D7.3

Information sharing policies in disaster situations - Version 1

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 / D7.3 / 1.0
Work package contributing to the deliverable:	WP 7
Due date:	May 2015 – M12
Actual submission date:	1st June, 2015

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

Security Sensitivity Committee Review performed on:	18th May, 2015
Comments:	N/A

Abstract:	This deliverable focuses on the legal framework related to the sharing of data in disaster situations. It builds upon the work completed in D 7.1 Analysis of the applicable legal framework and D7.2 Legal Requirements and provides a detailed assessment of the applicable requirements to the ECOSSIAN project.
Keywords:	Information sharing, Disaster management, Critical Infrastructure Protection, Security.

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

Editor

Damian Clifford (KUL)

Contributors (ordered according to beneficiary numbers)

Alessandra Spangaro, Giusella Finocchiato (UNIBO)

Valerie Verdoodt (KUL)

Executive Summary

Information sharing in disaster situations is potentially crucial for relief and the prevention of further damage. ECOSSIAN aims to develop prevention and detection tools that facilitate preventive functions like threat monitoring, early indicator and real threat detection, alerting, support of threat mitigation and disaster management in a privacy compliant manner. In order to adequately comprehend the legal implications of sharing information regarding the ECOSSIAN solution one must have a detailed understanding of information sharing in the broader context of disaster management. The purpose of this deliverable is to provide an outline of the requirements and policies associated with information sharing in disaster situations in the context of ECOSSIAN.

Chapter 2 will first examine the current disaster management framework in the context of critical infrastructures ('Disaster management').

Chapter 3 will focus on the legal framework for information sharing ('Legal framework for information sharing').

Chapter 4 will assess the barriers to information sharing (Legal barriers to information sharing). The analysis provided in Chapters 2, 3 and 4 will then be applied in Chapter 5 to the context of ECOSSIAN ('Impact on ECOSSIAN).

Chapter 6 will provide guidance on the implementation of the identified requirements and finally Chapter 7 will conclude the analysis.

Contents

List of Tables

Chapter 1 Introduction

Information sharing in disaster situations is potentially crucial for relief and the prevention of further damage. ECOSSIAN aims to develop prevention and detection tools that facilitate preventive functions like threat monitoring, early indicator and real threat detection, alerting, support of threat mitigation and disaster management in a privacy compliant manner. In order to adequately comprehend the legal implications of sharing information regarding the ECOSSIAN solution one must have a detailed understanding of information sharing in the broader context of disaster management. According to the Parliament's and Council Decision on the Union Civil Protection Mechanisms, a disaster is defined as

> "any situation which has or may have a severe impact on people, the environment, or property, including cultural heritage".[1]

This includes all kinds of natural and man-made disasters, such as environmental disasters or marine pollution, acute health emergencies but also cyber-attacks against critical infrastructures.[2] The purpose of this Deliverable is to assess information sharing in these disaster situations. This Deliverable should be distinguished from D7.2 'Legal requirements' as its purpose is to assess information exchange in a disaster situation. In contrast D7.2 'Legal requirements' focused on the legal implications in relation to threat detection/analysis and the resulting sharing of information within the ECOSSIAN solution being developed with a particular emphasis on the data protection and privacy concerns.

Similar to D7.2 'Legal requirements'[3], this deliverable builds upon the initial analysis completed in D7.1 'Analysis of the applicable legal framework'.[4] Reference will also be made to the specific sub-scenarios and incidents highlighted in D1.5 'Use case scenario report' where relevant in order to stipulate the significance and application of the legal requirements. A draft version of this deliverable will be used as a point of reference in its current draft form. Importantly however, this will not provide a complete summary of the relevant scenarios and use cases as reference can be made to the specific deliverable for such insights. Instead, it will merely highlight the relevant actions from a legal perspective. Reference should also be made to the Data Protection Coordinator Reports. Finally, it should be noted that this Deliverable is the first iteration and as such will be supplemented by the work to be completed in D7.7 'Information sharing policies in disaster situations - Version 2.

The analysis will be divided as follows: Chapter 2 will first examine the current disaster management framework in the context of critical infrastructures ('Disaster management'). Chapter 3 will focus on the legal framework for information sharing ('Legal framework for information sharing'). Chapter 4 will assess the barriers to information sharing (Legal barriers to information sharing). The analysis provided in Chapters 2, 3 and 4 will then be applied in Chapter 5 to the context of ECOSSIAN ('Impact on ECOSSIAN). The application to ECOSSIAN will maintain these distinctions as they highlight the policy basis for action, the

[1] Article 4 (1) Decision No 1313/2013/EU of the European Parliament and of the Council of 17 December 2013 on a Union Civil Protection Mechanism, 20/12/2013, OJ L 347, 924–947.

[2] Ibid. Recital 3.

[3] D. Clifford, A. Spangaro, A. Ricci, and Y.S. Van Der Sype, 'ECOSSIAN D7.2 Legal requirements' (2015).

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

legislation requiring information sharing and finally the legal frameworks imposing restrictions on any such sharing. Chapter 6 will provide guidance on the implementation of the identified requirements and finally Chapter 7 will conclude the analysis.

Chapter 2 Disaster Management

As stated in the introduction this chapter focuses on the disaster management framework in relation to critical infrastructures. The analysis is divided into five sections. Section one focuses on the critical infrastructure framework; section two information sharing platforms in relation to critical infrastructure protection; section three disaster management more generally and the EU civil protection mechanism; section four public-private partnerships; and finally section five national approaches to disaster management.

2.1 Critical Infrastructure Framework

To begin our analysis it is important to first explore the scope of the obligations imposed by Directive 2008/114/EU.[5] Significantly, this Directive focuses on the identification (Article 3) and designation (Article 4) of European Critical Infrastructures.[6]

As noted in Deliverable 7.2[7], according to Directive 2008/114/EC, Member States are required to:

- ensure that ECI's possess and implement an operator security plan;8
- conduct a threat assessment;9
- ensure that a security liaison officer or equivalent is designated for each ECI;10 and
- appoint an ECI protection contact point who shall be responsible for the coordination of ECI protection issues.11

From these requirements it is clear that the operators have obligations in aiding the successful completion of each of the requirements. This will inevitably require some degree of cooperation and information exchange between the operators and the public authorities responsible.

More particularly in relation to information sharing Member States are required to:

---

[5] 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.

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

[7] D. Clifford, A. Spangaro, A. Ricci, and Y.S. Van Der Sype, 'ECOSSIAN D7.2 Legal requirements' (2015).

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

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

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

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

- identify potential ECIs12 and inform the Commission and the owner/operator13 and the Member States (which may be significantly affected by a potential ECI) about its identity and the reasons for designating it as a potential ECI;
- participate in bi/multilateral discussion with other potentially affected Member States when identifying a potential European Critical Infrastructure14; and
- provide a report every two years to the Commission including generic data on a summary basis on the types of risks, threats and vulnerabilities encountered per ECI sector in which there is an identified and designated ECI.15

From these Member State obligations it is clear that a certain degree of cooperation and information sharing is expected between the operators, Member States and the European Commission.

Moreover, it can be understood from a variety of provisions from Directive 2008/114/EU that such activity is encouraged and to a certain degree expected. Indeed recital 14 states that:

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

As further noted in recital 17 "effective protection of ECIs requires communication, coordination and cooperation at national and Community level". In addition to the above Recital 8 specifies that "Given the very significant private sector involvement in overseeing and managing risks, business planning and post disaster recovery, a Community approach needs to encourage full private sector involvement". Thus this recital encourages private sector involvement but does not establish any specific obligation for cooperation and information sharing.

Furthermore, recital 19 states that, "Information sharing regarding ECIs should take place in an environment of trust and security. The sharing of information requires a relationship of trust such that companies and organisations know that their sensitive and confidential data will be sufficiently protected." Similar to recital 8 this provision does not provide any direct requirements but instead encourages the establishment of "an environment of trust and security". This is also reflected in Article 9 which provides that only those with appropriate security clearance should be permitted to handle classified information, that such information submitted to the Member States or the Commission should not be used for a purpose other than the protection of Critical Infrastructures and that this applies to non-written information exchanged during meetings. Finally the obligation to create a Security Liaison Officer (Article 6) and the Commission's commitment to support Member States and critical infrastructure operators through the provision of best practice documentation is indicative of this expectation of cooperation and sharing.

However, it must be understood that within this framework there is no requirement to share threat or attack based information or in the context of this deliverable information in disaster

[12] Article 3 Directive 2008/114/EC

[13] Article 4 Directive 2008/114/EC

[14] Article 4 Directive 2008/114/EC

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

situations. Instead Directive 2008/114/EC focuses on coordination and preventative preparative action thus allowing a large degree of discretion to the Member States on the precise nature of the national critical infrastructure framework. It is clear that this framework does not focus on actual disaster situations. However, before analysing the current EU mechanisms for disaster management the Deliverable will first highlight the role of the relevant information sharing mechanisms in relation to critical infrastructure protection.

2.2 EU CI information sharing platforms

As was observed in Deliverable 7.1 'Applicable legal framework' at an EU level there are currently a variety of information sharing platforms that co-exist involving different purposes, partners and architectures.[16] The Critical Infrastructure Warning Information Network (CIWIN),[17] the Thematic Network on Critical Energy Infrastructure Protection (TNCEIP)[18] and the European Public Private Partnership for Resilience (EP3R)[19] provide voluntary participatory platforms for the sharing of best practices and other relevant information. More particularly, the CIWIN aims at providing a public information and communication system offering a platform through which critical infrastructure protection related information can be shared irrespective of the economic sector of activity.

The key objective of the CIWIN is to enable coordination and co-operation via information sharing on the protection of critical infrastructure at an EU level, ensuring secure and structured exchange of information and allowing its users to learn about best practices in other EU Member States in a fast and efficient way. In contrast the TNCEIP and the EP3R have a more focused objective. The EP3R is managed by ENISA and focuses on encouraging the exchange of information between the public and private sectors. As discussed further below (section 2.4) this is a major obstacle in ensuring the adequate protection of Critical Infrastructures. As noted in D7.1 this initiative has four action lines, (1) Encouraging information sharing and stock-taking of good policy and industrial practices to foster common understanding; (2) Discussing public policy priorities, objectives and measures; (3) Providing baseline requirements for the security and resilience in Europe; and (4) Identifying and promoting the adoption of good baseline practices for security and resilience.[20] In contrast to the two previous mechanisms the TNCEIP is specifically focused on the exchange of information in the EU energy sector and aims at facilitating the exchange

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

[17] Commission Staff Working Document Accompanying document to the Proposal for a Council Decision on creating a Critical Infrastructure Warning Information Network (CIWIN) {COM(2008) 676 final} {SEC(2008) 2702} accessed on 22/01/2015 at: ec.europa.eu/smart-regulation/impact/commission_guidelines/docs/sec_2008_2701_ia_ciwin_en.pdf

[18] Position Paper of the TNCEIP on EU Policy on Critical Energy Infrastructure Protection (November 2012) Accessed on 22/01/2015 at: http://ec.europa.eu/energy/sites/ener/files/documents/20121114_tnceip_eupolicy_position_paper.pdf

[19] ENISA, 'European Public Private Partnership for Resilience (EP3R)' accessed on 03/02/2015 at: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/european-public-private-partnership-for-resilience-ep3r

[20] ENISA, 'European Public Private Partnership for Resilience (EP3R)' accessed on 03/02/2015 at: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/european-public-private-partnership-for-resilience-ep3r

of information and to 'address topics such as 'Threat Assessment', 'Risk Management', 'Cyber Security', and others.'[21]

However, it must be observed that ECOSSIAN distinguishes itself from these models in that the information being shared relates more to threat identification and mitigation rather than best practice guidance. Moreover, the response to disaster situations also does not really fit within their remit.

2.3 EU Civil Protection

Significantly, cyber-attacks on Critical Infrastructures fit within the broader EU Civil Protection mechanism. As such, the role of this mechanism in the sharing of information in the event of a disaster is key. Indeed, the Civil Protection Mechanism is aimed at the coordination of responses following an actual disaster and thus contrast with the Critical Infrastructure orientated measures discussed above which primarily deal with information sharing related to prevention and the distribution of best practice documentation.[22]

Civil protection falls primarily under the responsibility of the Member States.[23] In recent years, the numbers and severity of natural and man-made disasters has increased significantly. The consequences and effects of such disasters are complex, trans-boundary and can be felt for a long period of time.[24] Examples include epidemics, financial crises and floods but also man-made disasters such as cyber-attacks and other technological hazards. Therefore, the European Union has taken initiatives to foster cooperation amongst national civil protection authorities across Europe with regard to disaster management.

The EU Civil Protection Mechanism was established in 2001.[25] The mechanism entails coordinated assistance and information sharing from all participating states, in situations of natural and man-made disasters in Europe and elsewhere.[26] Specifically, the assistance consists of governmental aid in the form of "*in-kind assistance, deployment of specially-equipped teams, or assessment and coordination by experts sent to the field*".[27] As

[21] Position Paper of the TNCEIP on EU Policy on Critical Energy Infrastructure Protection (November 2012) accessed on 22/01/2015 at: http://ec.europa.eu/energy/sites/ener/files/documents/20121114_tnceip_eupolicy_position_paper.pdf

[22] European Commission, 'EU Civil Protection Mechanism' accessed on 05/02/2015 at : http://ec.europa.eu/echo/what/civil-protection/mechanism_en

[23] French Red Cross, 'Analysis of Law in the EU Pertaining to Cross-Border Disaster Relief (EU IDRL Study) - Country Report by the French Red Cross' (August 2010) 18, retrieved from http://www.ifrc.org/PageFiles/93645/country-report-france-082010.pdf.

