proportionality of the processing operations in relation to the purposes. This is not as such worked out in a specific step in the German or French approach. However, both approaches require a description of the processing and its purpose. Since principally the amount of data is limited to what is strictly necessary to fulfil this purpose, processing would be illegal if the processing operation would exceed the purpose. Furthermore, in an analysis of the risk the German approach also considers at least the intensity of the interference of the processing operation and especially the data protection goal of data minimisation. Use of the data protection goal of data minimisation includes in principle an assessment of the necessity and proportionality of the processing operations in relation to the purpose, as it requires that only those data should be processed which are directly necessary for the purpose.[43]

In general: the main focus of both approaches lies on the risks.

[43] Felix Bieker, Marit Hansen, and Michael Friedewald, "Die Grundrechtskonforme Ausgestaltung Der Datenschutz-Folgeabschätzung Nach Der Neuen Europäischen Datenschutz-Grundverordnung," 192.

3) An assessment of the risks to the rights and freedoms of data subjects

Both approaches require an identification of possible attackers, attacking reasons and attacking goals (in the French wording: the relevant risk sources and their capabilities).

Which risk needs to be assessed and how should that risk be defined? The GDPR requires an assessment of the risks to the rights and freedoms of data subjects.

At this point, differences between the German and the French approach become visible. The German approach considers that every processing of personal data is in principle an interference with the fundamental right as specified in art. 8 ECHR.[44] Accordingly, every processing is a risk for the rights of the data subjects and the intensity of the interference needs to be assessed (also in order to balance the rights and interests of the data subject and the controller).[45] The German approach focuses on the data protection goals (data minimisation, unlinkability, transparency, intervenability, availability, integrity and confidentiality). The intensity of interference (Eingriffsintensität) assesses the impact of the interference for the data subject. The protection standard is established from the view of the data subject, and should never be lower than normal.[46] Depending on the circumstances (e.g. processing of special categories of data, missing transparency or intervenability) the necessary protection standard can be higher.[47] The German approach distinguishes three categories of protection standards: normal, high (e.g. special categories of data, or the data subject is dependent on the organisation and the processing can have serious impacts on the data subject, or there are no controls available for the data subject) or very high (e.g. the service or decision of the controller is existential for the data subject and other risks exists, or an accumulation of different aspects exists, e.g. when personal data of a big group of data subjects are collected or for various purposes and data subjects are affected in different roles).[48]

The French approach focuses on three feared events (illegitimate access to personal data, unwanted modification of personal data and disappearance of personal data).[49] For these feared events the potential impact on the data subjects' privacy is assessed, and the prejudicial effect of the potential impact and the controls to modify it (considered the *severity* of the feared event). Furthermore, it is assessed how these feared events could happen (considered the threats), which risk sources could be responsible for it and how likely it is, considering the capabilities of the risk sources, the vulnerabilities of the systems and the controls (*likelihood*).[50]

The risk assessment in the French approach is then done by using the severity of the feared event and the likelihood of the threats associated with the feared event to determine the level of different risks for data protection.

On the contrary, the German approach rejects the idea of using specific values of severity and likelihood to determine the risk, as e.g. the damage to the data subject is rarely possible to be measured in numerical values. Therefore, they prefer that the controller provides a

[44] Ibid., 190.
[45] Ibid., 190, 192.
[46] Ibid., 192.
[47] Ibid., 193.
[48] Ibid.
[49] even though in their examples they seem to consider also other feared events.
[50] CNIL (Commission Nationale de l'Informatique et des Libertés, "Privacy Impact Assessment: Methodology (How to Carry out a PIA)," 15.

comprehensible documentation of the argumentation of the risk level, depending on the attack scenarios and the data protection goals.[51]

In general: Assessment of the risk for the rights and freedoms of the data subject:

Main questions: In how far is the processing a risk for the fundamental rights (especially the right to data protection) of the data subject?

- identification of possible sources of risks (e.g. attackers, but also the controller itself), their reasons, goals and possible capabilities
- Which impact could the processing (also possible illegal processing because the data was illegally accessed) have on the data subject or others? German approach: intensity of interference and standard of protection, French approach: severity.
- What is the likelihood of the threats?

4) The measures envisaged to address the risks (e.g. safeguards and security measures)

Finally, the GDPR requires a specification of the envisaged measures to address the identified risks.

One difference between the two approaches is the point at which potential safeguards/controls are first identified. The French approach already as a second step identifies existing or planned controls, while the German approach does this towards the end, after identification of the risk (though it might implicitly be included in the description of the system). However, as both approaches envisage a continuous improvement process, which might require several iterations, this should make no difference.

Both approaches require throughout the whole analysis to possibly go back to previous steps and to analyse which safeguards can be implemented for identified risks. The German approach might have an advantage, since the technical working group of the conference of German data protection authorities (AK Technik) develops a catalogue of data protection measures, which can be useful in the identification of possible protection measures.[52] However, in the end these measures need to adequately remedy the identified risks. In order to assess this, the German approach requires testing and documentation of the effectiveness of the protection measures.[53] Likewise, the French approach requires an evaluation of the assessment and whether it can be considered acceptable. Furthermore, it requires, like the German approach, an action plan for all the planned controls and that these controls should be set out formally, implemented, monitored regularly and improved continuously.[54]

As a final step, it is always required to document all the information, prepare and publish a report and possibly provide this report to the supervisory authority.

In general:

- identification of adequate measures for each risk (catalogue of reference data protection measures can help)
- analysis the remaining risk and whether it can be further mitigated. If not, is it acceptable?

[51] Felix Bieker, Marit Hansen, and Michael Friedewald, "Die Grundrechtskonforme Ausgestaltung Der Datenschutz-Folgeabschätzung Nach Der Neuen Europäischen Datenschutz-Grundverordnung," 193.

[52] Felix Bieker et al., "A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation," 32.

[53] Hansen, "Datenschutz-Folgenabschätzung–gerüstet Für Datenschutzvorsorge?," 590.

[54] CNIL (Commission Nationale de l'Informatique et des Libertés, "Privacy Impact Assessment: Methodology (How to Carry out a PIA)," 16.

- Implementation of the measures and test whether they are effective
- Documentation and proof of compliance, possibly publish the report

Conclusion:

As the comparison shows, both approaches generally align with the requirement of the GDPR and have advantages and disadvantages. The advantage of the French approach is the checklist approach, which makes the assessment easier, but also entails the risk of overly focusing on the points set out instead of adapting the process to the specific risks and requirements of an individual data processing operation.[55] The restriction of the French approach is accordingly the focus on certain limited feared events. The focus of the German approach is more fundamental, since every data processing is considered an infringement of a fundamental right.

3) What happens when the DPIA is done?

1) The DPIA indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk:

In case the DPIA indicates a high risk for individual rights, the competent data protection authority needs to be consulted [art. 36]. Certain information needs to be provided to the supervisory authority, including the DPIA. The supervisory authority shall then provide written advice within a period of maximum eight weeks (which may be extended by six weeks if the intended processing is very complex), and the periods may be suspended until the supervisory authority has obtained all requested information.[56] In case a supervisory authority does not consider it possible to bring processing operations into compliance with the Regulation, it has the power to impose a ban on processing.[57]

2) The DPIA indicates that the processing would not result in a high risk, and that the measures taken mitigate the risk:

The GDPR does not specifically provide for what needs to be done regarding documentation or presentation of results of a DPIA.[58] Regarding the general documentation, it is advisable that the controller keeps the records of the DPIA, since according to art.30 GDPR and recital (82) in order to demonstrate compliance with the Regulation, the controller is required to keep a record of processing activities under its responsibility. The supervisory authority can request the information.[59] For transparency it would be useful to publish at least a shortened version of the DPIA report.[60]

Finally, in case the risk changes, a new iteration of the DPIA might be required.[61]

Recommendation ECOSSIAN

As ECOSSIAN is a large scale project, which can be implemented in various different ways and in different sectors, it is not possible to make a complete DPIA for ECOSSIAN itself at

