D7.1

Analysis of the applicable legal framework

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

Deliverable type:	Report
Deliverable reference number:	ICT-607577 / D7.1/ 1.0
Work package contributing to the deliverable:	WP 7
Due date:	Nov 2014 – M06
Actual submission date:	1st December, 2014

Responsible organisation:	KU Leuven
Editor:	Damian Clifford
Dissemination level:	PU
Revision:	1.0

Security Sensitivity Committee Review performed on:	28th November, 2014
Comments:	

Abstract:	This deliverable provides a detailed analysis of the applicable legal framework through an assessment of the EU framework and an analysis of national implementations.
Keywords:	Privacy, Data Protection, Critical Infrastructure Protection, Security.

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

Editor

Damian Clifford (KU Leuven)

Contributors (ordered according to beneficiary numbers)

Annarita, Ricci (UNIBO)

Giusella Dolores, Finocchiaro (UNIBO)

Luisa, Proenca (PJ)

Yung Shin Van Der Sype (KUL)

Karine e Silva (KUL)

.

Executive Summary

The purpose of this Deliverable is to set out the legal framework applicable to the European COntrol System Security Incident Analysis Network (herein ECOSSIAN) project. The document provides a detailed assessment of the security, privacy and data protection framework and provides an initial examination that will be furthered developed in the future Work Package 7 Deliverables. The analysis is divided into two main parts namely: first, an assessment of the current and proposed legislation at an EU level and second, an examination of the implementation of the Critical Infrastructure Protection Mechanisms and Privacy and Data Protection Framework at a National Level.

As described in Chapter 2, there is a wide array of EU instruments with relevance to the operations to be performed in the ECOSSIAN project. Currently, the protection of Critical Infrastructures is concentrated on the classification and designation of European Critical Infrastructures. The deliverable analyses this protection and the thus the Directive 2008/114/EC. In addition the proposed NIS Directive is assessed in detail. In the Data Protection and Privacy analysis the current framework is analysed in detail and the potential impact of Proposed Data Protection Regulation is examined. It is also important to highlight the potential changes regarding notification requirements for data breaches as contained in the proposed Data Protection Regulation. If adopted this would impose positive action on behalf of data controllers.

Chapter 3 provides the country level analysis and the implementations in the United Kingdom, Italy, Ireland, France, Portugal and Belgium are highlighted in detail. As will become apparent in the analysis each of these countries has key peculiarities in the implementation of the EU legislative framework. The assessment of the implementation in these countries is completed through the selection of 4 standardised questions. These are as follows:

1. Regarding the detection and information sharing processes relating to the protection of Critical Infrastructures, what are the key variations in the national implementation of thresholds for the application of the Data Protection framework in the context of ECOSSIAN?
2. What are the key peculiarities of the relevant national provisions which ensure legal compliance legitimising the processes and operations which may be undertaken in relation to threat detection as a part of the activities to be performed by ECOSSIAN?
3. In the application of the national data protection framework to the specific parameters of the project, is the data controller subject to particular guarantees, liabilities or requirements (e.g. administrative/security) which deviate from those under the terms of the Directive and may affect the implementation of ECOSSIAN?
4. At its core ECOSSIAN aims to facilitate the sharing of information. Are there any specific concerns at national level regarding public-private sector cooperation or vis-a-vis the transfer of data (and more specifically cross-border data transfer) in the context of the project?

As is seen in the conclusion section of Chapter 3, the analysis highlights the disparities that exist between the Member States and acts as an overall flavouring of the potential disparity in the 28 Member States. The examination highlights the specific need for an awareness of the variance in implementation at a national level. This has a specific impact not only on the rules for the implementation of ECOSSIAN at an O-SOC and N-SOC level but also on the selection of country in which the E-SOC as a data subject will be located. This is an issue which should be weighted carefully.

Contents

Chapter 1 Introduction 1
1.1 ECOSSIAN Context 1
Critical Infrastructures 1
i. Critical Infrastructure versus Critical Information Infrastructure 1
Application to and Assessment of the Project Sectors 2
i. Energy 2
ii. Transportation 2
iii. Finance 3
iv. ICT Infrastructure 3
1.2 Methodology of the Analysis 3
Chapter 2 Applicable EU framework 4
2.1 European Programme for Critical Infrastructure Protection (EPCIP) 4
2.2 Directive 2008/114/EC 5
Legal Basis for Critical Infrastructure protection 5
Identification 6
Critical Infrastructure and European Critical Infrastructure 6
Designation of European Critical Infrastructures 7
Protection 8
Reporting 8
2.3 Critical Infrastructure Warning Information Network (CIWIN) 8
2.4 Sector Specific Considerations 9
Energy 9
Transport 9
Finance 10
2.5 European Security Framework 10
The Digital Agenda for Europe (DAE: Trust and Security) 10
Directive on attacks against information systems (2013/40/EU) 11
Proposed NIS Directive 12
i. Current Status 12
ii. Applicable provisions 13
2.6 Privacy and Data Protection Framework 14
Critical Infrastructure attacks and threat identification 14
Information Sharing Platforms 14
Fundamental introduction – Privacy and Data Protection in the Primary Sources 15

Directive 95/46/EC....16
i. Definitions: personal data and data processing....17
ii. Data Processing....19
iii. The Controller....20
iv. Legal grounds for legitimate processing....21
v. Lawful processing....24
vi. Data subject's rights....26
The e-Privacy Directive....27
Proposed Data Protection Regulation....28
i. Introduction....28
ii. Data subject's rights....29
iii. Security of processing....30
The Proposed Police and Criminal Justice Data Protection Directive....34
2.7 EU Level Conclusions.... 35
Chapter 3 Country Level Analysis.... 36
3.1 Country Report – United Kingdom.... 36
Thresholds for the application of the Data Protection framework....39
Legitimising the Processes and Operations - Threat Detection....40
Guarantees, Liabilities or Requirements....44
Facilitating Inforamtion Sharing....45
3.2 Country Report – Italy.... 48
Thresholds for the application of the Data Protection framework....51
Legitimising the Processes and Operations - Threat Detection....53
Guarantees, Liabilities or Requirements....54
Facilitating Inforamtion Sharing....56
3.3 Country Report - Ireland.... 57
Thresholds for the application of the Data Protection framework....60
Legitimising the Processes and Operations - Threat Detection....61
Guarantees, Liabilities or Requirements....64
Facilitating Inforamtion Sharing....66
3.4 Country Report - France.... 68
Thresholds for the application of the Data Protection framework....70
Legitimising the Processes and Operations - Threat Detection....71
Guarantees, Liabilities or Requirements....74
Facilitating Inforamtion Sharing....76
3.5 Country Report – Portugal.... 77
Thresholds for the application of the Data Protection framework....79
Legitimising the Processes and Operations - Threat Detection....79

Guarantees, Liabilities or Requirements 81
Facilitating Inforamtion Sharing 82
3.6 Country Report – Belgium 83
Thresholds for the application of the Data Protection framework 85
Legitimising the Processes and Operations - Threat Detection 85
Guarantees, Liabilities or Requirements 86
Facilitating Inforamtion Sharing 87
3.7 Country Level Analysis Conclusions 88
Chapter 4 Conclusion 89
Chapter 5 List of Abbreviations 90
Chapter 6 Bibliography 91
6.1 Primary Sources 91
Legislation 91
i. EU 91
ii. UK 92
iii. Italy 92
iv. Ireland 92
v. France 93
vi. Portugal 93
vii. Belgium 94
Case law 94
i. United Kingdom 94
ii. Ireland 95
iii. Italy 95
iv. France 95
Secondary Sources 95
i. Opinions/Reports/Best Practice Documentation 95
ii. Books/Articles 98
iii. Websites 99

Chapter 1 Introduction

This Deliverable is responsible for laying the foundations of the legal framework applicable in the context of the European COntrol System Security Incident Analysis Network (herein ECOSSIAN) project. It provides an outline of the relevant legal framework more specifically relating to security, data protection and privacy. This document is the result of a joint effort between Policia Judiaciara (PJ), University of Bologna (UNIBO) and the University of Leuven (KUL). The following sections explore the main legal instruments applicable to the ECOSSIAN environment based on the Project Proposal (DoW), D1.1 State of the Art and D1.5 Use Cases (draft). Due to the evolving nature of the project's architecture, the results of this deliverable will be refined and verified in the future deliverables D7.2 (Legal Requirements) and D7.3 (Information Sharing Policies).

1.1 ECOSSIAN Context

ECOSSIAN aims at supplementing the detection and management of cyber security incidents and attacks on critical infrastructures. Due to the significant impact of these incidents the project has the objective of creating a pan-European early warning and situational awareness framework. In order to adequately protect Critical Infrastructures, a holistic system that can integrate the necessary functionalities and deal with the increasing demands (at a national and pan-European level) is necessary.