[24] Decision No 1313/2013/EU of the European Parliament and of the Council of 17 December 2013 on a Union Civil Protection Mechanism, *OJ L* 347, 20 December 2013, 924–947.

[25] Council Decision 2001/792/EC, Euratom of 23 October 2001 establishing a Community mechanism to facilitate reinforced cooperation in civil protection assistance interventions, *OJ L* 297, 15.11.2001, 7.

[26] At the moment, there are 31 participating states, including all 28 EU Member States as well as Iceland, Norway, and the former Yugoslav Republic of Macedonia. See: 'EU Civil Protection Mechanism', accessed on 22/01/2015 at http://ec.europa.eu/echo/what/civil-protection/mechanism_en.

[27] See: 'EU Civil Protection Mechanism', accessed on 22/01/2015 at http://ec.europa.eu/echo/what/civil-protection/mechanism_en.

mentioned, the mechanism covers man-made disasters, including cyber threats and physical attacks. As it is an all-encompassing framework for disaster management it has an impact on critical infrastructure protection. For instance, the mechanism could be triggered by a cyberattack that causes the failure of a Critical Infrastructure.

In 2009, Article 222 of the Treaty on the Functioning of the European Union (the Lisbon Treaty) introduced the Solidarity Clause. This clause explicitly calls upon the EU Member States to act jointly and provide assistance to one another in disaster situations and crises on the European continent.[28] As a result, a wave of new policy initiatives regarding disaster management were set in motion. One of the most important developments was the development of so-called "sense-making tools" which collect, analyse and share information on transboundary threats. Examples include the External Action Service's Situation Room, which is linked to the Intelligence Analysis Centre; DG ECHO's Emergency Response Centre, which aims at providing situational awareness during large-scale disasters; and Argus, a web-based system that facilitates the sharing of disaster information across the different directorates of the Commission.[29]

The EU Civil Protection Mechanism was updated in 2013, by a joint decision of the European Parliament and the Council.[30] According to the Decision, a general framework for information sharing on risks and risk management capabilities needs to be established. This framework should take Article 346 TFEU into account, which guarantees that Member States should not be obliged to share information if this would go against their essential security interests. Within the framework Member States have certain notification obligations. In particular:

> "In the event of a disaster within the Union, or of an imminent disaster, which causes or is capable of causing transboundary effects or affects or is capable of affecting other Member States, the Member State in which the disaster occurs or is likely to occur shall, without delay, notify the potentially affected Member States and, where the effects are potentially significant, the Commission."[31]

The notification, as well as any other information sharing within the Mechanism, will go through the Common Emergency Communication and Information System ("CECIS"). The CECIS facilitates the communication between the Emergency Response Coordination Centre ("ERCC") - which has the 24/7 capacity to monitor and respond to disasters - and the National Authorities, enabling a faster and more effective response. It hosts a database on potentially available assets for assistance, handles requests for assistance, exchanges information and documents the traffic of all messages and actions.[32]

[28] A. Boin, M. Rhinard and M. Ekengren, 'Managing Transboundary Crises: The Emergence of European Union Capacity (2014) Journal of Contingencies and Crisis Management 3.

[29] Ibid.

[30] Decision No 1313/2013/EU of the European Parliament and of the Council of 17 December 2013 on a Union Civil Protection Mechanism Text with EEA relevance, *OJ L 347*, 20 December 2013, 924–947.

[31] Ibid Article 14.

[32] Ibid.

2.4 Public-private partnerships

2.4.1 The privatisation of public assets

It must be understood that a key concern in the protection of critical infrastructures is that many of these public assets are in private ownership. The European Commission has repeatedly stressed the importance of private-public coordination and cooperation and ENISA has undertaken a clear mandate in recommending and facilitating such involvement. However, it is not entirely clear where private sector obligations end and public sector responsibilities begin.[33] This is an important consideration as this privatisation changes the regulatory landscape.[34] Indeed as observed by Lazari, this private ownership has brought a mix of public duties imposed by legislators and private business interests associated with the protection of a business asset.[35] As a result standards for measuring and counteracting threats as a means of managing risk have been developed. De Bruijne and van Eeten have noted that despite the fact that these infrastructures are critical for society has not stopped this institutional restructuring resulting in a situation in which governments are increasingly reliant on private parties.[36]

2.4.2 The difficulties associated with access

2.4.2.1 What complicates the sharing of data by private actors?

A clear difficulty with this situation is that in this institutionally fragmented environment, although all parties may agree that critical infrastructure protection is important, problems arise when it becomes clear that governments expect private sector investment in the security and reliability beyond what it would deem necessary for its business continuity requirements.[37] The issues surrounding public-private partnerships will be discussed in more detail in Deliverable 7.1 'Partnerships: opportunities and constraints', however, it is important to note the significance of this divide in this report given the potential legal significance. Aside from the economic interests associated with critical infrastructure protection the private ownership of critical infrastructures also means that cooperation and information sharing is often built on voluntary action as described above. As observed by Willis *et al.,* this presents certain clear difficulties in relation to the perception that within the private sector there is a concerned about sharing information with the public sector and confidentiality.[38] This concentrates on the risks associated with making vulnerabilities public, issues concerning

[33] A. Fritzan, K. Ljungkvist, A. Boin and M. Rhinard, 'Protecting Europe's Critical Infrastructures: Problems and Prospects' (2007) 15 Journal of Contingencies and Crisis Management 30-41.

[34] A. Fritzan, K. Ljungkvist, A. Boin and M. Rhinard, 'Protecting Europe's Critical Infrastructures: Problems and Prospects' (2007) 15 Journal of Contingencies and Crisis Management 30-41.

[35] A. Lazari, *European Critical Infrastructure Protection*, (2014 Springer) 68.

[36] M. De Bruijne and M. van Eeten, 'Systems that should have failed: Critical Infrastructure Protection in an Institutionally fragmented environment' (2007) 15 Journal of Contingencies and Crisis Management 18-29.

[37] Ibid.

[38] H. Willis, G. Lester and G. Treverton, 'Information sharing for infrastructure risk management: Barriers and solutions (2009) 24 Intelligence and National Security 339-365.

liability and the potential for inadvertently highlighting the need for new regulatory mechanisms.[39]

2.4.2.2 What positive obligations exist for "public authorities" to grant access?

The Member States interpretations and implementations of Freedom of Information legislation vary significantly. This area of law focuses on the public sector bodies' rights and obligations in relation to making "public information" available upon request (but also encouraging proactive release) to the general public in order to support accountability and transparency. This is an issue which remains in the sole competence of the Member States thus facilitating clear disparities.[40]

Indeed this is dominated by the principle of subsidiarity which stipulates that

> "in areas which do not fall within its exclusive competence, the Union shall act only if and in so far as the objectives of the proposed action cannot be sufficiently achieved by the Member States, either at central level or at regional and local level, but can rather, by reason of the scale or effects of the proposed action, be better achieved at Union level."

Accordingly, in general access to public sector information is dictated by national law with no precise framework at an EU level. However, there are two clear exceptions in relation to environmental and spatial data namely:

- Directive 2003/4/EC of the European Parliament and of the Council of 28 January 2003 on public access to environmental information and repealing Council Directive 90/313/EEC L 41/26
- Directive 2007/2/EC of the European Parliament and of the Council of 14 March 2007 establishing an Infrastructure for Spatial Information in the European Community (INSPIRE) L 108/1

However, these legal frameworks relate to the sharing of information in these restricted contexts and therefore have perhaps limited relevance for ECOSSIAN.

2.4.2.2.1 Public Sector Information (PSI) Re-use

Public sector bodies collect vast amounts of data. The potential economic and social benefits of exploiting this data is well established and has been recognised by the European Commission.[41] Increasing computing capacity has opened up new avenues for the re-use and exploitation public sector data sets. The adoption of the PSI Directive (Directive 2003/98/EC)[42] was the culmination of the Commission's efforts in encouraging re-use.

[39] ENISA, 'A flair for information sharing- encouraging information exchange between CERTs' (2011) accessed on 01/03/2015 at: http://www.enisa.europa.eu/activities/cert/support/fight-against-cybercrime/legal-information-sharing

[40] For more see: http://journalism.cmpf.eui.eu/maps/freedom-of-information/

[41] K. Janssen, 'The influence of the PSI directive on open government data: An overview of recent developments' (2011) 28 Government Information Quarterly 446.

[42] Directive 2003/98 of November 17, 2003 on the re-use of public sector information [2003] OJ L345/90.

Fundamentally, the framework is designed to stimulate the European information services market. In 2010, the Commission began a public consultation process measuring the effect of the 2003 Directive.[43] The results indicated that although there had been considerable progress made, certain barriers were still preventing the realisation of the full potential of PSI re-use.[44] As a result the Directive was amended in 2013 by Directive 2013/37/EU and Member States are required to implement the changes by the 18th of July 2015.

PSI re-use has a potentially broad impact, both in terms of the types of data included and the legal areas it touches upon. The 2003 Directive and the 2013 amendment both find their legal bases in art.114 of the Treaty on the Functioning of the European Union (TFEU) (ex art.95 of the EC Treaty)[45], which aims to harmonise rules for the establishment and functioning of the internal market.[46]

The fundamental criticism of the PSI framework relates to the lack of EU competence to require a right of access in the Member States. This reflects the fact that this is an area of joint competence, and is thus dictated by the principle of subsidiarity. EU Member States have guarded their authority over Freedom of Information and access tightly and essentially decide which data sets become public. To exacerbate the shared competence issue under the 2003 process, not only did the Member States decide on the types of information the public had access to, they were also permitted to further decide on the publicly available information which could be re-used. The 2013 amendments have addressed this issue and Public Sector Bodies are now required to allow re-use, for non-commercial purposes, of existing and generally available PSI. However, this discretion presents a challenge to any project relying on the re-use of PSI.

There are two important stipulations on this right to non-commercial re-use which also potentially present a challenge. The first is the interaction between Intellectual property rights and the PSI framework. In the 2003 Directive, recitals 22 and 24 briefly mention the issue of intellectual property rights.[47] From these, it is clear that the intellectual property rights of third parties are not to be affected by the 2003 Directive. These issues and the potential licensing concerns could provide challenges for the project. It should also be noted that there is some disparity vis-à-vis charging. However, the 2013 Amendment does provide some advances towards a more harmonised approach by providing for the implementation of a marginal costs principle.

A second stipulation is that the re-use of PSI cannot breach the data protection legislation. The 2003 Directive only made vague references to data protection, as it did not make re-use obligatory in respect of already publicly accessible information.[48] However, given the 2013

[43] Council of the European Union, Proposal for a Directive of the European Parliament and of the Council amending Directive 2003/98/EC on re-use of public sector information, Interinstitutional File: 2011/0430 (COD).

[44] Ibid.

[45] See preamble to both the old and revised PSI Re-use Directives where this grounds is referred to specifically.

[46] See TFEU Article 114 (1).

[47] Directive 2003/98/EC recitals 22 and 24.

[48] See: C. Dos Santos et al, 'LAPSI Policy Recommendation N. 4: Privacy and Personal Data Protection', LAPSI Working Group 2: Privacy Aspects of PSI, accessed on 21/02/2015 at http://www.ivir.nl/publicaties/download/1098.

amendments, this omission required clarification.[49] As noted by the ENISA report on encouraging information sharing between CERTs:

> "For CERTs, this can be relevant when requesting permission to re-use information which is made available by public sector bodies, or inversely when they themselves are public sector bodies and make their own information available for re-use. In these circumstances, the PSI Directive provides a common framework for the rights of re-users, which could theoretically support the exchange of information. In practice, however, the impact of this framework is likely to be very limited for CERTs, primarily because the information which directly relates to security incidents that fall within their remit is unlikely to be made available for re-use."[50]

This is conceivably also the case in the current context of information sharing in disaster situations as the information needed to be shared and re-used would often be security sensitive.

2.4.2.2.2 Classified information

This security sensitive information is a key concern and national measures relating to the classification of certain types of information as secret and other such categorisations is a key concern for the ECOSSIAN platform. At a national level there is a large degree of disparity between the Member States. For example in Ireland no framework currently exists for the classification of data. However, the Official Secrets Act 1963 does stipulate the definition for an official secret. This contrasts sharply with the situation in many other countries. For example in Germany

> "Section 93-95 of the German Criminal Code is related to the definition of national security secrets. Additionally, the Safety Assessment Act 1994 requires data deemed in need of secrecy to protect the public interest be classified. Paragraph 4 of the act outlines a four-tiered system of classification levels. The levels are assigned according to the level of risk involved in disclosing the classified information."[51]

Similar classification systems are evident in the UK, Italy, Belgium and France.[52] The key issue however relates to the fact that the precise criteria and oversight into such classifications are not always apparent. At an EU level one must consider Decision 2013/488/EU[53] which provide the principles and standards for the protection of EU classified

[49] See: Article 29 Working Party Opinion 06/2013 on open data and public sector information ('PSI') reuse, adopted on June 5, 2013.