[55] Felix Bieker et al., "A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation." 22.
[56] art. 36 (2) GDPR.
[57] art. 58 (2) (f) GDPR.
[58] Felix Bieker et al., "A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation," 26.
[59] art. 58 (1) (a) GDPR
[60] Felix Bieker, Marit Hansen, and Michael Friedewald, "Die Grundrechtskonforme Ausgestaltung Der Datenschutz-Folgeabschätzung Nach Der Neuen Europäischen Datenschutz-Grundverordnung," 196.
[61] art. 35 (11) GDPR.

this point of time. Every sector will be processing different types of data, including e.g. health data, employee data or financial data. During the project time it was not possible to assess which data exactly will be transferred and it is not possible to automatically assess whether personal data and possibly even sensitive personal data is among the transferred data, therefore a human operator is included in the system which would check the dataset before transferring it in the ECOSSIAN system. In order to make a risk assessment of the possible data that could be transferred in the ECOSSIAN system, it is recommended that every CI provider, that will transfer information to the ECOSSIAN system, will make a DPIA when implementing the ECOSSIAN system. The results of this DPIA can also function as guidance for the human operator when deciding on which information may be transferred.

2.1.3 Data processed in ECOSSIAN

Req. number	Description	Importance* (M/O)	Relevant for Level			Comment
			O-SOC	N-SOC	E-SOC	
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.

Req. number	Description	Importance* (M/O)	Relevant for Level			Comment
			O-SOC	N-SOC	E-SOC	
GDPR GReq. 1.2'	If special categories of data, or personal data relating to criminal convictions or offences are processed, the specific restrictions should be complied with	M	x	x	x	Art. 9 and 10 GDPR + additional restrictions for these categories of data

GDPR changes:

Directive 95/46/EC provided special protection for so-called 'sensitive' data. The GDPR keeps this approach, but changes the name from sensitive to 'special categories' of data. Additionally, in Article 10 the processing of personal data relating to criminal convictions and offences is singled out and may only be carried out under the control of an official authority or with authorisation by law and including appropriate safeguards. Registers of criminal convictions may only be kept by official authorities. Aside from personal data relating to criminal convictions, Article 9 states that the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data to uniquely identify a natural person, data concerning health or a natural person's sex life or sexual orientation are prohibited except under certain circumstances, as listed in Article 9 (2). For the processing of genetic data, biometric data or data concerning health the Member States may maintain or introduce further conditions,

including limitations. Therefore, this requirement is in principle still applicable and in case ECOSSIAN systems would process special categories of data, the restrictions regarding the processing of these kind of data need to be identified per Member State and need to be complied with.

ECOSSIAN

As explained earlier, it depends upon the collection system/sensors of the CI operator which kind of data will be collected. Potentially, for example in case of a bank or a hospital, also special categories of data could be collected. In this regard, it is especially important that a DPIA will be done and that the personal data will be filtered by the human operator from the information that is sent out. For other systems, e.g. SCADA systems, it is less likely that special categories of data might be included in the collected information. In general, it is unlikely that these special categories of data can be useful for ECOSSIANs purposes, therefore they should not be sent in the ECOSSIAN system.

2.1.4 Distinction controller – processor

As explained in D7.2, the data controller is the natural or legal person, public authority, agency or any other entity which, alone or jointly with others, determines the purposes and means of the processing of personal data. The GDPR added to this definition that the controller or the specific criteria for its nomination may be provided by law in case the purposes and means are determined by Union or Member State law [art. 4 (7) GDPR]. In general, however, the allocation of the notion of controller is based on its concrete activities in a specific context. It should be noted that the assessment of the status is based upon a factual assessment, depending on who determines the purposes and means, while contractual arrangements can only provide an indication and always need to be checked against the factual circumstances.[62] Therefore, it depends on how the information sharing takes place, and whether or not the information sharing can be considered as one "set of operations" with a joint purpose or jointly defined means, in order to assess the status of the participants.[63]

Whether an entity is a controller or a processor is not based on the nature of the entity which processes data, but on its concrete activities in a specific context. The two basic conditions for a processor are[64]: It must be a separate legal entity, different from the controller, and it must process personal data on behalf of the controller. This processing may be limited to a very specific task or context or may be more general and extended. As soon as an entity does not solely act on behalf of the controller and according to the instruction of the controller, but determines the purposes and means of the personal data, it is considered a controller.[65] Accordingly, the same entity may act at the same time as a controller for certain

[62] Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor", 169, 16.02.2010.

[63] Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor", 169, 16.02.2010.

[64] Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor", 169, 16.02.2010, p. 25.

[65] see e.g. the opinion or the Article 29 Data Protection Working Party 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT), 22.11.2006, where SWIFT was considered a controller as it had taken on specific responsibilities which go beyond the set of instructions and duties incumbent on a processor (p.11.).

processing operations and as a processor for others and the qualification as controller or processor should be assessed with regard to specific sets of data or operations.[66]

Establishing who is controller is important since the controller is the one responsible for the personal data, and to whom therefore most of the legal requirements apply. For information sharing it is important since, in case the recipient is a processor, the processing will be done under the original legal ground for processing. In case the recipient is a separate controller, it needs to be ensured that the processing is still lawful and that a legal ground for processing applies.

For a profound legal evaluation, it is necessary to establish which entities are controllers and which are processors. However, without specific planned operations, this is not possible to assess and therefore only an abstract analysis and recommendations for the implementation can be provided.

ECOSSIAN

As ECOSSIAN can be implemented in different ways, we can only use certain basic assumptions. In case the O-SOC is not a separate legal entity but is part of the CI Provider, there cannot be a separate controller or processor and so the CI Provider will be the controller. In case the O-SOC is a separate legal entity, it depends on the situation whether the O-SOC is a controller or a processor regarding the personal data sent by the CI Provider. In case the O-SOC processes the data on behalf of the CI Provider and does not process the data for own purposes, the O-SOC could be considered a processor. In this case the GDPR provides certain requirements. For example it is required that the controller and the processor conclude a contract or that the processing is governed by a legal act under Union or Member State law. This should be binding on the processor with regard to the controller, it should be in writing (including electronic form) and it needs to stipulate that the processor:[67]

- processes the personal data only on documented instructions from the controller
- ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality
- ensures the security of processing (with reference to the requirements of article 32 GDPR)
- assists where possible the controller by appropriate technical and organisational measures for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights
- assists the controller in ensuring compliance regarding security, notification, requests, DPIA and prior consultation of a supervisory authority
- at the choice of the controller deletes or returns all the personal data to the controller after the end of the provision of services relating to processing and deletes existing copies unless Union or Member State law requires storage of the personal data
- gives the controller all information that is necessary to demonstrate compliance with the obligations and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller, and immediately inform the controller if an instruction infringes the Data Protection Regulation or any other Member State or Union data protection provision

[66] Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor", 169, 16.02.2010, p. 25.
[67] art. 28 GDPR.

- in case of sub-processing (e.g. the O-SOC uses Cloud or other services to process the data), the controller ensure that the same obligations as set out in the contract between the controller and processor shall be imposed on that sub-processor.

In the future, the Commission and supervisory authorities may provide standard contractual clauses addressing these requirements.

In case the O-SOC (and the N-SOC/E-SOC) process the data on its own behalf, the O-SOC (N-SOC/E-SOC) will considered to be a controller. In case two (or more) controllers are involved in the data processing, it could be a case of joint control. The Directive was not explicit on the issue of joint control and the concept of joint controllers was mainly provided by the Article 29 Working Party, however, the GDPR now includes explicitly the concept of joint controllers in article 26 GDPR. The Regulation specifies that where two or more controllers jointly determine the purposes and means of processing, they are joint controllers and they need to determine their respective responsibilities for compliance with the Regulation in a transparent manner. This includes an arrangement of which the essence shall be made available to the data subject, and which may designate a contact point for data subjects. Nonetheless, the data subject may exercise his or her rights in respect of and against each of the controllers (see also section 2.1.8).