This section of the analysis introduces the scope of the project by outlining the applicable sectors in detail, highlighting the sector specific threats and explaining the meaning of the term Critical Infrastructure. The project aims at analysing the impact of cyber security incidents and attacks in three specific sectors namely: Energy, Transport and Finance. Each of these brings particular difficulties, however it must be acknowledged that the ubiquitous ICT sector provides some degree of continuity vis-a-vis the challenges. To begin the analysis, it is significant to outline what is meant by the term Critical Infrastructure.

Critical Infrastructures

Critical Infrastructures are essential services for the well-being of citizens. Without their adequate protection there would be serious consequences for society. We are dependent on their proper functioning. However they are vulnerable, natural disasters, criminal or terrorist attacks all have the capacity to disrupt their functioning. These infrastructures range from energy and transport installations, electricity and gas supply and ports and airports. Given the increasing interconnectivity of Europe the potential for disruption is increased. Accordingly cross-border protections are essential.

i. Critical Infrastructure versus Critical Information Infrastructure

When defining the term Critical Infrastructure it is important to acknowledge the conceptual distinction between Critical Infrastructure Protection and Critical Information Infrastructure Protection. Dunn has observed that these terms are often used interchangeably and that

there is a certain level of inconsistency in literature.[1] In essence, CIP focuses on the protection of all subsets of a nation's infrastructure whereas CIIP merely focuses on a particular subset and thus the information infrastructure. This distinction recognises that there are two elements to CI's namely; the physical element, which is easily conceptualised as the physical structure itself (or part thereof), and the intangible element which refers the information or data stored on or in the physical element. It is therefore clear that CIIP forms a part of the overall CI protections. Given the increasingly ubiquitous nature of computing this subset is growing in significance and is hence of clear importance in the web 2.0 era. Hence, it should be acknowledged that a sole focus on either of these categories of protection would result in vulnerabilities.

The focus of ECOSSIAN relates to sharing of information following an attack on the informational infrastructures which support proper functioning. Accordingly, the legal framework needs to be assessed in a holistic manner in order to adequately assess the applicability of the relevant legislative instruments. As such, this deliverable will refer to CIP as including CIIP and any variations of this will be expressly noted. CIP in the EU owes its historical development to the rise in terrorist activity since 9/11. National governments enhanced the protection of these assets, due to the potential knock on effects any disruption could have on society. However, it is significant to note that it is not merely terrorist activities that can have a devastating impact on the operation of a CI. Indeed other potential threats include *inter alia*, non-terrorist criminal activities and natural disasters.

Application to and Assessment of the Project Sectors

The protection of these sectors, and by extension the Critical Infrastructures contained therein, is paramount to the safeguarding of the fundamental rights of the citizens of the Union.

ii. Energy

EU energy policy aims to ensure the continuous availability of energy products and services at affordable prices and with respect to the EU's wider climate and societal goals. Efficiency is a key target for 2020 and is also a key goal in achieving the long term EU goals in relation to energy saving and the climate.[2] For the purposes of Critical Infrastructure protection this industry is divided into 3 key sectors: Electricity, Gas and Oil.

iii. Transportation

The EU transport policy owes its origins to the founding treaties due to their focus on the free flow of people (Article 45 TFEU) and goods (Articles 34 and 35 TFEU) in the completion of the single Economic market. Currently, the EU transport policy still focuses on this notion of

[1] Myriam Dunn, 'Understanding Critical Information Infrastructures: An Elusive Quest' in Myriam Dunn and Victor Mauer (eds.) International CIIP Handbook 2006 Vol. II Analyzing Issues, Challenges, And Prospects (2006 Center for Security Studies) pp. 27-53.

[2] Communication 639-2010 from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Energy 2020 A strategy for competitive, sustainable and secure energy, http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52010DC0639.

completing the internal market and the development of transport corridors and international connections. The aim is open transport mode in order to create a safer and more sustainable transport system.

iv. Finance

EU finance policy also owes its to the founding treaties through the principle of the free movement of capital (Article 63 TFEU). Accordingly, policy in this area also focuses on the development of the internal market and the connections between Member States in order to ensure and higher degree of harmonisation across the union.

v. ICT Infrastructure

Although these three sectors are clearly distinguishable the ICT infrastructure provides a link to all of these sectors. Traditionally the protection of Critical Infrastructures would have solely relied on physical security protection against attacks. However, in an era of ubiquitous computing the ICT infrastructure surrounding these infrastructures requires protection. Accordingly, in general the legal requirements associated with the protection of these systems and the issues relating to the protection of privacy and data protection remain constant and shared.

1.2 Methodology of the Analysis

The examination of the legislative instruments aimed at protecting Critical infrastructures will be set out in detail in order to give context to the Privacy and Data Protection analysis, which is the primary concern of this deliverable. In addition, it should also be acknowledged that as the current relevant EU legislative structure is in the form of Directives, each of the national implementing provisions (and the disparities therein) must be analysed. However, the analysis will first outline (Chapter 2) the provisions at an EU level before delving into a national analysis of the chosen Member States (Chapter 3).

Chapter 2 Applicable EU framework

To adequately analyse the complex legal issues associated with this project one is required to consider the broad range of applicable EU sources. Significant in this regard are the Critical Infrastructure Protection Directive, the Directive on attacks against information systems the Proposed NIS Directive, the Data Protection Framework (including the Data Protection Directive, the *lex specialis* e-Privacy Directive and the proposed Draft Data Protection Regulation). The applicability of each of these legislative provisions will be assessed in detail as applied to ECOSSIAN.

2.1 European Programme for Critical Infrastructure Protection (EPCIP)

The EPCIP was launched in 2006 with the goal of improving the protection of critical infrastructures in the EU. COM(2006) 786 originated the present EPCIP, defining subsidiarity, complementarity, confidentiality, stakeholder cooperation, proportionality and sector-by-sector approach as the guiding principles of the EPCIP. However, the Communication lacks clarity and fails to examine the nature of these key principles in detail. According to COM (2006) 786:

- *Subsidiarity*. While the principle of subsidiarity safeguards critical infrastructures (herein CI) as a national matter, it establishes the EU interests and competence in managing infrastructure that is critical from a European perspective, in the terms of the EPCIP.
- *Complementarity.* The complementarity character of the EPCIP avoids doubled work and builds upon best practices developed at country-level.
- *Confidentiality.* This principle requires information related to critical infrastructure protection (herein CIP) to be classified and restricted in access both at EU and Member State levels, to be shared in circles of trust.
- *Stakeholder cooperation.* The Stakeholder cooperation principle calls for a multisectorial approach from private and public sector to work jointly towards better protection of CI.
- *Proportionality.* EU measures and regulation will only emerge where security gaps are identified. In light of the proportionality principle, these measures will at all times be balanced against the seriousness and nature of the associated threat.
- *Sector-by-sector approach.* With this principle, the Commission established the need for tailored and customised CIP. The abovementioned principles are, therefore, to be taken into account when examining the EU framework and the basic guidelines of the EPCIP.

The legislative framework, as set forth by the Commission, included a proposal for a directive on identification and designation of European critical infrastructures, and the creation of a Critical Infrastructure Warning Information Network (herein CIWIN). The complete programme, however, also included an action plan, the creation of experts groups and further CIP information sharing processes. For the purpose of the ECOSSIAN project

and this applicable legal framework deliverable, the analysis will focus on Directive 2008/114/EC and the CIWIN initiative.

2.2 Directive 2008/114/EC

Directive 2008/114/EC aims at protecting Critical Infrastructures through 'the identification and designation of European critical infrastructures and the assessment of the need to improve their protection'. The Directive concentrates on the energy (electricity, oil and gas) and transport (road, rail, air, inland waterways and ocean and short-sea shipping and ports) sectors.[3] However, under the review process other areas may be added. Member States were required to take the necessary measures in order to be in compliance with this Directive by the 12th of January 2011.

Legal Basis for Critical Infrastructure protection

The Directive is based on Article 308 EC (now Article 352TFEU). This article requires the unanimous action from the council, acting on a proposal from the Commission (following the obtaining of consent from the European Parliament), in order to take appropriate measures to achieve an objective set out in the Treaties if the Treaties have not already provided the necessary powers. Essentially this provision provides a basis for the adoption of secondary legislation where there is no specific legal basis elsewhere in the Treaties. As the EU CIP regime focuses on issues other than mere criminal threats (e.g. natural disasters), there was no other legitimate basis on which it could have been based. If it was merely criminal Article 4(2)(f) TFEU and or Article 84 TFEU may have been better suited.