[50] ENISA, 'A flair for information sharing- encouraging information exchange between CERTs' (2011) accessed on 01/03/2015 at: http://www.enisa.europa.eu/activities/cert/support/fight-against-cybercrime/legal-information-sharing

[51] http://cybersecurity.bsa.org/assets/PDFs/country_reports/cs_germany.pdf

[52] See: http://cybersecurity.bsa.org/countries.html

[53] Council Decision 2013/488/EU of 23 September 2013 on the security rules for protecting EU classified information.

information including such information classified in accordance with Council Decisions 2001/264/EU[54] and 2011/292/EU.[55]

Decision 2012/488/EU is applicable when the EU Council and the General Secretariat of the Council (GSC) are required to interact with classified information. As per Article 2 the classifications are Très Secret UE/EU Top Secret,[56] Secret UE/EU Secret,[57] Confidentiel UE/EU Confidential,[58] and Restreint UE/EU Restricted.[59] EU Member States are bound to respect minimum security standards in relation to such data as laid down in the Decision.[60] From Article 4 the EU Council and the GSC are required to ensure the adequate classification of any data shared by Member States this is supplemented by Appendix B to the Decision which elaborates a table of compliance with national standards for this purpose.

Also of note is Article 12 which stipulates the conditions in relation to information sharing. This indicates that:

> 1. The Council shall determine the conditions under which it may share EUCI[61] held by it with other Union institutions, bodies, offices or agencies. An appropriate framework may be put in place to that effect, including by entering into inter-institutional agreements or other arrangements where necessary for that purpose.
>
> 2. Any such framework shall ensure that EUCI is given protection appropriate to its classification level and according to basic principles and minimum standards which shall be equivalent to those laid down in this Decision.

Due to the significant role that the Member States play in the implementation of disaster management frameworks a more detailed examination of the relevant national laws and policies in relation to disaster management in relation to CIP is required.

[54] Council Decision 2001/264/EC of 19 March 2001 adopting the Council's security regulations (OJ L 101

[55] Council Decision 2011/292/EU of 31 March 2011 on the security rules for protecting EU classified information OJ L 141

[56] Decision 2012/488/EU Article 2(2)(a) "information and material the unauthorised disclosure of which could cause exceptionally grave prejudice to the essential interests of the European Union or of one or more of the Member States"

[57] Decision 2012/488/EU Article 2(2)(b): "information and material the unauthorised disclosure of which could seriously harm the essential interests of the European Union or of one or more of the Member States"

[58] Decision 2012/488/EU Article 2(2)(c): "information and material the unauthorised disclosure of which could harm the essential interests of the European Union or of one or more of the Member States"

[59] Decision 2012/488/EU Article 2(2)(d): "information and material the unauthorised disclosure of which could be disadvantageous to the interests of the European Union or of one or more of the Member States"

[60] Decision 2012/488/EU Article 1

[61] EU classified information

2.5 Disaster management and National CIP Mechanisms

Having outlined the current EU framework it is important to consider national approaches and legislation in relation to information sharing in the context of disaster situations and this is an area of supporting competence as per Article 196 TFEU.[62] This in addition to Article 222 TFEU (as discussed above) allow the EU to assist and act in this area. However, it is important to note that the EU does not have any additional legislative powers and that it can only support the actions of Member States and thus lacks the power to harmonise national law. As such, there may be some disparities in the national disaster management framework, which may include additional requirements that should be taken into account.

2.5.1 Disaster management framework

First of all, it is important to investigate how the disaster management framework has been implemented on a national level (i.e., through national legislation or policy). From our analysis, it can be concluded that certain Member States have specific national legislation regarding the management of disasters, which should be distinguished from the critical infrastructure protection framework. Belgium's legislation regarding civil protection and disaster management dates back from 1963.[63] More recently, the legal framework for managing disasters at the national level has been shaped by the Royal Decree of 31 January 2003.[64] From this legislation, immediate coordination at the national level will be activated in the event of a disaster. The Home Affairs Crisis Centre plays an important role in events that require coordination at the federal level.[65] Similarly in France[66], Germany and Italy, a legislative framework exists at the national level.[67]

Aside from the above, the national framework may also consist of additional legislation drafted at the regional or local level. For instance, due to Germany's specific legal system (i.e., each of the 16 states has the quality of state and restricted sovereignty), the legislative power is generally assigned to the federal states except when the Constitution explicitly assigns functions to the German Federation. In peacetime, the emergency planning and operational preparation falls under the responsibility of the 16 federal states. Only in a state

[62] Treaty on the Functioning of the European Union.

[63] Law on the civil protection of 31 December 1963 [Wet betreffende de civiele bescherming], *Public Gazette*, 16-01-1964, 422.

[64] Royal Decree of 31 January 2003 on Crisis Management at the national level, *Public Gazette*, 21 February 2003, 8619-8626.

[65] For more information see www.centredecrise.be.

[66] The French legal framework for civil defence and security consists of: The 1950 Ordinance and the 1965 Decree relating to civil defence, the Law of 22 July 1987 as amended by the Laws of 5 January 1988 and 28 November 1990 with respect to civil security; the Order of 24 August 2000 concerning the organisation and powers of the Directorate of Civil Defence and Security. European Commission, 'France - Disaster management structure Vademecum - Civil Protection', last update 10 July 2014, accessed on 15/03/2015 at http://ec.europa.eu/echo/files/civil_protection/vademecum/fr/2-fr-1.html#lega.

[67] See respectively European Commission, 'Germany - Disaster management structure Vademecum - Civil Protection', last update 10 July 2014, accessed on 15/03/2015 at http://ec.europa.eu/echo/files/civil_protection/vademecum/de/2-de.html and European Commission, 'Italy - Disaster management structure Vademecum - Civil Protection', last update 10 July 2014, accessed on 15/03/2015 at http://ec.europa.eu/echo/files/civil_protection/vademecum/it/2-it.html.

of war will the federal responsibility and legislation apply, or if the Parliament decides that there is a "state of tension" (for instance at the preliminary stage of war). Consequently, the disaster management framework consists of legislation and procedures at three different levels[68]:

1) German Federation level
    a) German Civil Protection and Disaster Assistance Act (2009);
    b) bilateral agreements regarding mutual assistance in case of disasters with all nine neighbouring states, as well as Russia, Hungary and Lithuania.
2) Federal state level[69]
    a) 16 different disaster relief acts of the federal states;
    b) the federal states have the right to conclude agreements with foreign countries (but only with the consent of the federal government).
3) Local level (German municipalities and their neighbours across the border)

Certain member states have also set up bilateral agreements for the coordination of disaster management. Clear examples include France, which has set up agreements with 42 countries[70], as well as Italy and Germany.

In contrast to Italy, Germany, France and Belgium, the United Kingdom's framework for disaster management and critical infrastructure protection has been integrated into one single piece of legislation, the Civil Contingencies Act (2004). The Act was introduced in an attempt to modernise previous legislation and to better protect the UK against modern day disasters caused by climate change or terrorism.[71] The Act imposes responsibilities on local responders regarding the preparation and coordination of emergency response and also foresees certain emergency powers for the government. More in particular, the government can 'fast track' legislation if it is deemed necessary to alleviate a serious threat to security, human welfare or the environment.[72]

Finally, it is possible that member states do not have any specific legislation regarding disaster management. For instance in Ireland, emergency planning is part of the general

[68] If there are any conflicts of law, the higher ranking law prevails. German Red cross, 'Analysis of Law in the EU Pertaining to Cross-Border Disaster Relief (EU IDRL Study) - Country Report Red Cross Report'', May 2010, 6, accessed on 17/03/2015 at https://www.ifrc.org/Global/Publications/IDRL/country%20studies/IDRL-Report_GerRC_May2010.pdf.

[69] According to Article 70 of the German Constitution there is no explicit assignment of legislative power to the German Federation.

[70] European Commission, 'France - Disaster management structure Vademecum - Civil Protection', last update 10 July 2014, accessed on 17/03/2015 at http://ec.europa.eu/echo/files/civil_protection/vademecum/be/2-be-1.html#lega.

[71] Civil Contingencies Secretariat, 'Civil Contingencies Act 2004: a short guide (revised)', accessed on 17/03/2015 at http://www.essex.gov.uk/Your-Council/Local-Government-Essex/Documents/15mayshortguide.pdf.

[72] British Institute of International and Comparative Law, 'Analysis of Law in the United Kingdom pertaining to Cross-Border Disaster Relief' 30 June 2010, 27, accessed on 14/02/2015 at http://www.ifrc.org/PageFiles/93649/idrl-uk-cross-border-analysis-0810.pdf.

planning of each Government department. Any emergency planning arrangements are based on a framework adopted by the Government in 2006.[73]

2.5.2 Competence for disaster management

The competence for disaster management differs within the EU Member States. This is the result of the specific political systems and the level of decentralisation. In Belgium and Germany for instance, the government delegates authority to the Home Office or the Ministry of Internal Affairs, which is located in the country's capital and remains accountable to the premier or president.[74] However, depending on the cause of the disaster, other federal ministries or authorities might have competence and get involved in disaster management. In Germany for example, this may be the Federal Ministry for Transport, Building and Urban Affairs ("Bundesministerium für Verkehr, Bau und Stadtentwicklung"), who will have competence if the impending or occurred disaster affects the transport sector.[75]

Furthermore, competence may depend on the impact of the disaster in question. For instance in Belgium, for incidents that only have a provincial or municipal impact, the responsibility for crisis management will fall respectively on the provincial governor or the mayor. To define the appropriate level of crisis management, several factors should be taken into account such as the geographical extent of the disaster, its environmental impact, economic impact, the number of victims, etc.[76] Similarly in the UK, responsibility for disaster management depends on the impact of the disaster. The guiding principle is that prime responsibility for disaster management should remain at the local level.[77]

In other countries, competence for disaster management may be shared among different levels. For instance in France, the civil protection structure is organised at three different levels. Firstly, at the national level, the Minister of the Interior will coordinate the response. The Minister will receive assistance from the defence senior civil servants as well as the Interdepartmental Crisis Management Operations Centre. Secondly, at the zonal level, the zone prefect has the responsibility to coordinate the emergency response in the defence zone. The zone prefect will receive assistance from the Interregional Civil Security Operational Coordination Centre. Finally, at the level of the departments, it will be the departmental prefect that coordinates the response, with the help of the Departmental Operations Centre of the Fire and Emergency Services.

It is also possible that disaster response is coordinated through a specific body. The Office of Emergency Planning in Ireland, which can be administratively associated with the Ministry of

[73] The so-called Framework for Major Emergency Management, see European Commission, 'Ireland - Disaster management structure Vademecum - Civil Protection', last update 10 July 2014, accessed on 14/02/2015 at http://ec.europa.eu/echo/files/civil_protection/vademecum/ie/2-ie-1.html#lega.

[74] E. Kirchner http://uaces.org/documents/papers/1201/kirchner.pdf p 5

[75] German Red cross, '"Analysis of Law in the EU Pertaining to Cross-Border Disaster Relief (EU IDRL Study) - Country Report Red Cross Report', May 2010, 9, accessed on 12/03/2015 at https://www.ifrc.org/Global/Publications/IDRL/country%20studies/IDRL-Report_GerRC_May2010.pdf.

[76] European Commission, 'Belgium - Disaster management structure Vademecum - Civil Protection', last update 10 July 2014, accessed on 12/03/2015 at http://ec.europa.eu/echo/files/civil_protection/vademecum/be/2-be-1.html#lega.

[77] European Commission, 'United Kingdom - Disaster management structure Vademecum - Civil Protection', last update 10 July 2014, accessed on 12/03/2015 at http://ec.europa.eu/echo/files/civil_protection/vademecum/uk/2-uk-1.html#over.

Defence is a clear example in that regard. However, each Government department remains responsible for having actual emergency plans and procedures in place in their own area of responsibility. Finally, it is important to note that certain sector-specific legislation may foresee additional powers to specified actors. An example can be found in the UK, where the 1993 Railways Act or the 1989 Electricity Act allows the Secretary of State to give directions to specific actors in case of a great national or civil emergency.[78]

As can be extracted from our analysis, the competence for disaster management may vary across the different Member States. Therefore, it is recommended for each partner to keep the relevant national implementations of the disaster management framework into account.

2.5.3 Mechanisms for public-private partnerships: what is the status?

The majority of critical infrastructures in the countries examined for the purposes of this deliverable were not state-owned facilities, but were operated by private companies. This explains the increasingly important role of public-private cooperation in the field of civil protection and CIP.[79] This form of cooperation includes partnerships for critical infrastructure protection, for the prevention of cyber-attacks or even ensuring a secure supply.