It is not necessary that the participation of the parties is equally shared. However, in order for joint control to be established, it is important that the two or more controllers share purposes and means in a common set of operations. The mere fact that different parties cooperate when processing personal data does not mean that they are joint controllers. In case they do not share common purpose or means with regard to the specific processing, then it might only be a transfer of data between separate controllers. [68] Whether several controllers are considered to be joint controllers or separate controllers, and in case they are considered joint controllers, to which extent, depends on the factual circumstances (in how far they determine the essential elements of the means) and might often not be clear-cut.[69]

Therefore, in case the O-SOC is considered to be a controller, O-SOC and CI Provider could either be separate controllers or it could be a case of joint control. Similarly, the N-SOC can be a joint or separate controller. Considering the potential tasks of an E-SOC it is an open question whether it would be necessary for these purposes to share any personal data with the E-SOC.

2.1.5 Legal ground for processing

Req. number	Description	Importance* (M/O)	Relevant for Level			Comment
			O-SOC	N-SOC	E-SOC	
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.

[68] Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor", 169, 16.02.2010, p. 19. The notion of joint control has been taken up and codified in the Draft Data Protection Regulation (art. 24 of the text adopted by Parliament).

[69] 1/2010, p.20.

Req. number	Description	Importance* (M/O)	Relevant for Level			Comment
			O-SOC	N-SOC	E-SOC	
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 processing must be necessary to fulfil the contract.	M	X	X	X	Article 7(b) Directive 95/46/EC. This could happen if an external entity is used to process personal data.
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

GDPR changes

The data controller is required to have a legal ground in order to process the personal data. The original requirements 1.4 till 1.9 refer to the different legal grounds which could be possibly invoked in order to legitimize the processing of personal data. In Directive 95/46/EC these were listed in Article 7, in the GDPR the grounds have only slightly changed and are listed in Article 6.

The only changes as compared to Directive 95/46/EC are: 1) Consent: in the Regulation it is not specified that the consent must be unambiguous, since this is anyway a requirement for valid consent as can be seen in its definition in Article 4 (11) GDPR. Instead, the Regulation

stipulates that the consent must have been given for one or more specified purposes and enumerates the conditions for consent in article 7 GDPR. 2) Vital interest: While the Directive only covered the vital interest of the data subject as a legal ground, the Regulation also considers the vital interest of another natural person as a valid reason to process personal data of the data subject. 3) Public interest and official authority: the Directive, when requiring that the processing must be necessary for a task carried out in the exercise of official authority vested in the controller, also included a third party to whom the data are disclosed and which could carry out the task. The Regulation does not mention a third party. 4) Finally regarding the legitimate interest of the controller, which is especially interesting for ECOSSIAN, the Regulation adds special protection for children and excludes processing carried out by public authorities in the performance of their tasks from the application of this legal ground.

ECOSSIAN

Requirement 1.3 specially emphasises as potential legal grounds for processing in the ECOSSIAN system 1) consent, 2) the existence of a legal obligation (art. 6 (1) (c) GDPR), 3) performance of a task in the public interest or in the exercise of official authority (art. 6 (1) (e) GDPR), and 4) the legitimate interest of the data controller (art. 6 (1) (f) GDPR). The vital interest of the data subject is considered to be potentially a legal ground for processing in case of disaster situations, however, not in the day to day operation of ECOSSIAN.

1) Consent: Article 7 GDPR provides the conditions for valid consent, which are that the controller must be able to demonstrate that the data subject has consented to the processing and that the data subject must have recognised the request for consent and it must have been in an intelligible and easily accessible form, using clear and plain language. Furthermore, the data subject has the right to withdraw his or her consent at any time. For ECOSSIAN consent could possibly play a role regarding the surveillance of the systems, since employees should be aware that potentially their personal data may be within a data set (though of course it should be avoided if possible and the human operator must delete all data that is not required for the purposes of network and information security). In general, however, consent is not advisable as a legal basis for the processing within ECOSSIAN.
2) In case a legal obligation exists, the legal ground for processing can be found in that obligation. However, often the legal obligation will be specified for a specific sector (e.g. based upon article 94 and 95 PSD II Directive[70] it is possible that national legislation exists permitting the processing of personal data for banks for specific security reasons) and often define the exact processing. Therefore, it needs to be assessed how far the processing in the ECOSSIAN system falls within the scope of the legal obligation. It is possible that only certain processing operations may be covered by the legal obligation As an example, mandatory notification of a competent authority using the ECOSSIAN system would be covered by the legal ground that the controller is obliged by a legal obligation to do so. However, further exchange of the information with another entity might not be covered or it needs to be assessed whether another legal obligation exists (e.g. the competent authority might be obliged to share the information with Law enforcement). In general, the legal basis should determine the purpose of the processing, or the purpose must be necessary for the performance of the task. It should be assessed when new legislation is enacted due to the NIS Directive whether it could provide for this.

[70] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.

3) For processing based on a legal obligation or performance of a task in the public interest, the Member States may maintain or introduce more specific provisions by determining specific requirements for the processing. The basis for the processing must be laid down by Union or Member State law to which the controller is subject, the law shall meet an objective of public interest and it must be proportionate to the legitimate aim pursued. The legal basis should determine the purpose of the processing, or the purpose must be necessary for the performance of the task.

4) When it comes to legitimate interest of the controller, the GDPR clarifies that the processing of personal data which is necessary to ensure network and information security by public authorities, by computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), by providers of electronic communications networks and services and by providers of security technologies and services constitutes a legitimate interest of the controller (recital 49 GDPR).[71]

Limitations for using the legitimate interest of the controller as legal ground for processing:

First, the general limitation of art. 6 (1) (f) is that there must not be interests or fundamental rights and freedoms of the data subject that are more important and override the interest of the controller. Second, the processing of the personal data must be strictly necessary and proportionate for the purpose of ensuring network and information security. This means that information cannot be generally collected and shared in order to see whether it could be useful to e.g. detect an attack, but it needs to be assessed beforehand how the security should be ensured and which data exactly is necessary for this aim. Furthermore, the data subject has at any time the right to object to the processing based upon the legitimate interest of the controller. In this case the processing must be stopped, except if the controller demonstrates compelling legitimate grounds for the processing that override the interests, rights and freedoms of the data subject, or is necessary for legal claims.[72] This includes that e.g. a normal employee or customer whose data is shared can object to the processing, however, an attacker generally will not be able to use data protection law to object to the processing of his personal data. Overall, it implies that an assessment must be done for different processing operations, and the result of the assessment can vary, depending on the incident.

With regard to the legitimate interest of the controller the status of the entity needs to be considered. Public authorities in the performance of their task are not allowed to use 6 (1) (f) GDPR as legal basis for their processing, but should in general be able to rely upon the fact that the processing is necessary for either the compliance with a legal obligation (art. 6 1 (c) GDPR) or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (art. 6 1 (e) GDPR). Accordingly, it depends on whether the processing for network and information security lies within the task of the public authority. In case it is within the task, it is not possible to rely on article

[71] Network and information security is considered "*i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), by providers of electronic communications networks and services and by providers of security technologies and services". Recital 49 GDPR.*

[72] art. 21 GDPR.

6 (1) (f) GDPR. In case the network and information security measure is not within the scope of the task of the public authority, it might be possible for the public authority to rely upon the legal interest of the controller. The type of network and information system security measure and the reason for enacting it can provide clues in this regard.

The operator, who will generally be the controller[73] in case of the collection of NIS information of its own system, should normally be able to use the legitimate interest of the controller as a legal ground if the collection of data is proportionate to the goal.