The Lisbon Treaty did introduce some developments *vis-a-vis* civil protection (see Article 6(f) and Article 196 TFEU) which could potentially form a basis for future legislative developments. However, in the context of Article 196, the Commission in a 2012 working document found that:

> 'The framework for the CIP cooperation at EU level should be subsidiary to the competences of the Member States. Measures under Article 196 TFEU, while excluding any harmonisation of Member State laws, can still establish an obligatory framework for the Union. However, participation in this framework would remain voluntary or allow the Member States a large degree of discretion in how they participate. For any measures under Article 196, the main role of the Commission is to monitor the general implementation of any legislation and to coordinate, supplement and support the Member States.'

The importance of the principle of subsidiarity and the role of the Member States is thus clear.

[3] See Annex 1 of the Directive

Identification

Article 3 of the Critical Infrastructure Directive provides that each Member State of the EU has the responsibility for the identification of their Critical Infrastructures. The MSs are required to refer to Articles 2(a) and (b) in order to correctly identify the infrastructures which come under the scope of the Directive. Article 2(a) defines what is meant by the term Critical Infrastructure for the purposes of the Directive. It states that:

> 'critical infrastructure' means an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions;

Given the applicability of the principle of subsidiarity the identification and protection of national Critical Infrastructures that only affect one MS remain outside the scope of the Directive. Accordingly, the Critical Infrastructure Directive focuses on protection so-called European Critical Infrastructures. Article 2(b) further distinguishes between Critical Infrastructures and European Critical Infrastructures and it is this distinction to which we must now turn our attention.

Critical Infrastructure and European Critical Infrastructure

As highlighted by Christer Pursiainen[4], the difficulty imposed by the tentative of creating a framework for European CI was the diluted boundary between national and transnational systems. Economic integration in the region led to increased vulnerabilities and exposure of information systems and infrastructures. A single failure in a specific CI can generate enormous societal costs. The interdependency of systems operating in different Member States with multisectorial connectivity led to increased fear amongst national and regional authorities relating to cascading effect issues was. Consequently, the menace had to be counteracted beyond state level, from an EU perspective.

In the impasse between sovereignty and subsidiarity, EU and MS agreed that only systems essentially classified as European CI (ECI) could be embraced under the EPCIP framework, all the rest remaining under national regulation. This reflects the lack of competency for the EU to act in relation to national Critical Infrastructure and hence the scope within the treaties only to harmonise legislation vis-à-vis Critical Infrastructures having an effect on more than one MS. The concept of ECI enshrined under article 2 (b) of Directive 2008/114/EC:

> (b) 'European critical infrastructure' or 'ECI' means critical infrastructure located in Member States the disruption or destruction of which would have a significant impact on at least two Member States. The significance of the impact shall be assessed in terms of cross-cutting criteria. This includes effects resulting from cross-sector dependencies on other types of infrastructure.

[4] Christer Pursiainen (2009), The Challenges for European Critical Infrastructure Protection, Journal of European Integration, vol. 31:6, 721-739, November 2009.

A major drawback of the Directive 2008/114/EC, which was already anticipated by the time of its approval, is the rather narrow concentration on the energy and transport sectors (article 3(3) and Annex 1). Recital 5, however, highlighted the need to expand and improve the sectoral application of the law, especially to include the ICT sector. On 12 June 2012, the European Parliament presented a Resolution acknowledging that the Commission was considering revising Directive 2008/114/EC to expand its scope to include the ICT sector, as well as the financial, health, food and water supply, and nuclear energy sectors.[5] However, currently and in the context of ECOSSIAN, this Directive applies to only two of the project sectors namely: transport and energy. In its current format Critical Infrastructures in the Finance sector remain outside the scope of the Directive.

Aside from the ECI identification issue, the definition of critical infrastructure at Member State level is still far from harmonised. The current trends followed by Member States include definition of critical infrastructure based on defence strategies, national emergency management and long term national traditions.[6] This variation will be highlighted further in Chapter 3.

Designation of European Critical Infrastructures

Following identification each MS is required under Article 4(1) to inform the other MS(s) 'which may be significantly affected by a potential ECI about its identity and the reasons for designating it as a potential ECI.' Article 4(2) provides that MSs are subsequently required to engage in bilateral or multilateral negotiations (where appropriate) with the other potentially affected MS(s). Any MS that believes that it could also be significantly affected may contact the Commission with a request to join these negotiations. From Article 4(3) it is clear that following these negotiations and the reaching of an agreement, the MSs will designate the infrastructure as an ECI. However, for this to be valid the acceptance of the MS on whose territory it is located is required. It is important to note that only the host MS, the MS(s) significantly reliant on the critical infrastructure and the owner/operator (i.e. only those at an appropriate security level) are allowed to be aware of this status designation. This security level clearance is also reflected in Article 9 which deals with Sensitive European critical infrastructure protection-related information. Under the terms of this provision only persons of an appropriate clearance should have access to this genre of information. This reflects the aim of only revealing information to those who require such knowledge in order to reduce risk. This information should only be used within the aims of protecting the Critical Infrastructures and it applies to both written and verbal exchanges.

[5] Resolution 2011/2284(INI) on Critical Information Infrastructure Protection - achievements and next steps: towards global cyber security

[6] Christer Pursiainen (2009), The Challenges for European Critical Infrastructure Protection, Journal of European Integration, vol. 31:6, 721-739, November 2009.

Protection

Article 5 of the Directive outlines the Operator Security plans. Essentially these provisions outline the meaning of these plans and the requirements for their effective implementation. According to Article 5(1) the OSP 'procedure shall identify the critical infrastructure assets of the ECI and which security solutions exist or are being implemented for their protection.' Annex II of the Directive indicates the minimum content to be addressed by such a procedure. This involves three distinct steps; (1) the identification of important assets, (2) the conducting of risk analyses assessing the vulnerabilities and potential impacts of various threat scenarios and (3) the identification and prioritisation of the available counter measures with a distinction between permanent and graduated security measures. The remainder of Article 5 focuses on ensuring the effective monitoring by MSs to ensure that such mechanisms are in existence in their territories. It should be acknowledged that these provisions are entirely focussed on the security of the critical infrastructure in general rather than merely the security of personal data being held/processed therein. However, at the same time these issues are not mutually exclusive as a security breach could also result in a personal data breach. Accordingly the requirement for the security of personal data found in the Data Protection legislation (discussed *infra*) will often be covered by the Operator Security Plan vis-à-vis the ICT systems security related aspects.

Reporting

Article 7 of the Directive stipulates a number of requirements in relation to reporting. MSs are required to conduct a threat assessment within one year of Critical Infrastructure status designation. In addition, MSs are required to report to the commission on a summary basis in relation to 'the types of risks, threats and vulnerabilities encountered per ECI sector'. Based on the reports received the Commission can then decide as to whether further action in a particular sector is required.

2.3 Critical Infrastructure Warning Information Network (CIWIN)

The CIWIN was an initiative established by the Directorate-General for Home Affairs of the European Commission which aims at improving the protection of critical infrastructures in the Union and in all relevant sectors of economic activity. The CIWIN provides a public information and communication system offering its members the opportunity to exchange CIP-related information. As described in the Impact Assessment of a Council Decision on the creation of CIWIN[7], the specific objective of CIWIN is to enable co-ordination and co-operation on information on the protection of critical infrastructure at 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. Through the portal, which has been put in place since early 2013, actors involved in a specific CI field can become members of CIWIN and participate in the information sharing platform. Access to the platform is voluntary and ensures that the data shared within the CIWIN framework cannot

[7] Available at http://ec.europa.eu/smart-regulation/impact/commission_guidelines/docs/sec_2008_2701_ia_ciwin_en.pdf

be used for any other purposes beyond the one described in the Terms and Conditions of Service.

2.4 Sector Specific Considerations

As has been made clear from the above there are clear provisions guiding the protection of Critical Infrastructures at an EU level. However, it is also worth mentioning some of the more general sector specific initiatives that have been taken.