First of all, cooperation can happen in an informal way. For instance, Germany closely cooperates with CI operators within the framework of established security partnerships, both on sectoral and cross-sectoral issues.[80] This cooperation usually happens in an informal way and the operators represent different sectors including energy, transport and finance.[81]

However, public-private partnerships may also happen in a more formal framework. In the UK, the Centre for the Protection of National Infrastructure ("CPNI") acts as the facilitator of 14 different information exchanges. More specifically, it facilitates the sharing of information regarding financial services, the transport sector, etc.[82]

Other countries may have both informal cooperation as well as formalised specific information sharing requirements for the coordination of disaster response. For instance in France, the sharing of information during disaster situations will take place according to the External Protection Plan[83], but the French CERT-FR remains involved in the real-time sharing of information through a network of confidence. Through this network, critical infrastructure operators can share information related to the imminent or realised disaster. However, if the information is too sensitive, critical infrastructure operators can merely refer

[78] European Commission, 'United Kingdom - Disaster management structure Vademecum - Civil Protection', last update 10 July 2014, accessed on 12/03/2015 at http://ec.europa.eu/echo/files/civil_protection/vademecum/uk/2-uk-1.html#over.

[79] M. Suter, 'PPPs in Security Policy: Opportunities and limitation' (2012), 1, accessed on 15/03/2015 at http://www.css.ethz.ch/publications/pdfs/CSS-Analysis-111-EN.pdf.

[80] Ibid.

[81] http://ec.europa.eu/echo/files/civil_protection/vademecum/de/2-de-1.html#lega

[82] For more information see D. Clifford, A. Ricci, G.D. Finocchiaro, L. Proenca, Y.S. Van Der Sype, and K. e Silva, 'ECOSSIAN D7.1 Analysis of the applicable legal framework' (2014), 45-46.

[83] This plan defines the parameters in which the public sector may interact with the private CI operator in response to potential threats. For more information see D. Clifford, A. Ricci, G.D. Finocchiaro, L. Proenca, Y.S. Van Der Sype, and K. e Silva, 'ECOSSIAN D7.1 Analysis of the applicable legal framework' (2014), 75.

to the protection measures. In addition, French critical infrastructure operators have a sector specific obligation to inform the Prime Minister of incidents that affect the critical infrastructures operation or information systems (for instance a disaster).[84] France also has a national alert mechanism that allows for the warning of interested parties, both in the public and the private sector (the so-called Vigipirate plan).

Finally in other Member States, like Belgium and Ireland, no systematic partnerships for the sharing of information in disaster situations or for civil protection have yet been established.[85] In Italy, the current status of public-private partnerships is unclear, and even though certain partnerships have been formed, the stakeholders are prevented from reaping the full benefits of information sharing.[86] This situation might change in the near future as one of the actions of the Digital Agenda of Italy is to

> "Strengthen public-private cooperation: create mechanisms of debate, sharing and coordination between the public and private sectors, especially with regard to critical infrastructure protection"

and explicitly refers to Germany as a good example for public-private partnerships.[87]

The table below gives an overview of the requirements extracted from the analysis provided above.

Req. number	Description	Importance* (M/O)	Relevant for Level			Comment
			O-SOC	N-SOC	E-SOC	
GReq. 1.1	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. 1.2	National implementations of Directive 2008/114/EC must be consulted as they may (for example France) have specific requirements on the	M	X	X	X	

[84] Article L. 1332-6-2 Law no 2013-1168 Loi de Programmation Militaire 18 décembre 2013.

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

[86] M. Angelini, M.C. Arcuri, et al., 'Italian Cyber Security Report - Critical Infrastructure and Other Sensitive Sectors Readiness', (2013), 24.

[87] G. Ateniese, R. Baldoni et al., 'Critical Infrastructure Protection: Threats, Attacks and Countermeasures', (2014), Tenace Project, 13.

Req. number	Description	Importance* (M/O)	Relevant for Level			Comment
			O-SOC	N-SOC	E-SOC	
	security architecture implementation.					
GReq. 1.3	National measures relating to disaster management must be consulted in order to decipher the relevant authorities for the specific sector, any public-private information sharing initiatives/requirements and how this interacts with national critical infrastructure protection.	M	X	X	X	

*M – mandatory; O – optional

** Work Packages where this requirement should be implemented

Table 1. CI protection and the disaster management framework

Chapter 3 Legal framework for information sharing

As noted in the previous chapter although the current framework for the protection of critical infrastructures and disaster management encourages cooperation and participation, information sharing in disaster situations at an EU level happens on a voluntary basis. However, one must also consider other potentially applicable frameworks which may facilitate information sharing in disaster situations stemming from attacks on critical infrastructures. These can be divided into two categories: first those based on criminal law and second specific legal frameworks covering ICT security more generally. The purpose of this chapter is to analyse these frameworks in depth and extract the requirements that are relevant for ECOSSIAN, which need to be taken into account throughout the lifecycle of the project.

3.1 Criminal law - Implications for data sharing in disaster situations

3.1.1 Cyberwar - State of emergency

As extrapolated from the use cases developed in Task 1.2 'Use case definitions' (D1.5 'Use case scenario report') in WP1, it must be considered that attacks can originate from State actors as well as from terrorist organisations and more general criminal groups. In the case of State-supported attacks, the applicability of the law of armed conflict (namely the components of *jus ad bellum*[88] and *jus in bello*[89]) must be considered. This area of international law may provide a justification for subsequent measures taken.[90] However, although this may permit an attacked State to declare a state of emergency thereby increasing cooperation and coordination it is difficult to anticipate and thus criminal law specific considerations are perhaps more relevant in this context.

3.1.2 Cybercrime - Criminal attacks

It must be understood that in the case of terrorist or criminal group attacks two legal frameworks covering criminal justice may apply, namely international criminal and national criminal law. The purpose of this section is to examine the substantive and procedural frameworks which may have applicability in the context of information sharing in disaster situations following an attack on a critical infrastructure. A key issue in the deciphering of legal considerations is the legal status of the entity holding/sharing the information. For instance if it is private or a public entity without law enforcement competence there may be

[88] Law on the criteria for going to war.

[89] Law on ongoing armed conflicts.

[90] E. Tikk, K. Kaska and L. Vihul, 'International Cyber Incidents Legal Considerations 2010 Cooperative Cyber Defence Centre of Excellence 80. https://ccdcoe.org/publications/books/legalconsiderations.pdf.

specific requirements in relation to the sharing of information about a crime whereas public bodies with law enforcement competence have specific concerns in relation to the sharing of information with other such agencies in a cross-border manner. In the context of ECOSSIAN this has clear importance in relation to the status of the N-SOC and E-SOC levels as their obligations may differ depending on their status.

3.1.2.1 Private or public entities without law enforcement competence

As outlined in Chapter 2 a major issue in relation to information sharing in the context of disaster management and critical infrastructures lies in the fact that the majority of CIs are in private ownership. This raises some concerns in relation to their capacity to investigate criminal attacks against their assets. In the context of ECOSSIAN, this clearly affects the O-SOC level. However, one must understand that even if this infrastructure is public (and by extension the N-SOC and E-SOC), without law enforcement competence there may be a duty to report to the appropriate authorities if a genuine attack is identified. For instance in Ireland under Article 19 of the 2011 Criminal Justice Act there is a specific obligation to report relevant information of such serious crimes to the Gardai (national police force and more particularly Garda Computer Crime Unit).[91]

However, it must be understood that cyber-attacks can originate outside the EU and accordingly one must consider the EU mechanisms designed to help coordinate and effectively cooperate within the EU in obtaining evidence in criminal matters. In this regard the adoption of Directive 2014/41/EC on the European Investigation Order in criminal matters is significant.[92] This Directive will replace most of the existing laws regarding the transfer of evidence between Member States from the 22nd of May 2017. However, it must be understood that both Ireland and Denmark have opted out. Currently the legislative framework consists of:

- the Council of Europe Convention on Mutual Assistance in Criminal Matters of 20 April 1959 (and its two additional protocols);93
- parts of the Schengen Convention;94
- the 2000 EU Convention on Mutual assistance in criminal matters (and its Protocol);95
- the 2008 Framework Decision on the European evidence warrant;96 and

[91] Criminal Justice Act 2011, Number 22 of 2011 www.irishstatutebook.ie/2011/en/act/pub/0022/index.html.

[92] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters OJ L 130, 1–36.

[93] European Convention on Mutual Assistance in Criminal Matters Strasbourg, 20.IV.1959 accessed on 24/03/2015 at www.conventions.coe.int/Treaty/en/Treaties/Html/030.htm.

[94] Schengen Agreement of 1985.

[95] Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union (2000/C 197/01).

[96] Council Framework Decision 2008/978/JHA of 18 December 2008 on the European evidence warrant for the purpose of obtaining objects, documents and data for use in proceedings in criminal matters OJ L 350 72–92.

- the 2003 Framework Decision on the execution in the European Union of orders freezing property or evidence (as regards freezing of evidence). 97

This new Directive is an advance as it moves from the notion of legal assistance to mutual recognition. According to Article 1(1)

> "A European Investigation Order (EIO) is a judicial decision which has been issued or validated by a judicial authority of a Member State… to have one or several specific investigative measure(s) carried out in another Member State ('the executing State') to obtain evidence in accordance with this Directive. The EIO may also be issued for obtaining evidence that is already in the possession of the competent authorities of the executing State."

Thus the Directive applies to almost all investigative measures but will not apply to Schengen cross-border surveillance by Police officers under the Schengen Convention or the setting up/gathering of evidence by a joint investigation team. Indeed, as per recital 8 "the setting up of a joint investigation team and the gathering of evidence within such a team require specific rules which are better dealt with separately." In essence this mechanism will allow for more effective cross-border investigations which is important in the context of information sharing in disaster situations in order to identify and prosecute the perpetrators.[98] Given that there is still quite some time before the Directive must be adopted progress as regards implementation should be watched with interest. This is an area which will be assessed further in the second iteration of this report.[99]

3.1.2.2 Public bodies with law enforcement competences

Before delving into the specifics in this section it is important to observe that, as noted by the ENISA report on encouraging information exchange between CERTs, the utility of cooperation frameworks based on criminal law depends largely on the status of the entity, as only those public bodies with law enforcement competences can avail of certain mechanisms.[100] In the context of ECOSSIAN, given that we are dealing with concerted cyber-attacks it is important consider the application of such measures in relation the N-SOC and E-SOC levels as these entities may have such competences.

At an international level there has been some attempt at harmonisation in the form of the Convention on Cybercrime. However, despite the fact that this has been signed by 53 States 8 have failed to ratify including Ireland, Greece and Sweden.[101] In addition, the EU has also

[97] Council Framework Decision 2003/577/JHA of 22 July 2003 on the execution in the European Union of orders freezing property or evidence OJ L 196 45–55.

[98] E. De Capitani and S. Peers 'The European Investigation Order: A new approach to mutual recognition in criminal matters' accessed on 23/04/2015 at: eulawanalysis.blogspot.com/2014/05/the-european-investigation-order-new.html

[99] Due in month 36.

[100] ENISA, 'A flair for information sharing- encouraging information exchange between CERTs' (2011) accessed on 01/03/2015 at: http://www.enisa.europa.eu/activities/cert/support/fight-against-cybercrime/legal-information-sharing

[101] Convention on Cybercrime CETS No.: 185 accessed on 21/01/2015 at: conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG.

adopted Directive 2013/40/EU on attacks against information systems.[102] This Directive entirely replaces the provisions of Council Framework Decision 2005/222/JHA of 24 February 2005[103] and specifically according to Article 1 the "Directive establishes minimum rules concerning the definition of criminal offences and sanctions in the area of attacks against information systems. It also aims to facilitate the prevention of such offences and to improve cooperation between judicial and other competent authorities." The Directive is must be adopted before the 4th of September 2015.

3.1.2.2.1 Substantive harmonisation

Directive 2013/40/EU has a clear goal towards the harmonisation of minimum standards by ensuring that these types of crimes are punishable by effective, proportionate and dissuasive criminal penalties. Indeed, for example and of particular significance in our current context, Article 5(4)(c) states that attacks against Critical Infrastructures should be punishable by a term of imprisonment of at least 5 years.

However it must be noted that this is an important development as substantive harmonisation would allow for clarity in relation to cross-border substantive legal standards for offences as these can vary and may be broad. Indeed as noted by the ENISA report in the context of CERTs such disparities present a dual challenge:

> "in the absence of formal investigative mandates, there is a risk that activities they have engaged in to obtain or exchange information may themselves qualify as illegal activities as illegal activities, both tainting the information for further use by other CERTs or investigative bodies, and opening them up to legal liabilities. The risk of personal legal liability becomes greater when CERTs have no clear mandate from their national government to conduct specific investigations or collect new information, as this implies that their actions or requests have no official authority or basis in law. Thus, CERTs need to make sure that the information in their possession is lawfully obtained. In case of doubt, they are unlikely to make the information available to other CERTs or third parties."[104]

Nevertheless, the substantive provisions included in the Directive require transposition in the Member States and this raises concerns in relation to harmonisation and divergences and interpretation and could thus lead to disparity.[105]

[102] 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 OJ L 218, 14.8.2013 8–14

[103] Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems OJ L 69, 16.3.2005, 67–71.

[104] ENISA, 'A flair for information sharing- encouraging information exchange between CERTs' (2011) accessed on 01/03/2015 at: http://www.enisa.europa.eu/activities/cert/support/fight-against-cybercrime/legal-information-sharing

[105] ENISA, 'The Directive on attacks against information systems A Good Practice Collection for CERTs on the Directive on attacks against information systems' (P/28/12/TCD 2013).