In case the personal data is transferred and for example the N-SOC or E-SOC uses another legal ground for processing, it needs to be assessed whether this is compatible. Art. 6 (4) GDPR provides that where the processing is for another purpose than for which the personal data have been collected (and it is not based on the data subject's consent or a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society), the controller shall make an assessment to ascertain whether processing for another purpose is compatible with the purpose for which the personal data were initially collected. This assessment should take into account:

a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing

b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller

c) the nature of the personal data

d) the possible consequences of the intended further processing for data subjects

e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

Therefore, it needs to be assessed whether the purpose when the data is shared is still compatible with the original purpose when the data has been collected. Most likely, the CI operator as controller will rely on article 6 (1) (f) GDPR, the legitimate interest being the processing for network and information security of its company. In case the N-SOC and, if existing, the E-SOC would process the data, they might, in case they are public authorities, not be able to rely on article 6 (1) (f) GDPR. However, normally their function and goal of processing should be specified in legislation and they will therefore be able to rely upon 6 (1) (e) GDPR. As is obvious throughout the whole analysis, it needs to be ensured that only the data that is indeed necessary for network and information security is shared.

2.1.6 Data quality

Req. number	Description	Importance* (M/O)	Relevant for Level			Comment
			O-SOC	N-SOC	E-SOC	
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

[73] The one who determines the purposes and means of the processing of personal data (Art. 4 (7) GDPR) and who is responsible to comply with the data protection obligations.

Req. number	Description	Importance* (M/O)	Relevant for Level			Comment
			O-SOC	N-SOC	E-SOC	
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 take every reasonable step. As such the accuracy of personal data stored should be constantly assessed an inaccurate data should be deleted.	M	X	X	X	Article 6(d) Directive 95/46/EC
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

GDPR changes

Req. number	Description	Importance* (M/O)	Relevant for Level			Comment
			O-SOC	N-SOC	E-SOC	
GDPR GReq. 1.10'	The controller must be able to demonstrate compliance with the requirements 1.11 – 1.15 and 1.18.	M				Art. 5 (2) GDPR

Req. number	Description	Importance* (M/O)	Relevant for Level			Comment
			O-SOC	N-SOC	E-SOC	
GDPR G.Req. 1.11'	All processing operations involving personal data in ECOSSIAN must be completed fairly, lawfully and in a transparent manner, and cannot contravene the protections afforded under the Data Protection Framework.					Art. 5 (a) GDPR

Directive 95/46/EC identified in Article 6 five principles. The GDPR extends and clarifies this list in Article 5 GDPR. The main part, as seen below, is still comparable with the Data Protection Directive and therefore does not need to be amended extensively. Only the principles 'integrity and confidentiality' (art. 5 (f) GDPR) and 'accountability' (art. 5 (2) GDPR) need an adjustment. However, the requirement of integrity and confidentiality is already covered in Requirement 1.18, therefore only the requirement that the controller will need to

be able to demonstrate the compliance with the principles is added to the list of requirements.

Requirement 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' equates with Article 5 (a) which requires lawfulness, fairness and transparency. The addition of transparency in the principle is new, however, it had already been considered in general as important in the Data Protection Directive and is now mainly codified in this principle.

Requirement 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.': Article 6 (b) Directive 95/46/EC and Article 5 (b) GDPR stayed in principle the same, therefore no changes are required for this Requirement.

Requirement 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.' The only change between the data minimisation Article 6 (c) Directive 95/46/EC, and the new Article 5 (c) GDPR is that the previous 'not excessive' has been changed into 'what is necessary'. This wording could possibly be considered slightly more strict, but will have no influence on the requirement 1.13.

Requirement 1.14 'In order to ensure that the personal data is accurate and up to date the responsible data controller MUST take every reasonable step. As such the accuracy of personal data stored should be constantly assessed and inaccurate data should be deleted.' The only difference in the accuracy principle as established in the Directive and the Regulation (Article 6 (d) Directive 95/46/EC and Article 5 (d) GDPR) is the added clarification that the rectification of inaccurate data must happen without delay. Therefore, no change in the requirement is needed.

Requirement 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.' establishes the storage limitation principle as codified in Article 6 (e) Directive 95/46/EC and Article 5 (e) GDPR. Both provisions stayed in essence the same, and therefore no adjustment is needed.

ECOSSIAN

As the system allows lawful and fair processing and does not contravene the protections of the Data Protection Framework, GReq 1.11 should in principle be fulfilled. However, in a final implementation it still needs to be ensured by the data controllers that the system is not misused in any way and that it is transparent. Also ensuring that the personal data must only be processed for specified and legitimate purposes and not further processed in a way incompatible with these processes is upon the controller, in this case especially the CI provider, which is the first one in line that decides which personal data will be processed. Requirement 1.13 relates to the previous requirement. This includes that for example when the ECOSSIAN system is implemented with the sole purpose to protect critical infrastructure by exchanging information on network and information system attacks, it cannot be used to exchange data by banks regarding fraudulent bank clients. As explained earlier, the legal ground needs to be determined, relating to the purposes of the processing. As ECOSSIAN in principle allows for the data to be updated and to be deleted, GReq 1.14 and GReq 1.15 could be considered as generally fulfilled, however, the practical implementation must be ensured. This could further be improved by ensuring the tagging of personal data and secure storage with specified (possibly agreed with a DPA) deletion times Finally, the controllers (depending on the implementation, this can include the CI operator, O-SOC, N-SOC or even

E-SOC) need to be able to demonstrate the compliance with these requirements, by being able to provide documents, possibly certifications, etc. proving compliance.

2.1.7 Automated individual decisions

Req. number	Description	Importance* (M/O)	Relevant for Level			Comment
			O-SOC	N-SOC	E-SOC	
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

GDPR changes:

Req. number	Description	Importance* (M/O)	Relevant for Level			Comment
			O-SOC	N-SOC	E-SOC	
GDPR GReq. 1.16'	ECOSSIAN should not make automated individual decisions regarding the data subject, unless authorised by law or provided the data subject has given explicit consent					

Under the Data protection Directive it was forbidden to make a natural person subject to decisions based solely on automated processing which would produce legal effects concerning the data subject, except if it was necessary for a contract or authorized by a law, and provided suitable safeguards are in place. The GDPR adds to these exceptions also the possibility that the data subject explicitly consents with the automatic decision making. The GDPR further adds 'profiling' as a specific form of automated processing which is done to evaluate certain personal aspects relating to a natural person [art. 4 (4)]. However, as also pressed in the recitals, data subjects should be informed on the existence of profiling and the consequences of the profiling [Rec. 24, 63, 71, art. 13, 2 (f)]. Furthermore, in order to ensure fair and transparent processing, the *"controller should use appropriate mathematical or statistical procedures for the profiling, implement technical and organisational measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimised, secure personal data in a manner that takes account of the potential risks involved for the interests and rights of the data subject and that prevents, inter alia, discriminatory effects on natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation, or that result in measures having such an effect. Automated decision-making and profiling based on special categories of personal data should be allowed only under specific conditions."*

ECOSSIAN

As ECOSSIAN currently does not include profiling of people or automatic decision making functionalities and there are no indications to assume that they could be included this requirement is fulfilled. In case of a future implementation of ECOSSIAN the profiling of people or automatic decision making regarding them would be included, the fulfilment of this

requirement would need to be reassessed and the requirements provided in the GDPR need to be taken into account.

2.1.8 Data subject rights

Req. number	Description	Importance* (M/O)	Relevant for Level			Comment
			O-SOC	N-SOC	E-SOC	
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

GDPR changes:

Since requirement 1.17 is written in a general manner, requiring that the data subject's rights are ensured without specifying these rights, the requirement itself does not need to be amended. However, it needs to be noted that Directive 95/46/EC specified the data subject's rights as the right to object, the right to access to the data and the right to be informed. The Regulation extends this, by specifying additionally explicitly the right to rectification, the right to erasure, the right to restriction of processing and the notification obligation of the controller regarding these rights, while the Directive only generally referred to these rights under the right to access to the data. Additionally the Regulation includes now the right to data portability. These rights of the data subject must be taken into account when assessing this requirement.