Energy

There is a higher focus on Critical Infrastructure Protection in the EU energy sector. With this in mind the European Commission established the Thematic Network on Critical Energy Infrastructure Protection (TNCEIP).[8] This network, which launched in December 2010, aims at facilitating the exchange of information regarding experiences related to security issues. The network aims to 'address topics such as 'Threat Assessment', 'Risk Management', 'Cyber Security', and others.' [9]

Transport

In relation to the Transport sector there are a number of key legislative initiatives which are important to mention. These have provided a general framework in certain areas on the protection of specified transport assets. These have focused on securing Ports and Aviation security. In particular it is worth noting *inter alia*:

- Directive 2005/65/EC of the European Parliament and of the Council of 26 October 2005 on enhancing port security
- Regulation (EC) No 725/2004 of the EP and of the Council of 31 March 2004 on enhancing ship and port facility security
- Regulation (EC) No 2320/2002 of the European Parliament and the Council of 16 December 2002 establishing common rules in the field of civil aviation security; and its implementing regulations and amendments
- Regulation (EC) No 300/2008 of the EP and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002
- Regulation (EC) No 2096/2005 of 20 December 2005 laying down common requirements for the provision of air navigation services
- Regulation (EC) No 550/2004 of the EP and of the Council of 10 March 2004 on the provision of air navigation services in the single European sky
- Regulation (EC) No 1315/2007 of 8 November 2007 on safety oversight in air traffic management and amending Regulation (EC) No 2096/2005

These provisions provide specifically tailored requirements and are accordingly important. However, it is important to note that they are clearly applicable outside the context of Critical Infrastructures.

[8] Position Paper of the TNCEIP on EU Policy on Critical Energy Infrastructure Protection (November 2012) at: ec.europa.eu/energy/infrastructure/doc/20121114_tnceip_eupolicy_position_paper.pdf
[9] http://ec.europa.eu/energy/infrastructure/critical_en.htm

Finance

At an EU level Finance sector specific legislation has focused on the protection of users/consumers against fraud and the detection and prevention of crimes such as money laundering. However, despite the lack of a coordinated European response to this issue it is acknowledged as being a Critical Infrastructure. As noted in the 2013 report on the implementation of the Directive:

> 'The sector-focused approach of the Directive likewise represents a challenge to a number of Member States, as in practice the analysis of criticalities is not confined to sectoral boundaries and follows rather a 'system' or 'service' approach (e.g. hospitals, financial services).'

2.5 European Security Framework

The Digital Agenda for Europe (DAE: Trust and Security)

As part of the DAE the EU attempted to stimulate the digital economy and address ICT challenges. This was adopted in 2010 and forms an integral part of the Europe 2020 strategy.[10] The agenda lists a number of issues of importance relating to topics such as data protection, Critical infrastructure protection and network and information security. [11] In relation to the Critical Infrastructure protection discussion there is a focus on the information infrastructure and Computer Emergency response Teams and the importance in establishing effective responses to the increasing threat. As part of the agenda the Commission highlighted the following actions:

Pillar III of the DAE 'Trust and Security' requires the following actions[12]:

- Action 28: Reinforced Network and Information Security Policy
- Action 29: Combat cyber-attacks against information systems
- Action 30: Establish a European cybercrime platform
- Action 31: Analyse the usefulness of creating a European cybercrime centre
- Action 32: Strengthen the fight against cybercrime and cyber-attacks at international level
- Action 33: Support EU-wide cyber-security preparedness
- Action 38: Member States to establish pan-European Computer Emergency Response Teams
- Action 39: Member States to carry out cyber-attack simulations

[10] The Digital Agenda for Europe is one of the seven flagship initiatives of the Europe 2020 Strategy, set out to define the key enabling role that the use of Information and Communication Technologies (ICT) will have to play if Europe wants to succeed in its ambitions for 2020. European Commission, Communication 245 on a Digital Agenda for Europe, 2010, http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52010DC0245.

[11] Brussels, 19.5.2010 COM(2010)245, Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions A Digital Agenda for Europe, eur-lex.europa.eu/legal-content/EN/TXT/PDF/?Uri=CELEX:52010DC0245&from=EN

[12] http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

- Action 41: Member States to set up national alert platforms.
- Action 29: Combat cyber-attacks against information systems.
- Action 123: Proposal for a Directive on network and information security (NIS Directive see below).
- Action 124: EU Cyber-security strategy.

The DAE certainly provides a roadmap in this area and has certainly progressed regarding these actions. In December 2012 the Commission released their digital 'to do list' which included seven new priorities for the development of the digital economy and society. Of particular importance is priority 4 which states: 'Security and freedom online go hand-in-hand. The EU should offer the world's safest online environments, valuing user freedom and privacy. The Commission will deliver a strategy and proposed Directive to establish a common minimum level of preparedness at national level, including an online platform to prevent and counter cross-border cyber incidents, and incident reporting requirements. This will stimulate a larger European market for security and privacy-by-design products.'[13] The more recent legislative developments will now be assessed.

Directive on attacks against information systems (2013/40/EU)

The European Council adopted the Directive on attacks against information systems in July 2013 in order to harmonise domestic approaches in domestic criminal law in relation to attacks against information systems. The Directive replaces entirely the provisions of Council Framework Decision 2005/222/JHA of 24 February 2005 aims to allow for the consistent penalisation of illegal access and system and data interference thereby reinforcing the protection of personal data and the protection of Critical Infrastructures. The Directive includes provisions dealing with the use of Botnets as a means of committing these offences. Specifically 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.'[14] There is 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.

Article 5(4)(c) states that attacks against Critical Infrastructures should be punishable by a term of imprisonment of at least 5 years. Furthermore, 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), and ENISA. Article 10 of the Directive states that legal persons can also be found liable of offences committed for their benefit and also for failing to adequately supervise persons under their authority. However, this liability does not exclude the culpability of natural persons who perpetrate, incite or are accessories to any of the offences provided for under the terms of the Directive. Moreover, as per Recitals 26 and 30 any processing of personal data in the context of the Directive must comply with the Privacy and Data Protection Framework. The Directive must be adopted by the 4th of September 2015.

[13] http://europa.eu/rapid/press-release_IP-12-1389_en.htm
[14] Article 1

Proposed NIS Directive

There have been significant developments in relation to the protection of Network Information Security. Through EU Regulation (EC) No. 460/2004 the European Network and Information Security Agency (ENISA) was established under the mandate of assisting the Member States in the establishment of a high level of Network Infrastructure Security (NIS). In January 2013 the European Commission also established the European Cybercrime Centre under the scope of EUROPOL and 'at the core of cybercrime law enforcement within the EU.'[15]

This was supplemented in February 2013 with the recommendations contained in the EU cybersecurity strategy published by the Commission. This document 'outlines the EU's vision in this domain, clarifies roles and responsibilities and sets out the actions required based on strong and effective protection and promotion of citizens' rights to make the EU's online environment the safest in the world.'[16] These strategic actions relate to: (i) achieving cyber resilience; (ii) drastically reducing cybercrime; (iii) developing cyberdefence policies and capabilities related to the Common Security and Defence Policy (CSDP); (iv) developing the industrial and technological resources for cybersecurity; and (v) establishing a coherent international cyberspace policy for the European Union and promote core EU values. In order to help achieve these action points the Commission proposed the adoption of a Directive and this resulted in the adoption of NIS Directive proposal which was subsequently passed by the European Parliament in March 2014. The Directive aims to coordinate the MS actions to improve cyber security and to develop a common and consistent approach in order to allow for a level playing field across Europe and to avoid a weakest link situation.[17]

vi. Current Status

In their acceptance of the proposal in March the parliament recommended a series of modifications to the text of the Directive. These modifications can be seen as a severe watering down of the original obligations in that the modifications severely narrow the scope of the original provisions. The modifications exclude 'public administrations'. Moreover, 'market operators' are much more narrowly defined. Nevertheless, for the purposes of the current analysis under the scope of ECOSSIAN, it must be understood that this has no effect on Critical Infrastructures. Indeed, the modified text stipulates that it will still apply to 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

[15] 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/.

[16] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, 2013, p3, http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security.

[17] ENISA Threat Landscape Responding to the Evolving Threat Environment [Deliverable – 2012-09-28]

which would have a significant impact in a Member State […] insofar as the network and information systems concerned are related to its core services'. The finalised version of the text is yet to be agreed. However, if adopted the proposed NIS Directive is likely to have an impact on activities within the project's scope.

vii. Applicable provisions

It is important to note that from Article 2 of the proposal the terms of the NIS Directive are subject to the principle of minimum harmonisation. In essence this establishes minimum levels of protection but does not prevent MSs from adopting provisions ensuring higher levels of protection. This reflects the importance attached to the principle of subsidiarity during the adoption of the provisions. However, as expressed in the explanatory memorandum attached to the proposed Directive, given the cross-border nature of NIS a failure to act at an EU level would lead to the disregarding of the interdependencies between MSs and divergences in national approaches. Furthermore, as noted by the memorandum 'regulatory obligations at EU level are needed to create a level playing field and close legislative loopholes. A purely voluntary approach has resulted in cooperation only among a minority of Member States with a high level of capabilities. In order to involve all the Member States, it is necessary to ensure that they all have the required minimum level of capability.'