3.1.2.2.2 Procedural

The concerns highlighted in relation to the disparities is also potentially an issue in relation to the procedural aspects of Directive 2013/40/EU. At an EU level the harmonisation of criminal procedural law has been limited due to a lack of competence and as such harmonisation is fragmented. Although the Convention on Cybercrime does contain a section on procedural law (section 2) and thus a degree of harmonisation this is limited.[106] For instance there are no rules on the safe storage of information thus implying that there may be disparities and that storage practices in one country may not satisfy those in another hence affecting the information's evidentiary value). Moreover, there are no comparable measures at an EU level. As such, this also implies that entities investigating cybercrime may not be able to avail of the same tools (depending on their status as a public body with law enforcement competences).[107]

In essence Directive 2013/40/EU aims to increase criminal justice cooperation through two key means:

- strengthening the existing structure of 24/7 contact points, including an obligation to answer within 8 hours to urgent requests (at least in terms of whether the request will be answered, and the form and estimated time of the answer);
- introducing an obligation to collect basic statistical data on cybercrimes.

The Directive also aims to improve the cooperation between the competent authorities, agencies and bodies (such as national authorities), Eurojust, Europol (and its European Cyber Crime Centre[108]), and ENISA. This is indicative of the general move towards more harmonisation and increasing judicial cooperation.

3.1.3 Data protection and Police and judicial cooperation in criminal matters

In the context of data sharing between public entities it is significant to consider the Framework Decision "on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters".[109] From Article 1(1) the Framework Decision aims to provide "a high level of protection of the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data in the framework of police and judicial cooperation in criminal matters, provided for by Title VI of the Treaty on European Union, while guaranteeing a high level of public safety."

---

[106] Convention on Cybercrime CETS No.: 185 accessed on 21/01/2015 at: conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG.

[107] ENISA, 'A flair for information sharing- encouraging information exchange between CERTs' (2011) accessed on 01/03/2015 at: http://www.enisa.europa.eu/activities/cert/support/fight-against-cybercrime/legal-information-sharing

[108] This Centre has 4 key functions: (1) serve as the European cybercrime information focal point; (2) pool European cybercrime expertise to support Member States; (3) provide support to Member States' cybercrime investigations; (4) become the collective voice of European cybercrime investigators across law enforcement and the judiciary. For more see: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012DC0140&from=EN; C. O'Donoghue, T.J. Nagle and C. Nielsen Czuprynski, *EU Proposed Directive on Network and Information Security*, 13 February 2013, http://www.reedsmith.com/EU-Proposed-Directive-on-Network-and-Information-Security-02-13-2013/.

[109] Council Framework Decision 2008/977/JHA, OJ L 350/60, 30.12. 2008.

The Decision covers intra-Member State personal data processing.[110] In essence, this means that data processing in this context in one Member State falls outside the terms of the Decision and leaves this matter for the Member States to decide.[111] As noted by de Hert and Papakonstantinou,

> "The scope limitation (the DPFD[112] applies only to sets of data that are transmitted among Member States) has made necessary the introduction of a series of Articles on such ''international'' cooperation, regulating issues, for instance, of ''logging and documentation'', verification of quality, compliance with national processing restrictions, or even transmission to private parties (Art. 9–15)."[113]

However, it should be observed that from Article 1(4) "this Framework Decision is without prejudice to essential national security interests and specific intelligence activities in the field of national security". Despite this Article 3(1) stipulates that "personal data may be collected by the competent authorities only for specified, explicit and legitimate purposes in the framework of their tasks and may be processed only for the same purpose for which data were collected. Processing of the data shall be lawful and adequate, relevant and not excessive in relation to the purposes for which they are collected." Furthermore this is supplemented by Article 4(1) states that "personal data shall be rectified if inaccurate and, where this is possible and necessary, completed or updated." However, the application of this Directive is restricted by a series of exemptions. As per de Hert and Papakonstantinou,in essence this "exempting methodology has been meticulously applied on each and every one of the basic data protection principles, most of the times thus emptying them of their content for the protection of individuals." This is clearly evident in relation to Article 3(1) which states that ''further processing for another purpose shall be permitted in so far as:''(a) it is not incompatible with the purposes for which the data were collected; (b) the competent authorities are authorised to process such data for such other purpose in accordance with the applicable legal provisions; and (c) processing is necessary and proportionate to that other purpose. The competent authorities may also further process the transmitted personal data for historical, statistical or scientific purposes, provided that Member States provide appropriate safeguards, such as making the data anonymous''.

3.1.4 The Proposed Police and Criminal Justice Data Protection Directive

It should also be noted that the reform of the Data Protection Framework in the EU is not limited to the proposed Regulation but also encompasses the proposal[114] to replace the existing Framework decision covering personal data processing in the area of law

[110] Framework Decision 2008/977/JHA Article 1(2)(a).

[111] Indeed from Article 1(5): Member States can adopt, "for the protection of personal data collected or processed at national level, higher safeguards than those established in this Framework Decision."

[112] Data Protection Framework Decision.

[113] P. de Hert and V. Papakonstantinou, 'The Data Protection Framework Decision of 27 November 2008 regarding police and judicial cooperation in criminal matters – A modest achievement however not the improvement some have hoped for', *Computer Law & Security Review 25 (2009): 403-414.*

[114] Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, Brussels, 25.1.2012 COM(2012) 10 final 2012/0010 (COD)

enforcement and criminal justice. The proposed introduction of this Directive aims at simplifying and supplementing the current Framework Decision.

According to the explanatory memorandum attached to the Directive:

> 'Article 1 defines the subject matter of the Directive, i.e. rules relating to processing of personal data for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal offences, and sets out the Directive's two-fold objective, i.e. to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data while guaranteeing a high level of public safety, and to ensure the exchange of personal data between competent authorities within the Union.'[115]

Article 2 defines the scope and in contrast to the current Framework Decision provides that its application is not limited to cross-border processing but instead applies to all activities covered by the Directive performed by 'Competent Authorities'. These authorities are defined in Article 3(14) as: 'competent authorities' means any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties'. Therefore, it appears that activities undertaken at the O-SOC level are unlikely to fall under the scope of application of this proposal. However, depending on their status within the State it is possible that it may have an influence at the N and E-SOC levels. Another interesting definition that is provided in the draft Directive is that of personal data breach. The Directive provides that "'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed". The development of this proposed Directive should be watched closely as it may have a strong potential impact on the operations to be undertaken in the context of ECOSSIAN.

The table below gives an overview of the requirements extracted from the analysis provided above.

Req. number	Description	Importance* (M/O)	Relevant for Level			Comment
			O-SOC	N-SOC	E-SOC	
GReq. 2.1	The legal status of the entity wishing to share information needs to be established in order to decipher the specific legal considerations relevant.	M	X	X	X	
GReq.	The origin of the attack might need clarification in order to	O	X	X	X	This will often be extremely difficult as

[115] See: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0010:FIN:EN:PDF

Req. number	Description	Importance* (M/O)	Relevant for Level			Comment
			O-SOC	N-SOC	E-SOC	
2.2	establish the correct legal basis for information sharing.					the motivations/entities behind an attack may not always be clearly identifiable.
GReq. 2.3	National implementations should be consulted following the adoption of legislation.	M	X	X	X	This is a reference to Directive 2014/41/EC and Directive 2013/40/EU which are yet to be transposed into national law in all 28 Member States.

*M – mandatory; O – optional

** Work Packages where this requirement should be implemented

Table 2. Criminal law - Implications for data sharing in disaster situations

3.2 ICT specific legal frameworks

The purpose of this section is to analyse the additional legal frameworks which have an impact on information sharing in disaster situations. In this context the obligation to report security and personal data breaches will be assessed.

3.2.1 Breach notification obligations

In analysing the specific ICT law frameworks one must first acknowledge that in the context of critical infrastructures there is a clear disparity in legal requirements between the obligations of a critical information infrastructure offering a public communications network and a critical infrastructures operating on a closed network. This disparity has been highlighted in both of the previous reports but is nonetheless again important to specify.[116] To reiterate, currently in the context of data protection and privacy, data breach notification requirements are restricted in application to the communications sector with both the E-

[116] D. Clifford, A. Ricci, G.D. Finocchiaro, L. Proenca, Y.S. Van Der Sype, and K. e Silva, 'ECOSSIAN D7.1 Analysis of the applicable legal framework' (2014) and D. Clifford, A. Spangaro, A. Ricci, and Y.S. Van Der Sype, 'ECOSSIAN D7.2 Legal requirements' (2015).

Privacy Directive[117] and the recent Data Breach Notification Regulation[118] providing such obligations and the provision of a communications network or service to the public.[119] However, as the operations in ECOSSIAN remain outside the scope of their application (i.e. ECOSSIAN is neither a public communications network nor a service provider) these requirements appear to have no effect. However, it is significant to note that this does not prevent Member States from introducing a more general requirement to report personal data breaches into national law.

Indeed, and as highlighted in D7.2, in Germany a breach notification duty was added in section 42a of the Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG).[120] This applies in relation to sensitive personal data and personal data related to:

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

As discussed in D7.1 this contrasts sharply with the legislation in other Member States where such notification requirements are restricted to the telecommunications sector.[121] Indeed, in Ireland and the UK the DPAs have issued Codes of Conduct on the requirement to report data breaches generally. However, this is soft law and it must be understood that currently Germany is the only Member State that extends this requirements beyond the telecommunications sector in hard law.

However, the proposed changes as contained in the draft General Data Protection Regulation should be considered. The draft aims towards the introduction of an obligation to notify personal data breaches in Articles 31 and 32 to the relevant parties “without undue delay”. The requirement is further reflected in the proposed Police and Criminal Justice Data Protection Directive[122] and in the area of network and information security to which our attention now turns.

---

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

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

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

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

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

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

Similar to the draft General Data Protection Regulation, the proposed Network and Information Security Directive[123] aims at bridging the gap in notification requirements, and in particular for Critical Infrastructure operators. As this legislative reform is likely to be implemented during the lifecycle of ECOSSIAN it is important to weigh its impact accordingly.

Under article 14 and 15 of the current draft proposal include the following obligations for "market operators" [124]

- notify the competent authority of incidents having a significant impact on the security of the core services they provide, and
- (a) provide information needed to assess the security of their networks and information systems, including documented security policies;
- (b) undergo a security audit carried out by a qualified independent body or national authority and make the results thereof available to the competent authority.125

Thus, in practice the proposed NIS Directive will impose information sharing obligations to CI operators, whenever an incident having a significant impact on the security of their services occurs. As such, the link with the disaster management is clear, as a major cyber attack (a so-called "incident") against a CI resulting in a civil incident could also qualify as a disaster under the disaster management framework.

The table below gives an overview of the requirements extracted from the analysis provided above.

Req. number	Description	Importance* (M/O)	Relevant for Level			Comment
			O-SOC	N-SOC	E-SOC	
GReq. 3.1	National legislation on the requirements in relation to breach notification must be consulted.	M	X	X	X	i.e. the disparity between Germany and other Member States and also Ireland and the UK that have adopted codes of conduct should be

[123] Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union /* COM/2013/048 final - 2013/0027 (COD).

[124] Article 3 (8) of the proposed NIS Directive explicitly includes operators of Critical Infrastructures in its definition of "market operators": "operators of infrastructures that 'are essential for the maintenance of vital economic and societal activities in the fields of energy, transport, banking, financial market infrastructures, internet exchange points, food supply chain and health, and the disruption or destruction of which would have a significant impact in a Member State […] insofar as the network and information systems concerned are related to its core services'".

[125] Article 15 proposed NIS Directive.

Req. number	Description	Importance* (M/O)	Relevant for Level			Comment
			O-SOC	N-SOC	E-SOC	
						assessed.
GReq.3.2	Developments in relation to proposed amendments should be consulted following the adoption of legislation.	M	X	X	X	

*M – mandatory; O – optional

** Work Packages where this requirement should be implemented

Table 3. ICT specific frameworks requirements

Chapter 4 Legal barriers to information sharing

When a disaster hits or is imminent, the collection and sharing of information may invoke the application of specific legal frameworks, which may present potential barriers. Before going into the analysis, it must be understood that whenever assessing the legality of information sharing in disaster situations, one must always consider other overlapping frameworks and the applications contained therein. Key to this, there is the assessment of what is proportionate, and the application of the principle of proportionality. As per Article 5 (4) TEU, the principle of proportionality refers to the fact that any measure to be imposed must be strictly necessary to the public interest in order to achieve its purpose. Thus, measures affecting fundamental rights should be appropriate, reasonable and necessary.

4.1 Data protection requirements

The collection and sharing of personal data may be necessary in disaster situations. In this regard, the analysis of the data protection framework D7.1 remains relevant. Article 7 of Directive 95/46/EC requires a legitimate ground for processing (i.e., the sharing of information) personal data. The most relevant ones that may apply in disaster situations are art. 7 (c) necessary to comply with a legal obligation, 7 (e) necessity for the performance of a task in the public interest (i.e., disaster management) or 7 (f) the legitimate interest of the data controller (i.e., the CI operator sharing information to protect its CI). However, it is important to analyse how Article 7 has been transposed into national legislation as there may be some variations.