However, these data subject's rights may be restricted by national law, as specified in article 23 GDPR, by Union or Member State Law in order to safeguard amongst other reasons, the national security, defence, public security and prevention, investigation, detection or prosecution of criminal offences. These legislative measures need to comply with certain requirements and must contain specific relevant provisions, as specified in Article 23 GDPR.

Furthermore, in case the controller is demonstrably not in a position to identify the data subject, the articles 15 to 20 (specifying the right of access, the right to rectification, right to erasure, right to restriction of processing, a notification obligation regarding these three rights, and the right to data portability) are not applicable except when the data subject provides additional information.

The right to object, which was already provided in the Directive 95/46/EC exists also in the GDPR. As already mentioned in the section regarding legal grounds, in case data processing is based upon performance of a task in the public interest or the legitimate interest of a controller, the data subject has the right to object. However, the controller can further process the data in case he can demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject, or for the exercise or defence of legal claims.

ECOSSIAN

This requirement relates to the identification of controllers and processors, as the controller is responsible for accommodating the data subject requests, and should provide, especially in

case of joint control, a transparent way to accommodate these. As it is not clear who will be (joint) controllers and processors in an ECOSSIAN system, it is not possible to assess in how far this requirement will be fulfilled. For an implementation of ECOSSIAN it will be important that especially the CI operator when collecting personal data informs the data subject and provides the possibility to exercise the data subjects rights. However, it is possible that in many cases in the ECOSSIAN system the controller will in fact not be able to identify the data subject, which implies that the exception provided by article 11 GDPR can be applicable. Furthermore, art. 14 GDPR requires to inform the data subject in case the personal data have not been obtained from the data subject. In case it is possible for the controller to identify the data subject this should be adhered to (e.g. informing employees), however, in case e.g. an IP address of an adversary is shared an exception ground such as art. 14 (5) (b) GDPR could be invoked, as the provision of such information proves impossible or would involve a disproportionate effort or would render impossible or seriously impair the achievement of the objectives of the processing. However, in these cases the controller must take appropriate measures to protect the data subject's rights and freedoms and legitimate interests. Regarding safeguards, the article refers in the case of processing for public interest archiving and other specified purposes to technical and organisational measures, including pseudonymisation. As the anonymization tool will pseudonymise the IP addresses, this can be considered as a safeguard.

2.1.9 Data security

Req. number	Description	Importance* (M/O)	Relevant for Level			Comment
			O-SOC	N-SOC	E-SOC	
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

GDPR changes:

Requirement 1.18 is general enough that the GDPR does not necessitate any changes in the wording of the requirement. However, the GDPR specially stresses the fact that appropriate technical and organisational measures must be taken, which should meet in particular the principles of data protection by design and data protection by default [recital 78, article 25 GDPR] and specifies certain measures, which should be taken into account when assessing this requirement.

Measures mentioned in the GDPR are for example data minimisation, pseudonymisation of personal data as soon as possible [recital 78, art. 32], encryption [recital 83, art. 32], the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services [art. 32 (1) (b)], the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident [art. 32 (1) (c)] and a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measure for ensuring the security of the processing [art. 32 (1) (d)].

This also needs to be ensured if a processor (as defined in 2.1.4) is involved in the processing of the personal data, where article 28 3 (b) and (c) require that the contract with the processor in particular stipulates that the authorised person have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and take all measures to ensure appropriate security of processing.

The GDPR, however, softens the requirement by considering the appropriate level of security taking into account not only the state of the art but also the costs of implementation in relation to the risks and the nature of the personal data to be protected (recital 83).

ECOSSIAN

ECOSSIAN employs several technical measures, described below. Regarding the recommended implementation of the data minimisation principle, as can also be seen in the section of privacy by design, ECOSSIAN includes a human operator in the system, which can assess and delete personal data before it is shared. Furthermore, the secure gateway includes a special anonymization tool, which hashes and therefore pseudonymizes the IP address and the 'country' field (relating to the entity concerned by the incident) and possibly other fields. Furthermore the data shared between the different entities can be sent encrypted using the ABE module and the data storage is also encrypted.

Access is controlled through technical measures within the secure gateway. This aims to ensure that the person accessing the information has a right to know (clearance) and need to know, including attribute-based encryption. Examples are the access to N-SOC report store which only allows SOCs with attributes matching the access policy to decrypt the data (see D3.2, p.26) and the research on searchable symmetric encryption (D3.2, p.27).

However, policies for clearance and need to know must be defined structurally by organizations or nationally. It is also noteworthy that the classification of data within the clearance system seeks to protect national security interests, not personal data. Nevertheless, it is possible to adjust this in order to align with the different interests or requirements. However, the protection of the data integrity is considered fulfilled (see D5.6 REQ-2.4.4.). Requirements regarding organizational safeguards are not possible to be assessed on the ECOSSIAN technical project level, as they will depend on the final implementation.

2.1.10 Privacy and data protection by design in the GDPR

D7.2 gave a general overview on the privacy by design concept, pointed out several general objectives and showed the current status of the General Data Protection Regulation, which was still a draft at that time.

The final GDPR specifically includes data protection by design and by default in article 25 as one of the controller's obligations. The controller should implement appropriate technical and organizational measures to implement data-protection principles in an effective manner and to integrate the necessary safeguards in the processing. This should happen both at the time of determination of the means for processing and at the time of the processing itself, and the controller should take into account the state of the art, the cost of implementation and the nature, scope, context and purpose of processing, as well as the risks for rights and freedoms of natural persons posed by the processing. Article 25 mentions pseudonymisation as an example of appropriate measures and points out data minimization as one of the data protection principles which should be implemented.

ECOSSIAN

For information relating to data security measures please see the previous section 2.1.9. An important function regarding data minimisation will be set for the human operator. The human operator should receive all possible support when deciding whether certain (personal) data is necessary for the ECOSSIAN operation. Therefore before the processing in the ECOSSIAN system starts a DPIA should be done, assessing already possible types of data that can be involved and introducing guidelines on whether or not they may be shared.

In the ECOSSIAN system, files/logs containing personal data should generally be indicated as such and securely stored. It is difficult to assess how long data should be retained. According to the developers' information, information about incidents are usually kept for a couple of years. However, for information about potential attacks, all the data is kept for extended retention periods to be able to make a possible identification of the attack in the future. Therefore it is important that national laws and data protection authorities are consulted under such circumstances. Technical solutions such as the tagging of personal data files can also provide support to human operators in understanding how long personal data has been stored and how long it ought to be stored, and a separate storage including common deletion timeframes for personal data can ensure that certain storage timeframes, agreed with the data protection authority, are abided.

2.2 Security and critical infrastructure protection requirements

The requirements imposed by the Critical Infrastructure Directive[74] and the Directive on attacks against information systems[75] are targeted towards the EU Member States and thus should guide implementation at the national level.. The responsibility for protecting European Critical Infrastructures (ECI) lies with the EU Member States and the owners or operators.[76] However, a number of activities of distinguishing guidelines for harmonization of CIP and Cyber security measures and for providing common support and coordination from the EU level is on-going.

2.2.1 Security requirements

Current requirements

Req. number	Description	Importance* (M/O)	Relevant for Level			Comment
			O-SOC	N-SOC	E-SOC	
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[77]	National requirements on the requirements in relation to security breach notification must be consulted.	M	X	X	X	

[74] 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.
[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.
[76] Recital 6 Directive 2008/114/EC.
[77] For more detailed information about the national law, see D7.1.

As the ECOSSIAN solution is a modular system that can be implemented in different ways, it should be possible to integrate it with the already existing or planned Operator Security Plan. Similarly it is in principle possible to adjust it to nationally varying obligations. More information regarding notification obligations will be available in D7.7.