From Recital 24, Article 1(4) and Article 3(8) it is clear that the application of the NIS Directive is to be viewed in conjunction with the Critical Infrastructure Protection Directive. Article 1(4) provides that the proposed Directive is to be viewed 'without prejudice' to the CI Directive and Article 3(8) includes the operator of a critical infrastructure in the definition of a 'market operator' under the terms of the Directive. The key chapters of the Directive outlining the substantive requirements relate to the following key areas: (1) the implementation of national framework (Chapter 2), (2) the cooperation between competent authorities (Chapter 3) and (3) the enhancement of security of the NIS systems of public administrations and market operators (Chapter 4). The relevant provisions of each of these key chapters will now be highlighted.

Specifically in relation to Chapter 2, the proposal requires that the MSs 'ensure a high level of security of the network and information systems in their territories'.[18] Article 5 requires the implementation of NIS strategies and national NIS cooperation plans. The Article lists a variety of requirements related to the focus of the strategy, the requirements of such a strategy and the communication of this to the Commission. Article 6 deals with the designation and defining of the monitoring role of national competent authorities and Article 7 outlines the establishment and enforcement of Computer Emergency Response Teams that under the proposal are tasked with the handling of incidents and risks. The requirements under Chapter 3 deal with the establishment of a Cooperation Network (Article 8), provisions relating to the securing of information-sharing operations (Article 9), the establishment of early warning mechanisms the resulting coordinated response system (Articles 10 and 11), the empowerment of the Commission to adopt of a cooperation plan (Article 12) and a

[18] Article 4

provision relating to international cooperation (Article 13). The final chapter outlines the Security requirements and incident notification (Article 14), implementation and enforcement (Article 15) and standardisation (Article 17). It is also significant to note the specific provisions relating to Data Protection namely recital 31, Article 6(5) and Article 8(3)(f). Essentially these provisions stipulate that the competent authorities and the data protection authorities should cooperate and that data protection rules should be respected vis-à-vis the exchange/processing or personal data and the reporting of data breaches.

2.6 Privacy and Data Protection Framework

Having analysed the protection of Critical Infrastructures at an EU level it is now necessary to begin the analysis of how this, and the operations to be performed under ECOSSIAN, may be impacted by the Privacy and Data Protection Framework. The operations at the heart of ECOSSIAN potentially raise serious concerns in relation to this framework if personal data is involved. More specifically at the threat detection, information sharing and breach response stages. Accordingly, it is necessary to outline the data protection framework and assess the requirements contained therein. However, before delving into this framework it is perhaps prudent to first briefly outline the concept of information sharing platforms and the potential consequences of attacks against the ICT infrastructure and the potential data leakage.

Critical Infrastructure attacks and threat identification

Given the strategic importance of CIs it is reasonable to consider the risks associated with attacks from a data protection viewpoint. Attacks motivated from a cyber-espionage perspective, by their very nature, may not always aim to directly disrupt or damage the CI but instead may target the retrieval of particular types of information (e.g. power grid mapping in the energy sector). If these attacks are targeted towards systems containing personal data then the Data Protection Framework will be applicable. Moreover, during the threat detection and assessment stage, if personal data is processed in order to successfully analyse and counteract the attacks the Data Protection legislation needs to be kept in mind. In the context of ECOSSIAN, it is clear that the project also has a clear focus on establishing a system that can react appropriately to an attack by sharing information in order to isolate and mitigate the effects (i.e. from the O-SOC to the N-SOC and to the E-SOC levels). As such, for the purposes of ECOSSIAN there are also potential Data Protection issues surrounding the sharing of this genre of information if it contains personal data as defined under the Data Protection Directive.

Information Sharing Platforms

For the purpose of this document, information sharing shall mean the exchange of a variety of network and data security related information such as risks, vulnerabilities, threats and internal security issues as well as good practice policies[19]. Security experts prefer to adopt the term Security Information Sharing (SIS) to explain these systems. However, there is no existing regulation at an EU level which specifically targets the exchange of security data.

[19] ENISA, Incentives and Barriers to Information Sharing in the Context of Information and Network Security.

Currently, different types of information sharing platforms coexist in the EU each with different purposes, partners and architectures. By examining the state-of-the-art in security data exchanges, we can identify common operations and legal issues involved in the sharing of data related to security incidents. Aside from the CIWIN and the TNCEIP (see *supra* for more detail) the European Public Private Partnership for Resilience (EP3R) is another relevant example. The EP3R was launched in 2009 and was developed with the goal of facilitating the exchange of security information and best practices in public and private sector. Managed by ENISA, the EP3R objectives are divided in four action lines:

- Encourage information sharing and stock-taking of good policy and industrial practices to foster common understanding;
- Discuss public policy priorities, objectives and measures;
- Baseline requirements for the security and resilience in Europe;
- Identify and promote the adoption of good baseline practices for security and resilience.

However, it must be noted 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. Accordingly, the exchange of information relating to the protection of critical infrastructures must be analysed in light of the Data Protection Framework, namely Directive 95/46/EC (herein Data Protection Directive) and Directive 2002/58/EC (e-Privacy Directive).

Fundamental introduction – Privacy and Data Protection in the Primary Sources

According to Article 1 of Directive 95/46/EC, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data. Article 1 of the Data Protection Directive calibrates the concept of privacy in relation to the particular sector of the personal data processing. Despite an apparent affinity of meaning, it is appropriate to recognise respect for private life and protection of personal data as closely related but separate fundamental human rights.

Article 8 of the European Convention on Human Rights, adopted in 1950, incorporates the right to privacy, stating that everyone has the right to respect for his private and family life, his home and his correspondence. The Article requires a justification for any interference with privacy. This approach is based on a general prohibition of interference with the right to privacy and allows exceptions only under strictly defined conditions.

The Council of Europe's Convention for the Protection of Individuals with regard to automatic processing of personal data introduced the protection of personal data as a separate concept. The underlying idea at the time was not that the processing of personal data should always be seen as ‘interference with privacy’, but rather that it should be monitored in order to protect individuals’ fundamental rights and freedoms, and more specifically their right to privacy.

The legal notion of privacy has subsequently moved from this narrow idea of a space of seclusion to a more complex notion which combines the original definition with new additional caveats. In particular, the need to grant people the ability to exert some control over the circulation of their data and to autonomously define the effective limits of their privacy is widely recognised. This means that people should be given the legal instruments

to understand who is doing what with their personal data and to intervene in the process. Such a legal approach usually comes under the definition of the phrase 'privacy control theory' which has spread both in the United States and in Europe, with several specific variations and angles.

Echoes of the right to 'informative self-determination' can be found in the primary legal sources. According to the Article 8 of the European Union Charter of Fundamental Rights:

> 'everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified (..)' [20].

Moreover, Article 16 of the Treaty on the Functioning of the European Union provides that *'everyone has the right to the protection of personal data concerning them'* and that Parliament and the Council shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities that fall within the scope of Union law.

The right to the protection of personal data forms part of the more general right to privacy protected under Article 7 of the Charter, which more generally guarantees the right to respect for private and family life, home and correspondence and lays down the conditions under which restrictions of this right are permitted. The right to protection of personal data is not, however, an absolute rights, but must be considered in relation to its function in society. Article 52 (1) of the Charter thus accepts that limitations may be imposed on the exercise of fundamental rights, as long as these limitations are provided for by law, respect the essence of those rights and freedoms and, subject to the principle of proportionality, are necessary and genuinely meet the objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others.

Directive 95/46/EC

Directive 95/46/EC is the main reference source of the EU legal framework on the personal data protection[21]. In 2012 the European Commission proposed a major reform of the EU data protection legal framework. The result is the proposal for a regulation relating to the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)[22]. The General Data

[20] This provision reinforces both the importance of the principle of lawfulness and the need for an adequate legal basis for the processing of personal data that will be analyzed in the following. Finally, it is important to note that since the Lisbon Treaty entered into force on 1 December 2009, the European Union Charter of Fundamental Rights enjoys the same legal value as the Treaties.

[21] The Data Protection Directive text is available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML; in general about Data Protection Directive see: AA.VV., *Concise. European IT Law*, BULLESBACH - GIJRATH - POULETT - PRINS (edit by), Second Edition, 2010, Kluwer Law International.

[22] The Proposal text is available at: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

Protection Regulation, if adopted, would revoke Directive 95/46/EC and would make significant substantive changes to the Data Protection Framework.

Against this background, the following paragraphs will analyse the requirements provided for by Directive 95/46/EC. In particular, there will be a particular focus on the general rules regulating the lawfulness of the processing of personal data.

Directive 95/46/EC (hereinafter referred to as the 'Data Protection Directive') was adopted on the 24th of October 1995 and implementation by the Member States was to have been completed by the 24th of October 1998.