An interesting example of a legal obligation (as required by 7 (c)) can be found in the UK's Civil Contingencies Act. More in particular, secondary legislation under the Civil Contingencies Act provides a legal basis for the sharing of information.[126] This legislation requires certain types of responders to share information related to civil protection with other responders on request. This requirement does not entail an exemption of the data protection requirements, but merely provides a ground for the exchange of information. Thus, responders will still have to comply with the requirements of the Data Protection Act. After the terrorist bombings in 2005, the UK Government produced guidelines on the sharing of data for emergency planners and responders. The guidelines include certain key principles to help responders to decide whether or not data should be collected or shared. [127] According to the Government,

> "the public interest in sharing data will generally be more be more significant than in normal circumstances".[128]

[126] British Red Cross, 'Analysis of Law in the United Kingdom pertaining to Cross-Border Disaster Relief' (2010), 44, accessed on 18/03/2015 at http://www.ifrc.org/PageFiles/93649/idrl-uk-cross-border-analysis-0810.pdf.

[127] Cabinet Office, 'Data Protection and Sharing – Guidance for Emergency Planners and Responders' (2007), accessed on 18/03/2015 at https://www.gov.uk/government/publications/data-protection-and-sharing-guidance-for-emergency-planners-and-responders.

[128] British Red Cross, 'Analysis of Law in the United Kingdom pertaining to Cross-Border Disaster Relief' (2010), 44, accessed on 18/03/2015 at http://www.ifrc.org/PageFiles/93649/idrl-uk-cross-border-analysis-0810.pdf.

The UK guidelines state that if individuals share personal data during a disaster situation in good faith, personal liability will be highly unlikely. It is more likely that the organisation to which the individuals belong will face legal action.[129] From this, it can be concluded that the UK data protection framework is sufficiently flexible to enable the sharing of information in disaster situations if necessary. The same reasoning can be used in the other Member States. Whenever personal data is exchanged in disaster situations it will be easier to provide evidence of the public interest as well as the legitimate interest of the data controller and rely on either one of these grounds for the processing.

Besides this, it is important to keep in mind that national data protection legislation may foresee in an explicit exemption of certain data protection requirements for the sharing of information in disaster situations. According to Directive 95/46/EC:

> "Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6 (1), 10, 11 (1), 12 and 21 when such a restriction constitutes a necessary measures to safeguard:
> (a) national security;
>
> (b) defence;
>
> (c) public security;
>
> (d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;
>
> (e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;
>
> (f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e); ..." "

Therefore, it is necessary to have a look at the national implementations of Article 13 of Directive 95/46/EC. In general, Member States have only made very limited use of the possibility to fully exclude the processing of personal data related to public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law.[130] For instance in the UK and Ireland no explicit exemption is foreseen in the Data Protection Act for the collection and sharing of information when a disaster hits or is imminent. Consequently, emergency responders will have to comply with the general data protection requirements. In other countries, like Italy, the sharing of personal data in the area of state security or defence is subject to special laws or rules, yet they still need to be conform to the data protection principles.[131]

The following table presents the extracts of the table from Deliverable 7.2 'Legal requirements' that are relevant to information sharing in disaster situations as described *supra*.

---

[129] 'Data Protection and Sharing – Guidance for Emergency Planners and Responders' February 2007, available at: http://www.cabinetoffice.gov.uk/media/132709/ dataprotection.pdf.

[130] See Article 3 (2) Directive 95/46/EC; 142, http://194.242.234.211/documents/10160/10704/Stato+di+attuazione+della+Direttiva+95-46-CE.

[131] D. Korff, 142, http://194.242.234.211/documents/10160/10704/Stato+di+attuazione+della+Direttiva+95-46-CE.

Req. number	Description	Importance* (M/O)	Relevant for Level			Comment
			O-SOC	N-SOC	E-SOC	
GReq. 4.1	As described in the Data Protection Coordinator's Report notification and authorisation requirements must be respected[132]	M	X	X	X	Articles 18, 19 and 20 Directive 95/46/EC and their national MS equivalents as stipulated by the national law of the competent Member State.
GReq. 4.2	If sensitive data is processed the specific restrictions should be complied with.	M	X	X	X	The more stringent national laws applicable for the processing of sensitive data and the requirements of Art. 8 Directive 95/46/EC (including export restrictions) must be complied with if these special categories of data are being processed.
GReq. 4.3	The data controller is required to have a legal ground in order to process the personal data. In the context of information sharing in disaster situations this table focuses on the most relevant and as such for a complete list D7.2 should be consulted. Finally, ***regard should also be had to any potential exemption in national law to the application of the legal requirements.***	M	X	X	X	Article 7 Directive 95/46/EC, and in the case of the exemption Article 13 and the relevant national legislation justifying this exemption.
GReq. 4.3.1	If the existence of a legal obligation is the legal ground for the data	M	X	X	X	Article 7(c) Directive

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

Req. number	Description	Importance* (M/O)	Relevant for Level			Comment
			O-SOC	N-SOC	E-SOC	
	processing, 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.					95/46/EC.
GReq. 4.3.2	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. 4.3.3	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. 4.3.4	If the legitimate interest of the data controller is used as the legal ground for data processing, the controller is required to have a legitimate interest in the data processing.	M	X	X	X	Article 7(f) Directive 95/46/EC
GReq. 4.4	ECOSSIAN must respect the Data quality principles.	M	X	X	X	Article 6 Directive 95/46/EC

Req. number	Description	Importance* (M/O)	Relevant for Level			Comment
			O-SOC	N-SOC	E-SOC	
GReq. 4.4.1	All processing operations involving personal data in ECOSSIAN must be completed fairly and lawfully and cannot contravene the protections afforded under the Data Protection Framework.	M	X	X	X	Article 6(a) Directive 95/46/EC
GReq. 4.4.2	The personal data 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. 4.4.3	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. 4.4.4	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. 4.4.5	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	M	X	X	X	Article 6(d) Directive 95/46/EC

Req. number	Description	Importance* (M/O)	Relevant for Level			Comment
			O-SOC	N-SOC	E-SOC	
	deletion of the unnecessary personal data.					
GReq. 4.5	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

*M – mandatory; O – optional

** Work Packages where this requirement should be implemented

Table 4. Data protection requirements

4.2 Requirements in intellectual property law

Intellectual property law is an ancillary area of law which may have an impact on information sharing in disaster situations. To efficiently respond to a disaster may require the sharing of information incorporating intellectual property (IP) protection. IP grants the rights holder exclusive rights, meaning that they have the exclusive power to perform certain categories of actions in relation to their works (e.g. dissemination and duplication).

At an international level attempts at harmonising resulted in the adoption of the Berne Convention for the Protection of Literary and Artistic Works on 9 September 1886. Current protections are a combination of international treaties, EU legislation and national provisions. Although there is some degree of harmonisation this is far from complete and clear disparities exist between Member States. The following is a list of the most significant international sources:

- Berne Convention for the Protection of Literary and Artistic Works (1886, latest version, Paris 1971);
- Rome Convention for the protection of Performers, producers of phonograms and broadcasting organisations (1961);
- Agreement on Trade related aspects of intellectual property rights (TRIPS) (1994);
- WIPO Copyright Treaty (1996);
- WIPO Performances and phonograms Treaty (1996).

For the purposes of this Deliverable our attention will focus first on the EU level legislative advances as they provide more precise insights and have grown from these international

foundations.[133] Indeed, this is evidenced by the fact that Ireland was in breach of its obligations by failing to comply with the right version of the Berne Convention by the 1st of January 1995 following the issuing of a reasoned opinion requiring compliance by the Commission.[134]

It must be understood that is unlikely that there would be an infringement of certain IP rights such as computer programme copyright, patent law or trademark law.[135] This is based on the assumption that the information that would be shared in a disaster situation would be unlikely to constitute anything other than information to be processed by a computer programme.

Accordingly the key Directives[136] in this context are as follows:

– Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (OJ 2001 L 167, p. 10);

- Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases (Database Directive).

The EU database Directive (1) harmonises the treatment of databases under copyright law and (2) establishes a sui generis right for the creators of databases which do not qualify for copyright. As such, for the purposes of this analysis there are three divisions to consider namely: ordinary copyright, database copyright and the *sui generis* Database right. Generally copyright (i.e. ordinary copyright and database copyright) as a legal concept grants the creator/author of an original work exclusive rights for a limited period of time (usually 70 years after the death of the creator/author). In contrast, the *sui generis* Database right does not protect the original result of an intellectual creation but instead the sweat of the brow of the database creator. Indeed according to recital 7 of the Database Directive this right was developed as "the making of databases requires the investment of considerable human, technical and financial resources while such databases can be copied or accessed at a fraction of the cost needed to design them independently."

In relation to each of these categories different objects come under the scope of protection, a variety of acts are restricted (i.e. acts that subject to authorisation of the right holder) but also a number of exceptions (i.e. acts that are not subject to the authorisation of the right holder). These are represented in the following table.

[133] See: Council Resolution of 14 May 1992 on increased protection for copyright and neighbouring rights [1992] OJ C138/1; Rental lending and related rights Directive; and Treaty establishing EEA.

[134] Case C-13/00 *Commission v Republic of Ireland* (ECJ 19 March 2002).

[135] However for absolute certainty regard must be had to all relevant IP rights.

[136] Other EU legislation includes: Directive 2006/115/EC of the European Parliament and of the Council of 12 December 2006 on rental right and lending right and on certain rights related to copyright in the field of intellectual property, OJ L 376, 28-35; Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs, OJ L 111, 16-22; Council Directive 87/54/EC of 16 December 1986 on the legal protection of topographies of semiconductor products, OJ L24, 36; Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, OJ L 195, 16-25;Council Directive 93/83/EEC of 27 September 1993 on the coordination of certain rules concerning copyright and rights related to copyright applicable to satellite broadcasting and cable retransmission, OJ L 248, 15-21.

Protection	Object	Restricted acts	Relevant exceptions
Ordinary copyright	A 'work' (i.e. a person's expression of an idea resulting in an intellectual creation).	Directive 2001/29/EC Articles 2-4 in addition to Directive 92/100/EEC[137] Article 5 The acts of 'reproducing', 'communicating to the public', 'distributing', 'lending' and 'renting' in relation to embodiments of the 'work'	- Temporary technical reproductions (Directive 2001/29/EC Article 5(1)) - Public security (Directive 2001/29/EC Article 5(3)(e)
Database copyright	A 'work' by reason of the selection or arranging of the contents of a database resulting in the author's own intellectual creations. (Directive 96/9/EC Article 1(2) a database is a collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means.)	Directive 96/9/EC Article 5 in addition to Directive 92/100/EEC Article 5: The acts of 'reproducing', 'adapting', 'distributing', 'communicating to the public', 'lending' and 'renting' in relation to the selection or arrangement	- Access and normal use by a lawful user (Directive 96/9/EC Article 6(1) - Public security (Directive 96/9/EC Article 6(c))
Database sui generis right	Directive 96/9/EC Article 7(1) The qualitatively and/or quantitatively substantial investment in obtaining, verifying or presenting the contents of a 'database' to prevent extraction and/or re-utilization of the whole or of a substantial part, evaluated qualitatively and/or quantitatively, of the contents of that database. (Directive 96/9/EC Article 1(2) a database is a collection of independent works, data or other materials arranged in a	Directive 96/9/EC Article 7(2) The acts of 'extracting' and 're-utilising' in relation to the whole or substantial parts of the content of the 'database'	- Use of insubstantial parts (Directive 96/9/EC Article 8(1) - Public security (Directive 96/9/EC Article 9(c))

[137] Council Directive 92/100/EEC of 19 November 1992 on rental right and lending right and on certain rights related to copyright in the field of intellectual property (OJ L 346, 27.11.1992, p. 61). Directive as amended by Directive 93/98/EEC.

Protection	Object	Restricted acts	Relevant exceptions
	systematic or methodical way and individually accessible by electronic or other means.)		

Table 5. Intellectual Property

Thus the question becomes whether the act of information sharing would constitute a breach of the IP holder's rights. It appears clear that under the terms of the protection for ordinary and database copyright such an action would be a breach. Indeed both ordinary and database copyright grant the right holder an exclusive power over the 'reproducing', 'communicating to the public', 'distributing', 'lending' and 'renting' of their work.

According to Article 2 of the Information Society Directive and Article 5(a) of the Database Directive, reproducing refers to any direct or indirect, temporary or permanent reproduction, in whole or in part and by any means and in any form. In principle this broad notion of 'reproducing', also covers the often short-lived duplications necessary for a computer to perform a task. In addition, 'reproducing' is usually taken to cover 'adapting' and 'translating'.

The notion of 'communicating to the public' is covered by Article 3 of the Information Society Directive. This notion must be understood broadly and according to recital 23 should cover and transmission or retransmission by wire or wireless means. However, Article 5(d) of the Database Directive, unlike the equivalent provision in the Information Society Directive, makes no reference to the whether members of the public can choose individually where they access the protected work. This is complicated as Article 1(2) of the information Society Directive explicitly provides that it does not amend the earlier Database Directive unless expressly indicated and such an indication is missing in relation to this provision. Nevertheless, in a reasonable interpretation one should consider this to be the case.