The NIS Directive

The new NIS Directive[78] aims at EU wide improvement of cybersecurity, with a focus on essential services and specific digital services. As a directive, Member States will have 21 months (until 9.5.2018) to transpose the Directive into their national legislative framework. The NIS Directive aims to achieve a high common level of security of network and information systems within the European and in order to achieve this specifies certain obligations for Member States. Member States must adopt a national strategy on the security of network and information systems, designate one or more national competent authorities, CSIRTs and a national single point of contact.

The NIS Directive not only introduces new entities in order to increase the national level of network and information security, but also includes some approaches to increase and improve information sharing. The Cooperation Group and the CSIRTs network are two groups established by the NIS Directive, which should increase exchange of information. The Cooperation Group is composed of representatives of the Member States, the Commission and ENISA and has a more strategic role, focusing on exchanging information regarding best practice e.g. on the exchange of information related to incident notification. On the other hand, the CSIRT network consists of representatives of the Member States' CSIRTs and CSIRT-EU. The aim of the network is to exchange information on CSIRTs' services, operations and cooperation capabilities, exchange and discuss non-commercially sensitive information (at the request of a representative of a CSIRT), exchange and make available on a voluntary basis non-confidential information concerning individual incidents. As becomes visible from the restrictions, the sharing is purely voluntary and it is provided that Member State's CSIRTs may refuse to contribute to discussions if there is a risk of prejudice to the investigation of an incident, and the sharing only involves non-confidential information and non-commercially sensitive information.

The main goal of the NIS Directive is to increase the security of network and information systems of 'operators of essential services'. While the proposal had a broader scope, including for example also public authorities, in the final directive 'operators of essential services' are public or private entities in the sectors energy, transport, banking, financial market infrastructure, health sector, drinking water supply and distribution and digital infrastructure which fulfil three criteria: 1) they provide a service that is essential for the maintenance of critical societal and/or economic activities, 2) the provision of their services depends on network and information systems, and 3) an incident would have a significant disruptive effect on the provision of that service.

The obligation to identify operators of essential services in their territory is upon the Member States, and what constitutes a 'significant disruptive effect' will be determined on a national level. However, the Member States are not completely free in their definition, as they should take into account the number of users relying on the service, the dependency of other essential services on the service, the possible impact of incidents in degree and duration on economic and societal activities or public safety. Furthermore, they should take into account the market share of the entity, the area that could be affected by an incident and the importance of the entity for maintaining a sufficient level of the essential service, taking into account the availability of alternative means for the provision of that service. In many

[78] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016.

countries it is likely that there will be an overlap between identified operators of essential services and nationally defined critical infrastructure providers. This is similar to the discussions regarding European CI as defined by Council Directive 2008/114/EC and national CI, whereby Member States generally identified European CI from their list of national CI. However, the designation of an European CI is reached via bilateral or multilateral discussions, whereby the Commission concludes that "*less than 20 European critical infrastructures have been designated and consequently very few new Operator Security Plans have been produced. Some clear critical infrastructures of European dimension, such as main energy transmission networks, are not included. Despite having helped foster European cooperation in the CIP process, the Directive has mainly encouraged bilateral engagement of Member States instead of a real European forum for cooperation*."[79] Differently from Council Directive 2008/114/EC, according to the NIS Directive the Member State can directly identify operators of essential services and send a list of them to the Commission, which aims to create better cooperation via the network established by the NIS Directive.

The NIS Directive specifies some obligations for identified operators of essential services: they must take appropriate and proportionate technical and organizational measures for risk management and to prevent and minimize the impact of incidents. Similar obligations are introduced for digital service providers (providers of online marketplaces, online search engines and cloud computing services) to ensure the security of their network and information systems.

Finally, the NIS Directive specifies notification obligations for operators of essential services and for digital service providers. In case an incident has a significant/substantial impact on their service, they need to notify it without undue delay to the competent authority appointed by the Member State or to the CSIRT. As the scope of the NIS Directive would in principle also cover entities already falling under notification obligations, the NIS Directive explicitly excludes service providers to whom already the notification provisions of the Framework Directive and the eIDAS Regulation apply. The Directive also provides an exception for operators of essential services or digital service provides in case a sector specific Union legal act (such as PSD II) already establishes obligations to notify that are at least equivalent to the NIS Directive [art. 1 (7)].

The NIS Directive furthermore includes exceptions regarding confidential information in art. 1 (5) and (6) Directive 2016/1148/EU, providing that information which is confidential based on Union or national rules, such as rules on business confidentiality shall only be exchanged with the Commission and other relevant authorities if the exchange is necessary for the application of the Directive and shall be confidential, protect the interest of the operators of essential services and be limited to what is relevant and proportionate to the purpose of the exchange. The Directive does not provide for the disclosure of information that the Member States consider contrary to the essential interests of national security.

How does ECOSSIAN align with the NIS Directive?

The NIS Directive stipulates certain requirements and aims, which ECOSSIAN can help to address.

For example the NIS Directive requires for operators of essential services to take appropriate and proportionate technical and organisational measures to manage the risks posed to the

[79] Commission Staff Working Document on a new approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures more secure, Brussels, 28.8.2013 SWD(2013) 318 final, p.4.

security of network and information systems which they use in their operations, and to prevent and minimise the impact of incidents. ECOSSIAN can help in this regard since the project developed technologies (the sensors) and provides the possibility via information sharing to improve the management of risks and to prevent incidents. Furthermore, ECOSSIAN provides a possibility to easily and in a structured manner fulfil the requirement to notify the competent authority or CSIRT in case of an incident having a significant impact on the continuity of the essential services they provide.

A difference between the approach of the NIS Directive and the proposed ECOSSIAN approach is that according to the NIS the countries can implement several competent authorities/CSIRTS (but only one single point of contact) while the ECOSSIAN approach envisages only one N-SOC[80]. In some countries there will most likely be only one competent authority/single point of contact in place, in which case the ECOSSIAN approach fits perfectly. In case several competent authorities are in place or responsible for the different sectors (see D7.7 for an overview on legislation regarding notification), the proposed ECOSSIAN system would need to be adjusted. However, technically this is feasible as the technology developed in ECOSSIAN is modular and the different parts of it can be implemented in different ways, if necessary it is also possible to implement only some parts, e.g. the secure gateway, for certain actions, e.g. secure notification.

The different levels of ECOSSIAN can address the NIS Directive in different ways:

O-SOC:

The O-SOC includes Threat Detection Modules (ICS Monitor, BPIDS, BroLHG, BroProfinet, AECID, Honeypot) focusing ICS (e.g. Modbus, IEC60870, Profinet, etc.) which can detect Incidents & Monitor operations (appropriate and proportional technical measures). Furthermore, it includes the Secure Data Storage which can provide forensic and proof of compliance, and Cymerius and the Secure Gateway, which provide analysis, reporting, Secure Information Sharing and Notification to the Competent Authorities but also national/sectorial CSIRT's (N/S-SOCs) and other Member State Operators or CSIRTs (O/N/S SOCs).

N/S-SOC:

The N/S-SOC includes the Acquisition Module, Cymerius & Secure Gateway, which provide a single point of contact and the possibility for cross-border cooperation. Furthermore, they provide the possibility to monitor incidents at a National level, including analysis, reporting and Secure Information Sharing with other MS National/Sectorial CSIRT's (N/S-SOCs) and CSIRTs Network (E-SOCs). Here, it would be possible to respond to Incidents, provide alerts and reports for external entities. CAESAIR and the Simple Event Correlator can provide early warning, the Cymerius Portal & Interdependency Model can provide national level Situational Awareness & cross-border cooperation and the Secure Data Storage provides for forensic and proof of compliance.

E-SOC

The ECOSSIAN vision of an E-SOC shows a possible form of operational cooperation in an entity that would be able to aggregate information from MSs and include analysis and Secure Information Sharing with Member States National/Sectorial CSIRT's (N/S-SOCs). It could coordinate pan-European responses to incidents and provide alerts.