According to Article 3(1) of the Directive, its provisions shall apply to the processing of personal data wholly or partly by automatic means, and to processing otherwise than by automatic means of personal data which form part of a filling system. This provision reflects recital 27 of the Directive which states that the scope of personal data protection must not in effect depend on the techniques used. However, Article 3 (2) states that the Directive *'shall not apply to the processing of personal data (…) by a natural person in the course of a purely personal or household activity'*.

viii. Definitions: personal data and data processing

The term 'personal data' is defined as follows in Article 2(a) of the Data Protection Directive:

'any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity'.

In the following we focus on three key elements of this definition:

1. 'any information';
2. 'relating to';
3. 'an identified or identifiable'.

1. The expression 'any information' illustrates just how wide the notion of personal data is defined. It is not infrequent to erroneously only regard 'personal data' as the information concerning the most intimate aspects of a person. However, the concept of personal data includes any sort of information about a person, including economic and professional data, and not just data about his personal life. Indeed, this expression covers 'objective' information, such as occupation or income as well as 'subjective' information, such as opinions or assessments. According to the Article 29 Data Protection Working Party[23]:

> *'considering the format or the medium on which that information is contained, the concept of personal data includes information available in whatever form, be it alphabetical, numerical, graphical, photographical or acoustic, for example. It includes information kept on paper, as well as information stored in a computer memory by means of binary code, or on a videotape, for instance. In particular, sound and image data qualify as personal data from this point of view, insofar as they may represent information on an individual'*.

[23] See Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, adopted on 20 June, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf.

2. In general terms, information can be considered to 'relate' to an individual when it is about that individual. In many situations, this relationship can be easily established. For instance, the data registered in a flight ticket are clearly 'related to' an identified passenger. Analogously, the image of a person filmed on a video is 'related to' that person. In other situations, however, it is not immediately possible to establish the relationship between the information and the individual. In order to clarify this point, the Article 29 Working Party noted that 'data relates to an individual if it refers to the identity, characteristics or behaviour of an individual or if such information is used to determine or influence the way in which that person is treated or evaluated'[24].

3. A natural person can be considered as 'identified' when, within a group of persons, he or she is 'distinguished' from all other members of the group. Accordingly, a natural person is 'identifiable' as soon as it is possible to do so even if that has yet to occur. This relates to the fact that the data subject can be identified through some characteristics or aggregation of data. The Data Protection Directive defines neither the terms 'identified' nor 'identifiable'. As per the Article 29 Working Party, identification is normally achieved through particular pieces of information which hold a close relationship with the particular individual.[25] The Data Protection Directive mentions those 'identifiers' in the definition of 'personal data'. Indeed Article 2 provides that a natural person *'can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity'.*

A key element in deciphering the meaning of the term 'identifiable' can be found in Recital 26 of the Directive. This provision states that: '*to determine whether a person is identifiable account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person*'. In this scenario, different degrees of identification could be envisaged. There appears to be division among Member States on whether or not to use a relative approach to the concept of personal data in the sense that data are considered personal only for someone who can link the data to an identified individual. The laws in some Member States make it clear for instance that encoded or pseudonymised data are 'personal' with regard to a person who has access to both the data and the 'key', but are not personal with regard to a person without access to the 'key'.

Deciphering the notion of identifiability can be also be aided through interpreting acts of the Council of Europe (for instance resolution R (73) 22, resolution R (74) 29, recommendation R (81) 1, recommendation R (83) 10). Moreover, an accurate investigation of this matter can be found in the *Explanatory Memorandum* to recommendation R (97) 18. See for instance point No. 52(d):

[24] See Article 29 Data Protection Working Party, working document on data protection issues related to RFID technology, adopted on 19 January, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp105_en.pdf.
[25] Article 29 Working Party Opinion 4/2007 on the concept of personal data Adopted on 20th June 01248/07/EN WP136

> 'Conditions for anonymity are relative, especially in relation to the technical means available for identifying data and taking away their anonymity. In this way, in view of the rapid progress in technological and methodological developments, the time and manpower required to identify a person, which would today be considered 'unreasonable', might no longer be so in the future. However, the present wording is sufficiently flexible to cover such developments'.

A critical element here is therefore represented by progresses in computational power, and in the methods of data mining and the organisation of information[26]. As a result, the Data Protection Directive may even encompass such things as Internet protocol ('IP') addresses. Although IP addresses -which consist of a series of numbers- may not directly identify the user, they may provide sufficient information to indirectly determine the user's identity[27]. Despite the fact that many of the national data protection authorities and the Article 29 Working Party have stated that IP addresses are indeed personal data this issue is yet to be definitively decided. The recent referral by the German Courts on the classification of IP addresses as personal data should be watched closely as it may provide the definitive response in this regard.[28]

The importance of these considerations within the scope of the Project's operations is obvious: if the data collected or shared by critical infrastructures are personal data, then the Data Protection Directive framework will be applicable. Finally, it is important to observe that the mere fact that data are publicly available will not exempt them from the scope of the Data Protection Directive.[29] Finally, although the Directive contains some exemptions related to 'a register established by law and intended for consultation by public or persons having a legitimate interest', these are limited to government-maintained public registries.

ix. Data Processing

Another important definition relates to the notion of 'processing'. According to Article 2(b) of the Data Protection Directive, processing is:

> *'any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.'*

[26] See also Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, adopted on 20 June, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf.

[27] The Working Party has stated that '*Internet access providers and managers of local area networks can, using reasonable means, identify Internet users to whom they have attributed IP addresses as they normally systematically 'log' in a file the date, time, duration and dynamic IP address given to the Internet user. The same can be said about Internet Service Providers that keep a logbook on the HTTP server. In these cases there is no doubt about the fact that one can talk about personal data in the sense of Article 2 a) of the Directive (...)'.* See Article 29 Data Protection Working Party, Working document, Privacy on the Internet - An integrated EU Approach to On-line Data Protection, adopted on 21 November 2000, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2000/wp37_en.pdf.

[28] BGH, 28. 10. 2014, >> Az. VI ZR 135/13) see:juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=pm&Datum=2014&Sort=3&nr=69184&pos=0&anz=152

[29] KUNER, *European Data Privacy Law and Online Business*, 2003, Oxford University Press, p. 52.

The definition of processing is extremely broad, so that it is difficult to recognise an operation performed on personal data which would not come within its scope. Thus, in relation to ECOSSIAN; collection, storage and registration of personal data by a single infrastructure would be considered as 'personal data processing'. Similarly, the sharing of personal data between various infrastructures is also covered by this definition (this operation, as we will discuss *infra*, may be subject in certain circumstances to further limitations).

x. The Controller

The responsibility for compliance rests on the shoulders of the 'controller', meaning '*the natural or artificial person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data*'[30]. It is important to highlight that the data protection rules are applicable not only when the controller is established within the EU. According to Article 4(1)(a) of the Data Protection Directive, the national law of a Member State is applicable to all processing of personal data carried out 'in the context of an establishment' of the controller on the territory of that Member State. Pursuant to Article 4(1)(c) of the Data Protection Directive, the national law of a Member State is also applicable in cases where the controller is not established on Community territory but makes use of equipment situated on the territory of that Member State. As such, controllers situated outside the EU, processing data in the EU, will have to follow the Data Protection Framework. The Directive extends privacy safeguards to personal data that are transferred outside of the European Union. Article 25 of the Data Protection Directive states that data can only be transferred to third countries that provide an '*adequate level of data protection*'. In particular, the adequacy of the level of protection afforded by a third country:

> '*shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country'*.

Determinations regarding which countries provide the requisite level of protection are made by the EU Commission with recommendations from a Working Party established pursuant to Article 29 of the Directive. The result is that personal data can flow from the 28 EU countries and three European Economic Area member countries (Norway, Liechtenstein and Iceland) to that third country without any further safeguards being necessary**.** Moreover, the Commission has recognised Andorra, Argentina, Australia, Canada (commercial organisations), Switzerland, Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Uruguay and the US Department of Commerce's Safe Harbour Privacy Principles as providing adequate protection.[31]

[30] See Article 29 Data Protection Working Party, Opinion 1/2010 on the notion of controller and processor, adopted on 16 February 2010, available at https://www.cbpweb.nl/downloads_med/med20100219_C.03%20DC-DP_Opinion_ADOPTED.pdf.

[31] See Safe Harbor Privacy Principles and annexed Frequently Asked Questions approved by European Commission with decision 2000/520/CE, 26 july 2000, available at http://eur-lex.europa.eu.

xi. Legal grounds for legitimate processing

In order to process personal data, Article 7 of the Data Protection Directive enumerates the grounds for the lawfulness processing. This article distinguishes six legal grounds for data processing: the data subject's unambiguously given consent; the necessity for the performance of a contract with the data subject; to protect the vital interests of the data subject; the necessity for compliance with a legal obligation; (for public authorities) to perform a task carried out in the public interest and the necessity for legitimate interests of controllers or of third parties[32].