Distributing refers to any form of distribution to the public by sale or otherwise of copies of the 'work.' 'Renting' and 'lending' are also subject to the authorisation of the right holder. 'Renting' is defined as the making available for use, for a limited period of time and for direct or indirect economic or commercial advantage.[138] 'Lending' refers to the making available for use, for a limited period of time and not for direct or indirect economic or commercial advantage, through establishments which are accessible to the public.[139] Finally, it is important to make one distinction regarding database copyright. From Article 3 it is the selection and arrangement of the contents of the database that constitutes the author's own intellectual creation and that this is without prejudice to any rights subsisting in the contents themselves. This does not mean that the database copyright extends to contents but rather

[138] Directive 2006/115/EC of the European Parliament and of the Council of 12December 2006 on rental right and lending right and on certain rights related to copyright in the field of intellectual property (codified version) *OJ* L 376, 27 December 2006 (hereinafter "Rental and Lending Directive (2006)"), Article. 2.1.

[139] Ibid., Article 2.1(b).

that any information contain in the database may also have an independent protection.

Under Article 7(1) of the sui generis database right two categories of acts - 'extracting' and 're-utilising' (as noted in the table) - are subject to authorisation. From Article 7(2) these refer to:

> "(a) 'extraction' shall mean the permanent or temporary transfer of all or a substantial part of the contents of a database to another medium by any means or in any form;
>
> (b) 're-utilization' shall mean any form of making available to the public all or a substantial part of the contents of a database by the distribution of copies, by renting, by on-line or other forms of transmission. The first sale of a copy of a database within the Community by the right holder or with his consent shall exhaust the right to control resale of that copy within the Community;"

These concepts are only in relation to acts covering the whole or substantial part (either qualitatively or quantitatively) of the content of a 'database'. Indeed, as can be thus inferred this sui generis right does then not give the right holder an exclusive power over individual elements of the database. However, from Article 7(5) the systematic and repeated extraction or re-utilisation would be deemed an infringement as soon such activities result in cumulatively a substantial part.[140]

In the context of ECOSSIAN, and hence information sharing in disaster situations, it appears clear that IP infringements may occur. This is an area which needs consideration as one must be aware of possible breaches which may occur if certain types of information are duplicated or disseminated without the right holder's permission. Significantly, as noted by the ENISA report on encouraging information exchange between CERTs:

> "The scope of application of these rights can be very broad, with the line between protection and unprotected information being particularly blurred in the case of copyrights… and *sui generis* database rights… as these do not require any prior registration."[141]

There are exceptions which may have potential relevance and thus legitimise such sharing. It should be noted that there are several other exceptions that are not discussed as they are not relevant in the context of information sharing in disaster situations.

4.2.1 Exceptions

In relation to ordinary copyright exceptions the table notes two as having particular significance. The first is the mandatory exception stipulated by Article 5(1) the Information Society Directive relating to temporary technical reproductions. This exception provides that

> "Temporary acts of reproduction referred to in Article 2, which are transient or incidental [and] an integral and essential part of a technological process and whose sole purpose is to enable:

[140] For more see: C-203/02 (*BHB v. William Hill*) European Court of Justice 9 November 2004, para 89.

[141] ENISA, 'A flair for information sharing- encouraging information exchange between CERTs' (2011) accessed on 01/03/2015 at: http://www.enisa.europa.eu/activities/cert/support/fight-against-cybercrime/legal-information-sharing

> (a) a transmission in a network between third parties by an intermediary, or
>
> (b) a lawful use
>
> of a work or other subject-matter to be made, and which have no independent economic significance, shall be exempted from the reproduction right provided for in Article 2."

The precise scope of this exception has given rise to debate.[142] Nevertheless, it is clear that this is exception may have relevance if the sharing of information requires the creation of temporary reproductions of a work as part of the technological process needed to transmit the information.[143]

Specifically in relation to database copyright the first relevant exception is the mandatory one provided by Article 6(1) of the Database Directive. This provides that:

> "The performance by the lawful user of a database or of a copy thereof of any of the acts listed in Article 5 which is necessary for the purposes of access to the contents of the databases and normal use of the contents by the lawful user shall not require the authorization of the author of the database. Where the lawful user is authorized to use only part of the database, this provision shall apply only to that part."

In essence, this provides that the lawful user of a database does not need the right holder's permission to perform acts that are necessary for the purposes of access and normal use of the contents of the database. However, this "lawful user" condition does present some uncertainty as there is debate as to whether this refers to:

> 1) only those granted a licence by the right holder;
>
> 2) to anyone who lawfully acquired an embodiment of the 'database'; or
>
> 3) also to everyone acting within the limits of a normal use of an embodiment of the 'database' regardless whether this embodiment was acquired lawfully.[144]

Regarding the *sui generis* database right the mandatory exception as provided for by Article 8(1) of the Database Directive provides that in relation to a

> "database which is made available to the public in whatever manner may not prevent a lawful user of the database from extracting and/or re-utilizing insubstantial parts of its contents, evaluated qualitatively and/or quantitatively, for any purposes whatsoever. Where the lawful user is authorized to extract and/or re-utilize only part of the database, this paragraph shall apply only to that part."

This exception reflects the discussion *supra* that the Database Directive does not grant rights to unsubstantial parts of the database.

---

[142] See: S. Clark, "Just browsing? An analysis of the reasoning underlying the Court of Appeal's decision on the temporary copies exemption in Newspaper Licensing Agency Ltd v Meltwater Holding BV"(*E.I.P.R.* 2011) 727.

[143] See also Directive 2001/29/EC Recital 33

[144] See: V. Vanovermeire, "The Concept of the Lawful User in the Database Directive" (*I.I.C.* 2000) 63-81.

The final exception is common to all and relates to that of public security as provided for by Article 5(3)(e) the Information Society Directive and Articles 6(1)(c) and 9(1)(c) of the Database Directive. Member States such as Germany[145] and the UK[146] have implemented such an exception in contrast to Belgium and Ireland. However, in their review of the current implementation in Ireland the Copyright Review Committee recommended such a provision.[147]

The table below provides an overview of the analysis provided above.

Req. number	Description	Importance* (M/O)	Relevant for Level			Comment
			O-SOC	N-SOC	E-SOC	
GReq. 5.1	The authorisation of IP right holder should be sought in relation to any protected work (most likely copyright)	M	X	X	X	
GReq. 5.2	If you are using more than an unsubstantial part of a database seek authorisation from the sui generis database owner	M	X	X	X	
GReq. 5.3	Consult national IP specialist in order to adequately assess the applicable exemptions/exceptions	M	X	X	X	

*M – mandatory; O – optional

** Work Packages where this requirement should be implemented

Table 6. Requirements in IP

[145] Section 45, 2) German Copyright Law

[146] Sections 45-50 UK Copyright

[147] Modernising Copyright A Report prepared by the Copyright Review Committee for the Department of Jobs, Enterprise and Innovation www.enterprise.gov.ie/en/Publications/CRC-Report.pdf

4.3 Confidentiality obligations

In addition to the data protection and intellectual property law obligations specified above it is significant to note that there may also be confidentiality obligations towards third parties which may have a restricting impact on the sharing of information in disaster situations. For example a third party may make its voluntary cooperation subject to a confidentiality agreement in the form of a non-disclosure agreement. Even without the adoption of formal contractual obligations trade secrecy rules may apply. Trade secrets are pieces of information of an economic value that are not generally known and are treated as confidential within a company.[148]

The European Commission has proposed a Directive on the protection of trade secrets which aims to build upon the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPs) agreement as currently the approach within the EU in fragmented vis-a-vis the level and type of protection available across the Member States. Indeed aside from the applicability of criminal law, Member States use a variety of other legal instruments. As noted in the impact assessment attached to the proposed Directive, Member States

> "use different types of legal instruments: a trade secret specific law (Sweden); Intellectual Property Codes (Portugal and Italy); unfair competition laws (several Member States); a few Member States only rely on general tort law (or breach of confidence law for common law Member States) or contract law only. Labour laws of most Member States are partially addressing the issue in so far as they may impose on employees a duty of loyalty towards their employers, including explicitly (or implicitly) the duty not to disclose their employers' trade secrets."[149]

Accordingly, the Directive aims to establish common definitions procedures and sanctions. Moreover, from Article 1 the Directive aims at harmonising approaches in order to protect such information from unlawful acquisition, use and disclosure.

The Directive defines trade secrets as,

> "information which meets all of the following requirements: (a) is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question; (b) has commercial value because it is secret; (c) has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret."

This definition is broad but mirrors the one provided in the TRIPs agreement. Article 3 outlines the circumstances in which unlawful acquisition, use or disclosure may occur. This states that unauthorised access will occur if the trade secret is accessed or copied without authorisation, or obtained through theft, bribery, deception, the breach or inducement to breach a confidentiality agreement or any other behaviour that "is considered contrary to

[148] Commission Staff Working Document Impact Assessment accompanying the document proposal for a Directive of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure Brussels, 28.11.2013 SWD(2013) 471 final accessed on 23/04/2015 at: eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013SC0471&from=EN.

[149] Ibid.

honest commercial practices."[150] Any use or disclosure of information obtained through such means will also been considered unlawful.[151] However, it has been noted that,

> "The Directive recognises that trade secrets should be shared in certain circumstances to foster innovation, research and development. As a result it is provided that an acquisition of a trade secret will be lawful in circumstances of independent discovery, reverse engineering and if "honest commercial practices" were exercised. It also permits disclosure to protect a worker's rights to information and consultation, to protect a legitimate interest or reveal illegal activities."

In relation to the context of information sharing in disaster situations any exchange will have to respect that such activities may be subject to confidentiality agreements or trade secrets. Developments in relation to the harmonisation of the approaches towards trade secrets must be watched closely and will be subject to further analysis in the second iteration of this Deliverable.

The table below provides an overview of the analysis provided above.

Req. number	Description	Importance* (M/O)	Relevant for Level			Comment
			O-SOC	N-SOC	E-SOC	
GReq. 6.1	All relevant legal persons should abide by any contractual obligations not to share confidential information as contained for example in Non-disclosure agreements.	M	X	X	X	
GReq. 6.2	Even in the event of a lack of a specific contractual obligation legal persons should be wary not to share commercially sensitive information except with express authorisation and approval.	M	X	X	X	
GReq. 6.3	National approaches to trade secrets should be consulted	M	X	X	X	

[150] Proposed Directive on the Protection of Trade Secrets Article 3(2).

[151] Ibid. Article 3(3).

Req. number	Description	Importance* (M/O)	Relevant for Level			Comment
			O-SOC	N-SOC	E-SOC	
	and developments in relation to proposed amendments should be consulted following the adoption of legislation.					

*M – mandatory; O – optional

** Work Packages where this requirement should be implemented

Table 7. Confidentiality obligations

Chapter 5 Impact on ECOSSIAN

The purpose of this chapter is to apply the requirements highlighted above to the context of ECOSSIAN. This will involve an application of the identified requirements to the use cases outlined in Task 1.2 'Use case definitions' (D1.5 'Use case scenario report') in WP1. A preliminary draft of these use cases has been developed in advance of the deadline (not due until month 12) as agreed by the partners for their use in deliverables such as this one (also submitted in month 12). As such this will be a continuation of the analysis as completed in Deliverable 7.2 'Legal Requirements' which focused on the application of the data protection requirements developed in relation to 1° Threat detection and analysis 2° and Information sharing. As the second of these overlaps with our current analysis there will be some degree of similarity in order to develop an indicative examination and thus a list of applied requirements.

As is evident from the examination thus far, this Deliverable has been divided into the following chapters, CI protection and the disaster management framework, Disaster situations: the legal framework for information sharing, Legal barriers to effective information sharing. From these Chapters it is clear that certain aspects of the analysis have particular influence in the context of ECOSSIAN. For instance, the potential law enforcement competence of the N-SOC and E-SOC levels may have a clear effect on the procedures for sharing in the context of criminal investigations. Moreover, regarding the legal barrier to effective information sharing it is clear that the operating of the ECOSSIAN system should take into account the data protection, intellectual property and confidentiality issues. As described in D7.2 'Legal requirements' this can be represented in the form of applied requirements in relation to the data protection issues and the implementation of the privacy by design principle. These applied requirements are represented in the following table:

Applied Req.	Description	Relevant general req.
AReq. 1.1	All communications should be encrypted	GReq. 4.5, GReq. 1.2, GReq. 3.1
AReq. 1.2	Personal data are only transmitted as frequently as necessary for the system to operate and any such transfer should be encrypted and anonymised	GReq. 4.5, GReq. 1.2, GReq. 3.1
AReq. 1.3	Systems should be designed to ensure that even where personal data are transmitted, any data elements which are not necessary to fulfil the purpose of the transmission are filtered out or removed.	GReq. 4.4.2, GReq. 4.4.3
AReq. 1.4	Systems should be designed so as to allow access to the transferred personal data only to the extent necessary for the role being	GReq. 4.5

Applied Req.	Description	Relevant general req.
	performed.	
AReq. 1.5	If possible, systems should be designed in separate compartments; this strategy calls for distributed processing instead of centralised solutions; in particular the ENISA suggests to store data in separate database, and these databases should not been linked.	GReq. 4.5

Table 8. Applied Requirements Table I

In relation to the IP and confidentiality issues a similar analysis can be made. It should be noted that in the context of ECOSSIAN these issues are not only relevant to the sharing of information by the O-SOC but also in the sharing of information downstream from the E-SOC and N-SOC levels to the relevant (and potentially affected) O-SOCs. Any such sharing will have to comply with IP and confidentiality requirements. Moreover, the IP of all third parties will also have to be respected.