Security Methodologies

The developed Security methodologies are another useful result of ECOSSIAN for the NIS Directive requirements. The ECOSSIAN Information Security Management and Risk

[80] one N-SOC per nation is a simplifying assumption within the project; The real operational environmeent will be mor complex

Management frameworks guidelines (see ECOSSIAN D1.6) can help establish standardised practices for incident and risk-handling and also address the requirement for operators of essential services to have appropriate and proportional organizational measures in place.

Chapter 3 Implementation Guidelines Evaluation:

The Guidelines were included in the general requirements table of ECOSSIAN D1.2 in section 4.4. One part of the assessment of these requirements was done in WP5 by functional and non-functional lab trials of integrated ECOSSIAN system. However, not all requirements can be assessed that way, therefore some requirements were considered to be out of the scope of D5.6 and had to be assessed from a broader point of view. This legal assessment is done by evaluating what the aim of the requirement is from a legal perspective, which measures exist in ECOSSIAN that can support this requirement and which functions of ECOSSIAN can possibly be detrimental for the aim of this requirement. The explanation of the different considerations is given in column four.

Req.	Description	D5.6 Assessment	Legal assessment
REQ-4.4.1	Only the minimum amount of personal data must be collected. The highest level of aggregation must be used including the least amount of detail as this will restrict the amount of personal data that remains.	requirement was considered as out of the scope of the assessment for D5.6	In ECOSSIAN the focus is not on personal data, but on data necessary to assess threats, which can include personal data. As it is not automatically assessable whether personal data are involved in an incident report (or other types of data which the CI operator does not want to share (information possibly relevant for competitors etc.), the function of a human operator is introduced which controls manually which data should be sent. Properly executed, this will ensure data minimisation. Support can be provided with a previous DPIA, to assess what kind of data may be involved within this entity, and which data possibly may be sent out, as well as guidelines for the human operator. Finally an automatic anonymization function provides automatic hashing of IP addresses and operator information, therefore minimising the risk.
REQ-4.4.2	Personal data and their interrelationships should be hidden from plain view. 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.	In D5.6 it was considered that the testable parts of this requirement are duplicates. Testing of obfuscation of traffic patterns is infeasible and not a functional requirement.	This requirement can only be introduced partially, which is however still in the meaning of this requirement. A balancing is required, in how far it is necessary to obtain certain personal data and link them to improve network and information system security. Useful in this regard is also the anonymization functionality, even though also e.g. hashed IP addresses are generally still linkable (which in this case is often desirable for the analysis) the security is heightened and a certain obfuscation provided. It should be ensured that the

Req.	Description	D5.6 Assessment	Legal assessment
			ECOSSIAN system is implemented in such a way that not high amounts of personal data are shared which could be used for example for surveillance.
REQ-4.4.3	The processing of the personal data should be in a distributed fashion to prevent the completion of full profiles of individuals. Currently no design patterns for this strategy are known.	Requirement was considered as out of the scope of the assessment for D5.6	See analysis of REQ-4.4.2.
REQ-4.4.4	Authentication protocols with privacy features must be implemented.	p.71: PASS Authentication is performed with the minimal necessary information (e.g: username and role within ECOSSIAN).	As the authentication is not a central part included in the ECOSSIAN project, this requirement cannot be analysed. In principle at the current moment only limited information is provided, however, it will need to be assessed when implementing ECOSSIAN how the authentication and authorization will be implemented, especially considering different national security clearance levels. The ABE can provide useful here, at it can limit the access to certain information. At the moment ECOSSIAN in principle provides for access on an entity level, however, for certain information it will be necessary to ensure only access on personal level (person with required security clearance) and in this case privacy features should be considered. This can only be ensured on an organisational level and is currently out of the scope of ECOSSIAN.
REQ-4.4.5	The security of the personal data must be protected throughout the data lifecycle. Encryption must be employed throughout with the default state of data being unreadable if there is a data leak.	p.47: PASS Data storage in SDS Logging is stored ciphered. Data shared between layers (O/N-SOC) can be sent ciphered using ABE module.	See D5.6 evaluation.
REQ-4.4.6	Personal data must be securely disposed of at the end of its life-cycle or anonymised in compliance with the limited retention and	p.47: FAIL: There is no process (compliant or not with the limited retention and data minimisation	At the moment of the legal evaluation a deletion timeframe of 90 days has been implemented, deleting all data in the SDS older than 90 days.

Req.	Description	D5.6 Assessment	Legal assessment
	data minimisation principles.	principles) for securely discarding or anonymizing data after the end of its life cycle. p.123: An action was identified to address this issue before the final demonstration.	
REQ-4.4.7	All communications must be encrypted.	p.41: PASS: All communication using the secure gateway is encrypted. Communication inside the respective SOCs is excluded from the test.	See D5.6 evaluation
REQ-4.4.8	Systems must 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	p.47: PASS: At the SGW, data transmitted between layers, can be filtered manually by an operator. An automatic anonymization feature is implemented for emails and IP addresses.	See D5.6 evaluation
REQ-4.4.9	Systems should be designed so as to allow access to the transferred personal data only to the extent necessary for the role being performed	requirement was considered as out of the scope of the assessment for D5.6	Considering the inclusion of ABE which allows for limited access based upon set requirements, this requirement can in principle be considered fulfilled. However, the establishment and verification of requirements for receiving access is essentially an organisational one, which needs to be considered in an organisational setup of ECOSSIAN. See also answer REQ 4.4.4..

Table 1: Implementation Guideline Assessment

Chapter 4 Conclusion and recommendations

The ECOSSIAN system generally addresses the legal requirements. Certain requirements cannot be assessed on a high-level but need to be assessed when the system is implemented.

As a broad conclusion, considering the steps provided by a DPIA according to the GDPR:

1) A systematic description of the envisaged processing operations and the purposes of the processing, and in case the legitimate interest of the controller is considered the legal ground for processing, it also includes the legitimate interest;

ECOSSIAN envisages a three tier structure. The O-SOC monitors the networks and systems of the organization for intrusions and additionally provides the functionality of sharing incidents with the corresponding N-SOC and receiving warning.[81] The mission of the N-SOC is to enable trusted information exchange between the different SOC levels and to aggregate information from different O-SOCs and it is supposed to be a coordinating SOC[82]. To help operators across different countries to defend against a coordinated, large-scale, transnational attack on the infrastructure (e.g. the power grid), the E-SOC is introduced with the main purpose of delivering situational awareness on a European level and to monitor CIs and their interdependencies, and to coordinate between national SOCs.[83]

Most of the information containing personal data will be processed within the organizations responding to threats and incidents (O-SOC level). O-SOCs may act as responders for multiple organizations. The O-SOCs will process data relating to devices, processes, and users. The users will most likely consist of employees or customers of a service. Information from attackers will also be processed if available. In certain cases, O-SOCs might have to deal with attacks where third party personal data is compromised both by the attacker and the responders, such as attacks launched via botnets.

So-called “indicators of compromise” vary between sectors. However, ECOSSIAN focuses especially on the ability to monitor Industrial Control Systems (ICS)[84] and relies specifically on systems such as Honeypot and BPIDS, which capture rogue traffic, MAC addresses and IP-addresses in particular. These can in general be considered personal data as normally legal means exist to access the identifying information at the ISP. It is difficult to assess in how far further personal data would be shared between O-SOC, N-SOC and possibly, E-SOC.

Especially on CI-operator level usually the controller will rely on art. 6 (1) (f) GDPR. The legitimate interest of the controller in this regard would normally be the processing for network and information security of its company. It will depend on the amount and type of personal data shared whether this legitimate interest can also cover the sharing of the information. In general it is advised that the N-SOC and E-SOC will be operating based on specific laws clearly establishing the purpose of the personal data processing.

2) An assessment of the necessity and proportionality of the processing operations in relation to the purposes;

[81] D2.2., p. 42.
[82] D2.2., p.42.
[83] D2.2, p.42.
[84] D2.2., p.42.