Consent is a very important ground as it gives some control to the data subject with regard to the processing of their personal data. The concept consent is defined in Article 2(h) and subsequently used in Articles 7, 8 and 26. The role of consent is also mentioned in recitals 30 and 45. According to Article 2(h) 'the data subject's consent' shall mean *'any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed'.* The Data Protection Directive does not define the form of the indication. As indicated by Article 29 Working Party, consent should include any indication of a wish, by which the data subject signifies his agreement: it could include a handwritten signature affixed at the bottom of a paper form, but also oral statements to signify agreement, or a behaviour from which consent can be reasonably concluded.[33] Consent can be considered voluntary and *freely given* if the data subject is able to exercise a real choice and there is no risk of deception, intimidation, coercion or significant negative consequences for failing to consent. Moreover, consent must be specific: it should refer clearly and precisely to the purpose of the data processing.

Therefore, 'general agreement' of the data subject would not constitute consent under the terms of Article 2(h) of the Data Protection Directive. Among its recommendations, the Working Party insisted also on the need to clarify what 'unambiguous consent' means. It observed that:

> 'clarification should aim at emphasizing that unambiguous consent requires the use of mechanisms that leave no doubt of the data subject's intention to consent. At the same time it should be made clear that the use of default options which the data subject is required to modify in order to reject the processing (consent based on silence) does not in itself constitute unambiguous consent. This is especially true in the on-line environment'.

It is important to note that the value of the consent is often overemphasised as the requirement necessary to ensure the fairness and lawfulness of the personal data processing. Instead, as properly highlighted by Waltraut Kotschy, all grounds for lawful

[32] See Article 29 Data Protection Working Party, Opinion 6/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, adopted on 9 April, available at http://www.cnpd.public.lu/fr/publications/groupe-art29/wp217_en.pdf.

[33] See Article 29 Data Protection Working Party, Opinion 15/2011 on the definition of consent, adopted on 13 July 2011, available at http://ec.europa.eu/research/participants/data/ref/fp7/89736/article-29_en.pdf.

processing indicated by Article 7 of the Data Protection Directive have the same status. 'Considering how difficult it is for a data subject to foresee all possible consequences of his consent to the use of his data in a globalized world, the protective effect of having been asked for consent should not be overestimated'[34]. Of particular importance is Article 7(e) of the Directive. According to this provision, all personal data processing in the public interest or in the exercise of official authority is automatically lawful. It is important to note that Article 7(e) refers to the public interest of the European Union or of a Member State: so the notion of official authority must be referred to as an authority granted by the European Union or a Member State. In other words, processing in the public interest of a third country or in the exercise of an official authority vested by virtue of foreign law do not fall within the scope of this provision. Article 7(e) covers two situations and is relevant both to the public and the private sectors. First, it relates to the situation in which the controller has official authority or a public interest task and the processing is necessary for exercising that authority or performing that task. Second, Article 7(e) also covers situations in which the controller does not have an official authority, but is requested by a third party having such authority to disclose data. However, the personal data processing must be necessary for the performance of a task carried out in the public interest. It is also important to emphasise that this official authority or public task will have been typically attributed in statutory laws or other legal provisions. Consequently, the legal basis should be specific and precise enough in framing the kind of data processing that may be allowed. These situations are becoming increasingly common, also outside the confines of the public sector, considering the trend to outsource governmental tasks to entities in the private sector.

It is also important to mention Article 7(f) of the Data Protection Directive. According to this provision, the personal data processing is legitimate if it is:

> 'necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject (...)'.

This provision requires a complicated balancing test (i.e. what is necessary for the legitimate interests of the controller (or third parties) must be balanced against the interests or fundamental rights and freedoms of the data subject). The open-ended nature of the provision allows for the application of this balancing test to the cases that do not fit in the scenarios pre-defined under the specified legal grounds indicated by Article 7 (a) to (e). As pointed-out by the Working Party[35], the balancing test must be strictly founded on the following criteria:

1. The legitimate interest of the data controller (or of the third party or parties to whom the data are disclosed). The interest of the data controller to the personal data processing must be lawful, sufficiently specific to allow the balancing test to be carried out against the interests and fundamental rights of the data subject and not

[34] KOTSCHY, Article 7 of the Directive 95/46/EC, in *Concise. European IT Law*, BULLESBACH - GIJRATH - POULETT - PRINS (edit by), Second Edition, 2010, Kluwer Law International, p. 55. – However, as we shall see in Chapter 3 France has elevated the importance of consent above these other grounds.

[35] See aforementioned Article 29 Data Protection Working Party, Opinion 6/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, adopted on 9 April, available at http://www.cnpd.public.lu/fr/publications/groupe-art29/wp217_en.pdf.

speculative. Moreover, the processing of personal data must also be necessary for the purpose of the legitimate interests pursued either by the controller or - in the case of disclosure - by the third party.

2. The interest or fundamental rights of the data subject. The notion of the 'interests' of the data subjects should be considered even more broadly as it does not require a 'legitimacy' element. If the data controller or third party can pursue any interests, provided they are not illegitimate, the data subject is entitled to have all categories of interests to be taken into account and weighed against those of the controller or third party.
3. Personal data processing impact on the data subject. This necessary preliminary analysis to legitimate the personal data processing must be considered the nature of the data, the way data are being processed, including whether the data are publicly disclosed or otherwise made accessible to a large number of persons, or whether large amounts of personal data are processed or combined with other data; the reasonable expectations of the data subject and the status of the controller and of the data subject (with a particular attention in case of more vulnerable segment of the population, as a child).
4. Additional safeguards to prevent undue impact on the data subjects, including: data minimisation; technical and organisational measures to ensure that the data cannot be used to take decisions or other actions with respect to individuals; extensive use of anonymisation techniques, aggregation of data, privacy-enhancing technologies, privacy by design, privacy and data protection impact assessments; increased transparency, general measures to empower data subjects.

After this complex analysis which must be conducted by the controller, guaranteeing transparency and visibility to the data subjects, it can be stated that the legitimate interests of the controller prevail over the rights and interests of the data subjects.

Finally, the Data Protection Directive adds an additional layer of protection to personal data considered sensitive. This category of personal data includes 'data revealing racial or ethnic origin, political opinions, religious or philo- sophical beliefs, trade-union membership, and the processing of data concerning health or sex life.' Processing of such data is prohibited except in a limited set of circumstances. Those circumstances exist where:

1. a data subject has given explicit consent;
2. necessary for controller to meet legal obligations with respect to employment law;
3. necessary to protect the vital interests of a data subject (or another person), and the data subject is physically or legally incapable of giving consent;
4. carried out by a non-profit organization whose aim is to advance an agenda related to one of the categories of sensitive data;
5. the data are manifestly made public by the data subject;
6. necessary to establish or defend legal claims, and
7. required by a health professional in the course of providing treatment or managing health-care services.

xii. Lawful processing

The conditions for legitimate personal data processing can be described in terms of the following principles: legitimate purpose, transparency, data quality and security. These principles constitutes the core of Data Protection legal framework.

Legitimate purpose: Article 6(b) of the Data Protection Directive provides that personal data must be collected for limited purposes. In particular, personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. As highlighted by the Article 29 Working Party on purpose limitation[36], specification of the purpose is a pre-requisite for applying other data quality requirements, including the adequacy, the relevance, the proportionality and the accuracy of the data collected and the requirements regarding the period of data retention. The purpose for which personal data are collected should be specified before the data processing takes place. The subsequent use should be limited to the fulfilment of those purposes or other such purposes that are not incompatible with the original and that are specified at each change. Therefore, the purposes of the data processing need to be well-defined and comprehensible for an average data subject without expert legal or technical knowledge. The principle of legitimate purposes is a crucial rule declinable along two coordinates: the controller must inform the data subjects of the processing purposes and those within which data processed for one or more specific purposes may be used for other purposes. The purpose of personal data processing cannot be changed neither during further use by the controller nor by transfer to third parties. This rule implies that before the transfer the initial controller has to check whether the purpose given by the recipient[37] (as a reason for the transfer) is not incompatible with the purpose for which the data was collected and was indicated in the information provided to the data subject.[38]

The principle of legitimate purposes limitation goes hand-in-hand with the principle of data minimisation[39]. In order to prevent unnecessary and potentially unlawful data processing, controllers must carefully consider on a case-by-case basis which data are strictly necessary to perform the processing purposes. Moreover, there is a strong connection between these principles and the principle of transparency. When the purposes are specified and sufficiently unambiguous and clearly expressed, the data subject's rights can be considered as fully

[36] Article 29 Data Protection Working Party, Opinion 3/2013 on purpose limitation, adopted on 2 April, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

[37] According to Article 2(g) of the Data Protection Directive, recipient is defined as 'a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients'.