The applied requirements derived as examples from this analysis are highlighted in the following table.

Applied Req.	Description	Relevant general req.
AReq. 2.1	All entities utilising the ECOSSIAN system should licence the use of any IP works being shared within the purposes of critical infrastructure protection.	GReq. 5.1, GReq. 5.2, GReq. 5.3
AReq. 2.2	All information shared through ECOSSIAN should automatically be treated as confidential.	GReq. 6.1, GReq. 6.2, GReq. 6.3
AReq. 2.3	All unnecessary information that is transferred should be deleted and should not be used for non-critical infrastructure protection purposes.	GReq. 5.1, GReq. 5.2, GReq. 6.1, GReq. 6.2
AReq. 2.4	Systems should be designed so as to only allow access to select persons to reduce the confidentiality concerns.	GReq. 6.1, GReq. 6.2, GReq. 6.3

Table 9. Applied Requirements Table II

Chapter 6 Guidelines

Following the above discussion the table provided *infra* indicates some key recommendations for the implementation of the legal requirements in the context of information sharing in disaster situations. These implementation guidelines are not exhaustive and have been deciphered from the analysis provided.

Guid. No.	Description	Associated Req.	Comment
Guid. 1	Identify and coordinate with the relevant national critical infrastructure protection authority.	GReq. 1.1, 1.2, 1.3	
Guid. 2	Consult specific national laws for reporting requirements and consider the overlap between disaster management and critical infrastructure protection frameworks and agencies.	GReq. 2.1, 2.2, 2.3, 3.1, 3.2	Due to the level of disparity, this consultation is necessary in order to decipher the relevant obligations.
Guid. 3	Refer to the specific privacy and data protection implementation guidelines described in D7.2 'Legal requirements'.		This would ensure a legally compliant ECOSSIAN solution.
Guid. 4	Conduct a privacy and data protection impact assessment.	Requirements as specified in Table 4 Data Protection Requirements.	This ensures that the fundamental rights to data protection and privacy of the data subjects concerned are sufficiently taken into account.
Guid. 5	Conduct impact assessments regarding IP rights.	Requirements as specified in Table 6 Requirements in IP.	This allows the identification of any IP rights holders.

Guid. No.	Description	Associated	Comment
Guid. 6	Designate specific person(s) with the authority to reveal trade secrets in the event of a disaster.	GReq. 6.1, 6.2, 6.3	This avoids confusion amongst employees, and a defined operational structure creates a clear division of responsibilities.
Guid. 7	Integrate non-disclosure agreements for all employees above a certain level with access to sensitive information and provide guidance to clarify responsibilities.	GReq. 6.1, 6.2, 6.3	

Table 10. Guidelines

Chapter 7 Conclusion

To conclude, this deliverable has outlined the requirements and policies associated with information sharing in disaster situations in the context of ECOSSIAN. It has built upon the work completed in D7.1 and D7.2 and has provided insights into the application of the general requirements provided for by the legislation. Furthermore, it has also provided insights in the form of requirements and guidelines. Reference should be made to the specific tables provided in the deliverable. The analysis provided in this Deliverable will be supplemented in D7.7 'Information sharing policies in disaster situations - Version 2' which will assess the legislative reforms currently ongoing and examine their impact.

Chapter 8 List of Abbreviations

CERT	Computer Emergency Response Team
CI	Critical Infrastructure
CII	Critical Information Infrastructure
CIP	Critical Infrastructure Protection
CIIP	Critical Information Infrastructure Protection
CIWN	Critical Infrastructure Warning Information Network
DAE	Digital Agenda For Europe
DPA	Data Protection Act
ECI	European Critical Infrastructure
ECHR	European Convention of Human Rights
EPCIP	European Programme for Critical Infrastructure Protection
ENISA	European Network and Information Security Agency
NIS	Network Information Security

Chapter 9 Bibliography

9.1 Primary sources

9.1.1 Legislation

Convention on Cybercrime CETS No.: 185 accessed on 21/01/2015 at: conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG

European Convention on Mutual Assistance in Criminal Matters Strasbourg, 20.IV.1959 accessed on 24/03/2015 at: conventions.coe.int/Treaty/en/Treaties/Html/030.htm

Schengen Agreement of 1985.

Council Directive 92/100/EEC of 19 November 1992 on rental right and lending right and on certain rights related to copyright in the field of intellectual property (OJ L 346, 27.11.1992, p. 61). Directive as amended by Directive 93/98/EEC.

Council Resolution of 14 May 1992 on increased protection for copyright and neighbouring rights [1992] OJ C138/1; Rental lending and related rights Directive; and Treaty establishing EEA.

Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union (2000/C 197/01).

Council Decision 2001/792/EC, Euratom of 23 October 2001 establishing a Community mechanism to facilitate reinforced cooperation in civil protection assistance interventions, *OJ L* 297, 15.11.2001, 7.

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

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

Directive 2003/98 of November 17, 2003 on the re-use of public sector information [2003] OJ L345/90.

Council Framework Decision 2003/577/JHA of 22 July 2003 on the execution in the European Union of orders freezing property or evidence OJ L 196 45–55.

Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems OJ L 69, 16.3.2005, 67–71.

Directive 2006/115/EC of the European Parliament and of the Council of 12December 2006 on rental right and lending right and on certain rights related to copyright in the field of intellectual property (codified version) *OJ* L 376, 27 December 2006 (hereinafter “Rental and Lending Directive (2006)”), Article. 2.1.

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.

Council Framework Decision 2008/978/JHA of 18 December 2008 on the European evidence warrant for the purpose of obtaining objects, documents and data for use in proceedings in criminal matters OJ L 350 72–92.

Proposal for a Directive of the European Parliament and of the Council amending Directive 2003/98/EC on re-use of public sector information, Interinstitutional File: 2011/0430 (COD).

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

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 OJ L 218, 14.8.2013 8–14

Decision No 1313/2013/EU of the European Parliament and of the Council of 17 December 2013 on a Union Civil Protection Mechanism, *OJ L* 347, 20 December 2013, 924–947.

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

'Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union' COM/2013/048 final - 2013/0027 (COD).

9.1.2 Case law

Case C-13/00 *Commission v Republic of Ireland* (ECJ 19 March 2002).

C-203/02 (*BHB v. William Hill*) European Court of Justice 9 November 2004, para 89.

9.2 Secondary Sources

Angelini M., Arcuri M.C., et al., 'Italian Cyber Security Report - Critical Infrastructure and Other Sensitive Sectors Readiness', (2013), 24.

Article 29 Working Party Opinion 06/2013 on open data and public sector information ('PSI') reuse, adopted on June 5, 2013.

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

Ateniese G., Baldoni R. et al., 'Critical Infrastructure Protection: Threats, Attacks and Countermeasures', (2014), Tenace Project, 13.

Boin A., Rhinard M. and Ekengren M., 'Managing Transboundary Crises: The Emergence of European Union Capacity (2014) Journal of Contingencies and Crisis Management

British Institute of International and Comparative Law, 'Analysis of Law in the United Kingdom pertaining to Cross-Border Disaster Relief' 30 June 2010, 27, retrieved from http://www.ifrc.org/PageFiles/93649/idrl-uk-cross-border-analysis-0810.pdf.

Clark S., 'Just browsing? An analysis of the reasoning underlying the Court of Appeal's decision on the temporary copies exemption in Newspaper Licensing Agency Ltd v Meltwater Holding BV' (2011) E.I.P.R. 727.

Commission Staff Working Document Impact Assessment Accompanying the document proposal for a Directive of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure Brussels, 28/11/2013 SWD(2013) 471 final accessed on 23/04/2015 at: eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013SC0471&from=EN

Commission Staff Working Document Accompanying document to the Proposal for a Council Decision on creating a Critical Infrastructure Warning Information Network (CIWIN) {COM(2008) 676 final} {SEC(2008) 2702} accessed on 22/01/2015 at: ec.europa.eu/smart-regulation/impact/commission_guidelines/docs/sec_2008_2701_ia_ciwin_en.pdf.

Clifford D., Spangaro A., Ricci A., and Van Der Sype Y.S., 'ECOSSIAN D7.2 Legal requirements' (2015).

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

'Data Protection and Sharing – Guidance for Emergency Planners and Responders' February 2007, available at: http://www.cabinetoffice.gov.uk/media/132709/dataprotection.pdf.

De Bruijne M. and van Eeten M., 'Systems that should have failed: Critical Infrastructure Protection in an Institutionally fragmented environment' (2007) 15 Journal of Contingencies and Crisis Management 18-29.

De Capitani E. and Peers S., 'The European Investigation Order: A new approach to mutual recognition in criminal matters' accessed on 23/04/2015 at: eulawanalysis.blogspot.com/2014/05/the-european-investigation-order-new.html

de Hert P. and Papakonstantinou V., 'The Data Protection Framework Decision of 27 November 2008 regarding police and judicial cooperation in criminal matters – A modest achievement however not the improvement some have hoped for', Computer Law & Security Review 25 (2009): 403-414.

Dos Santos C.et al, 'LAPSI Policy Recommendation N. 4: Privacy and Personal Data Protection' LAPSI Working Group 2: Privacy Aspects of PSI, available at: http://www.ivir.nl/publicaties/download/1098 [last accessed December 3, 2014].

European Commission, *Belgium - Disaster management structure Vademecum - Civil Protection,* last update 10 July 2014, retrieved from http://ec.europa.eu/echo/files/civil_protection/vademecum/be/2-be-1.html#lega.

European Commission, *France - Disaster management structure Vademecum - Civil Protection,* last update 10 July 2014, retrieved from http://ec.europa.eu/echo/files/civil_protection/vademecum/fr/2-fr-1.html#lega

European Commission, *Ireland - Disaster management structure Vademecum - Civil Protection,* last update 10 July 2014, retrieved from http://ec.europa.eu/echo/files/civil_protection/vademecum/ie/2-ie-1.html#lega

European Commission, *United Kingdom - Disaster management structure Vademecum - Civil Protection,* last update 10 July 2014, retrieved from http://ec.europa.eu/echo/files/civil_protection/vademecum/uk/2-uk-1.html#over.

ENISA, 'A flair for information sharing- encouraging information exchange between CERTs' (2011) accessed on 01/03/2015 at: http://www.enisa.europa.eu/activities/cert/support/fight-against-cybercrime/legal-information-sharing

ENISA, 'European Public Private Partnership for Resilience (EP3R)' accessed on 03/02/2015 at: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/european-public-private-partnership-for-resilience-ep3r

ENISA, 'The Directive on attacks against information systems A Good Practice Collection for CERTs on the Directive on attacks against information systems' (P/28/12/TCD 2013).

Fritzan A., Ljungkvist K., Boin A. and Rhinard M., 'Protecting Europe's Critical Infrastructures: Problems and Prospects' (2007) 15 Journal of Contingencies and Crisis Management 30-41.

French Red Cross, 'Analysis of Law in the EU Pertaining to Cross-Border Disaster Relief (EU IDRL Study) - Country Report by the French Red Cross' (August 2010) 18, retrieved from http://www.ifrc.org/PageFiles/93645/country-report-france-082010.pdf.

German Red Cross, 'Analysis of Law in the EU Pertaining to Cross-Border Disaster Relief (EU IDRL Study) - Country Report Red Cross Report' May 2010, 6, retrieved from https://www.ifrc.org/Global/Publications/IDRL/country%20studies/IDRL-Report_GerRC_May2010.pdf.

Janssen K., 'The influence of the PSI directive on open government data: An overview of recent developments' (2011) 28 Government Information Quarterly 446.

Lazari A., 'European Critical Infrastructure Protection', (2014 Springer) 68.

Modernising Copyright a Report prepared by the Copyright Review Committee for the Department of Jobs, Enterprise and Innovation www.enterprise.gov.ie/en/Publications/CRC-Report.pdf

O'Donoghue C., Nagle T.J. and Nielsen Czuprynski C., *EU Proposed Directive on Network and Information Security*, 13 February 2013, http://www.reedsmith.com/EU-Proposed-Directive-on-Network-and-Information-Security-02-13-2013/

Position Paper of the TNCEIP on EU Policy on Critical Energy Infrastructure Protection (November 2012) accessed on 22/01/2015 at: http://ec.europa.eu/energy/sites/ener/files/documents/20121114_tnceip_eupolicy_position_paper.pdf

Suter M., 'PPPs in Security Policy: Opportunities and limitation' (2012), 1, retrieved from http://www.css.ethz.ch/publications/pdfs/CSS-Analysis-111-EN.pdf.

Tikk E., Kaska K.and Vihul L., 'International Cyber Incidents Legal Considerations 2010 Cooperative Cyber Defence Centre of Excellence 80. https://ccdcoe.org/publications/books/legalconsiderations.pdf

Vanovermeire V., "The Concept of the Lawful User in the Database Directive" (*I.I.C.* 2000) 63-81.

Willis H., Lester G. and Treverton G., 'Information sharing for infrastructure risk management: Barriers and solutions (2009) 24 Intelligence and National Security 339-365.