The purposes of the ECOSSIAN processing operations are the protection of network and information structures. In this regard it should normally not be necessary to process or exchange a lot of personal data. The main type of personal data involved will be IP addresses. As long as it is ensured that only the amount of personal data is processed which is strictly necessary to ensure the purpose, this should be acceptable. However, measures such as identified below should be implemented, and the controller at all times need to ensure that the system is not used to exchange more data than is strictly necessary (e.g. IP addresses of employees or website visitors, which do not relate to any threat assessment).

3) An assessment of the risks to the rights and freedoms of data subjects

As long as only a limited and strictly necessary amount of personal data which is related to the identification of network and security threats (generally IP addresses) is exchanged, the risks to the rights and freedoms of data subjects should be minimal. In case ECOSSIAN would be misused, in order to exchange bigger amounts of personal data, or the sensors would be used to surveil data subjects, this would be different. However, the first risk can be reduced with the human operator, contractual measures and possible audits, while the second risk can be considered rather unlikely since there exists better technologies for these adverse aims. Another potential risk is the risk of data breach, which needs to be remedied with appropriate security measures.

4) The measures envisaged to address the risks (e.g. safeguards and security measures).

ECOSSIAN furthermore includes certain technologies to reduce potential risks. A human operator is included in order to ensure that only necessary data is transferred. This provides an additional safeguard for companies that data is not transferred without their knowledge. Furthermore, a secure gateway has been developed, which ensures secure communication between the different SOCs and includes the possibility to send the information only to specific recipients with e.g. a certain profile/security clearance. Thereby a certain access restriction is ensured. Another measure is encryption. All communication using the secure gateway is encrypted and the ECOSSIAN system will be deployed using file system encryption and/or disk encryption. The data in the SDS will be deleted after 90 days. Further improvement could be to implement different data storages with different deletion times, ensuring that personal data will be deleted after a certain timeframe, possibly agreed upon with the national DPA. Different data storages could also provide useful as different security levels could be applied. The access to the data needs to be restricted on an technical but mainly organisational level, with strict requirements regarding security clearance. However, this is out of the scope of ECOSSIAN. For an implementation of ECOSSIAN it is advisable that every CI operator will conduct a DPIA to assess which personal data is processed in the system (generally recommended) and which might possibly be transferred, providing guidelines for the human operator. It will need to be assessed which entities are controllers and processors and contracts need to be established. Finally, for the implementation of N-SOC and E-SOC it is advisable to establish N-SOC and E-SOC with the necessary task description and competences to process the data. Finally, the ECOSSIAN technologies can prove to be useful in the scope of the NIS Directive.

Chapter 5 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
CIWIN	Critical Infrastructure Warning Information Network
CJEU	Court of Justice of the European Union
DAE	Digital Agenda For Europe
DPA	Data Protection Act/Authority
DPIA	Data Protection Impact Assessment
ECI	European Critical Infrastructure
ECHR	European Convention of Human Rights
EPCIP	European Programme for Critical Infrastructure Protection
ENISA	European Network and Information Security Agency
GDPR	General Data Protection Regulation
IMM	Incident Management Module
IP	Internet Protocol
ISP	Internet Service Provider
MAC	Media Access Control
NIS	Network Information Security
RS	Reporting System
TDM	Threat Detection Module
TMM	Threat Mitigation Module
VM	Visualisation Module

Chapter 6 Bibliography

Legislation

Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC.

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.

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016

Case law

CJEU Judgement Case C-582/14 19 October 2016 (Breyer).

Doctrine

BIEKER F. et al., "A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation," in Privacy Technologies and Policy, vol. 9857, Lecture Notes in Computer Science (Cham: Springer International Publishing, 2016), 24, http://link.springer.com/10.1007/978-3-319-44760-5.

BIEKER F., HANSEN M., and FRIEDEWALD M., "Die Grundrechtskonforme Ausgestaltung Der Datenschutz-Folgeabschätzung Nach Der Neuen Europäischen Datenschutz-Grundverordnung," Zeitschrift für Datenschutz-, Informations- und Kommunikationsrecht, no. 4 (2016): 193.

BIEKER F., HANSEN M., and FRIEDEWALD M., "Die Grundrechtskonforme Ausgestaltung Der Datenschutz-Folgeabschätzung Nach Der Neuen Europäischen Datenschutz-Grundverordnung," 192.

HANSEN M., "Datenschutz-Folgenabschätzung–gerüstet Für Datenschutzvorsorge?," 590.

Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, "Das Standard-Datenschutzmodell - Konzept Zur Datenschutzberatung Und -Prüfung Auf Der Basis Einheitlicher Gewährleistungsziele, V.0.9," 2015.

HANSEN M., JENSEN M., and ROST M., "Protection Goals for Privacy Engineering" (2015 IEEE CS Security and Privacy Workshops, IEEE, 2015), 164.

HANSEN M., "Datenschutz-Folgenabschätzung–gerüstet Für Datenschutzvorsorge?," Datenschutz Und Datensicherheit-DuD 40, no. 9 (2016): 587–591.

Reports

R. Bourgue, J. Budd, H. Homola, M. Wladenko, D. Kulawik, Detect, SHARE, Protect – Solutions for Improving Threat Data Exchange among CERTs, October 2013.

Article 29 Working Party, Opinion 4/2007 on the concept of personal data, WP 136, 20 June 2007.; WP 37: Privacy on the Internet - An integrated EU Approach to On-line Data Protection-adopted on 21.11.2000

Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of “controller” and “processor”, 169, 16.02.2010.

CNIL (Commission Nationale de l’Informatique et des Libertés, “Privacy Impact Assessment: Methodology (How to Carry out a PIA),” 16.

Commission Staff Working Document on a new approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures more secure, Brussels, 28.8.2013 SWD(2013) 318 final.

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

D1.6: Gavin Davey, Alessandra Spangaro, Ilkka Karanta, Damian Clifford, Jessica Schroers, D1.6 Security Methodologies, ECOSSIAN Deliverable 1.6, 2015.

D2.2: Daniel Meister, Nils Motsch, Architectural Design of SOCs, ECOSSIAN Deliverable 2.2, 2017.

D3.2: Giuseppe Settanni, Daniel Meister, Florian Skopik, Roman Fiedler, Yegor Shovgenya, Mark Gall, Gerd Brost, Christophe Ponchel, Damien Conroy, Sami Noponen, Klaus Theuerkauf, Haustein Mirko, Incident Information Sharing, Analysis, Correlation, and Visualization System Concept, ECOSSIAN Deliverable 3.2, 2016.

D4.2: Ilkka Karanta, Gavin Davey, Mark Carolan, Heimo Pentikäinen, Tero Tyrväinen, Mika Rautila, Pia Olli, Mirko Haustein, Peter Klein, Threat mitigation and incident management in CI use cases of ECOSSIAN, ECOSSIAN Deliverable 4.2, 2016.

D5.6: Luis Silva, Konstantin Böttinger, Mark Gall, Gerd Brost, Cédric Bijard, Guillaume de Malet, Christophe Ponchel, Andreia Mordido, Bernardo Pacheco, João Guiomar, João Lima, Nelson Escravana, José Goncalves, Andre Katchic, Berta Santos, Carlos Nunes, Mark Carolan, Pia Olli, Integration test report, ECOSSIAN Deliverable 5.6, 2017.

D7.1: Damian Clifford, Annarita, Ricci, Giusella Dolores, Finocchiaro, Luisa, Proenca, Yung Shin Van Der Sype, Karine e Silva, Analysis of the applicable legal framework, ECOSSIAN Deliverable 7.1, 2014.

D7.2: Damian Clifford, Alessandro Spangaro, Annarita Ricci, Yung Shin Van Der Sype, Legal Requirements, ECOSSIAN Deliverable 7.2, 2015.

D9.3: Anton Vedder, Damian Clifford, and Yung Shin Van Der Sype, 'ECOSSIAN D9.3 Report from Data Protection Coordinator – Version 1', 2015.