[38] KOTSCHY, Article 6 of the Directive 95/46/EC, in *Concise. European IT Law*, BULLESBACH - GIJRATH - POULETT - PRINS (edit by), Second Edition, 2010, Kluwer Law International, p. 55.

[39] According to this principle, the collection should be limited to personal data that is directly relevant and necessary to accomplish the specified purposes. In other words, controllers should collect only the personal data they really need. Moreover, the personal data shouldn't be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data were collected or for which they are further processed. Data Protection Directive doesn't contain mandatory timeframes for keeping data: in this context, different timeframes could be provided in national laws. Article 6(e) of the Data Protection Directive provides that national laws may foresee longer terms of storage for historical, statistical and scientific purposes.

effective. Transparency ensures data subject's awareness and enables control about his data.

Transparency: Data subjects have the right to be informed about the details of the processing of their data. The Data Protection Directive sets out the focus of the controller's obligation and in this regard distinguishes between the situation in which data is obtained directly from the data subject (Article 10) and scenario in which data is obtained from other sources (Article 11). Under the terms of Article 10 of the Directive the controller must provide their name and address, the purpose of processing, the recipients of the data and all other information required to ensure the processing is fair. Information about the identity of the controller must be specific enough to allow the data subjects to contact the controller and so to exercise their rights. In accordance with Article 6 of the Data Protection Directive, the data subject must be informed about all purposes for which data is collected and further processed. This information ensures that the data is being used solely for the purposes declared. Moreover, the data subject must be informed about all elements that (despite not being enumerated by the Data Protection Directive) are necessary with regard to the specific circumstances in which the data is collected, to ensure fair personal data processing. Article 10(c) enumerates in the form of examples (with the expression 'such as') the following information: 'recipients or categories of recipients of data; whether replies are obligatory or mandatory; existence of the data subject's right of access to and right to rectify the data concerning him'. The Directive does not indicate a specific form in which the information is to be provided[40].

Data quality principles: Personal data may be processed only insofar as it is adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed. According to the principle of data-minimisation the requirement of data relevance must be interpreted as strictly as possible. Moreover, the data must be accurate, complete and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified. From this perspective, a critical element can the establishment of what constitutes reasonable measures. The concept of reasonableness appears to be vague. It is possible to determine its content in light of the following criteria: the nature of data; the data processing purposes; the preliminary and necessary analysis of the data processing risks and the state of art of knowledge about technical security measures. As acknowledged by the legal literature, the data quality principle is independent from the right of the data subject to have data corrected or deleted. Nevertheless, it is also true that due to this principle the right of 'informative self-determination', recognised to the data subject, becomes fully effective. The obligation to process only relevant and accurate data may require rectification and sometimes may even require the deletion of data. It may also be necessary to add data, namely, if its incompleteness would result in incorrect information that could potentially harm the data subject.

[40] The Article 29 Working Party took the view that the information must be given directly to the data subject: 'so it is not enough for information to be available somewhere (see Opinion 15/2011 on the definition of consent', adopted on 13 July 2011).

Security of processing: According to Article 17 of the Data Protection Directive, data controllers must take the necessary organisational and technical measures to ensure the protection of the personal data they process. Personal data must be protected by security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data. The measures must be appropriate with regard to the risks connected with the personal data processing, as well as with regard to the nature of the data collected. Hence, sensitive data (data referring to racial or ethnic origin, political opinions, religious or philosophical beliefs, membership in trade unions, health-related data and data concerning the sex life) may require more sophisticated security measures. Recital 26 of the Data Protection Directive provides an important specification and states:

> 'whereas the protection of the rights and freedoms of data subjects with regard to the processing of personal data requires that appropriate technical and organizational measures be taken, *both at the time of the design of the processing system and at the time of the processing itself* (italics added), particularly in order to maintain security and thereby to prevent any unauthorized processing (...)'.

Security must cover the lifecycle of the personal data processing. As a result, the organisational and technical measures have to be taken by all actors involved in the data processing, each according to their role and responsibility. The goal of compliance with the security obligation is twofold. It will empower data subjects to more stringently control their data, and enhance the level of trust in the entities that actually processes personal data.

In order to comply with security obligations, the principle of privacy by design becomes crucial. This requires a prior risk analysis in order to determine the privacy implications of the activity and evaluation of effective mitigating measures, including data minimisation, from the beginning of technical procedure's design. The concept of privacy by design is a very important principle which is indirectly in the Data Protection Directive and which, together with the principle of privacy by default emerges more clearly in the ePrivacy Directive[41]. The international security standards refer to the three following goals: confidentiality, integrity and availability. Confidentiality refers to the defining and enforcing of appropriate access levels for information. The rule also implies that the entities authorised to access and process personal data must keep the data confidential. Integrity relates to the protection of personal data from modification or unauthorised deletion. Finally, availability refers to the guarantee that authorised subjects are able to access the information when needed. It is important to set out that security needs a change of approach: security is not merely a specific obligation but also a value to spread trust amongst individuals and shorten the distance between data subjects and controllers.

xiii. Data subject's rights

The right of access, recognised by Article 12 of the Data Protection Directive, refers to a set of different and specific rights. The right to access may be instrumental to allowing the data

[41] 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, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML.

subject to remain informed about the existence and the principal features (purposes, underlying logic, etc) of the processing. This is in line with the aforementioned principle of transparency. According to Article 12(a) of the Directive, the data subject has the right to obtain, in an intelligible form, the data undergoing processing and any further available information as to their source. Giovanni Buttarelli points out that the expression 'without constraints' contained in Article 12 is full of meaning.[42] It implies that the controller must not restrict or complicate the data subject authority to exercise this right. Additionally, Article 12 provides that the data subject has the right to obtain a reply 'without excessive delay' and without excessive 'expense'. The data subject can also obtain rectification, erasure or blocking of data that has been processed in breach of the Data Protection Directive, in particular due to the inaccurate or incomplete nature of data. Finally, the data subject has the right to obtain the notification of any deletion, rectification or blocking of his data to a third party to whom the data have been disclosed.

The e-Privacy Directive

The e-Privacy Directive aims at defining rules of protection with regard to the processing of personal data specifically in the electronic communication sector (Article 3). As stated above, the e-Privacy Directive should be considered *lex specialis* relative to the *lex generalis* Data Protection Directive. Nevertheless, it is important to briefly outline the key terms of the Directive. Article 4 reflects the general principles set out by the Data Protection Directive and states that the provider of an electronic communications service must protect the security of its services by: ensuring personal data is accessed by authorised persons only; protecting personal data from being destroyed, lost or accidentally altered; ensuring the implementation of a security policy on the processing of personal data. A complementary duty to the service provider's obligation to implement appropriate security measures is represented by the general principle of confidentiality stated by Article 5 of the e-Privacy Directive. According to the first paragraph of this Article, 'Member States shall ensure, through national legislation, the confidentiality of communications and the related traffic data by means of a public communication network and publicly available electronic communication services'. Therefore, any communication by means of a private network or created in the context of a service not publicly available is not covered by the principle of confidentiality.

The e-Privacy Directive distinguishes three main categories of data generated in the course of an electronic communication: the data constituting the content of the messages sent during communication; the data necessary for establishing and maintaining the communication, so-called 'traffic data'; such as information about the communication partners, time and duration of the communication; within the traffic data, there are data specifically relating to the location of the communication device, so-called location data; these data are at the same time data about the location of the users of the communication devices and particularly relevant concerning users of mobile communication devices. The Directive determines that traffic data (Article 6) must be erased or made anonymous when they are no longer required for the conveyance of a communication or for billing. In relation to the location data other than traffic data, Article 9 of the e-Privacy Directive states that they

[42] See BUTTARELLI, Article 12 of the Directive 95/46/EC, in *Concise. European IT Law*, BULLESBACH - GIJRATH - POULETT - PRINS (edit by), Second Edition, 2010, Kluwer Law International.

may be processed only when they are made anonymous or with the consent of the data subject.

On the sensitive issue of data retention, Article 15 of the e-Privacy Directive states that Member States may withdraw the protection of data only to allow criminal investigations or to safeguard national security, defence and public security. Such action may be taken only where it constitutes a 'necessary, appropriate and proportionate measure within a democratic society'. In order to ensure the availability of communication data for the purpose of investigation, detection and prosecution of criminal offences, the Directive lays down provisions for the retention of data. Finally, it is also significant to note that through the 2009 modifications implemented by the Cookies Directive, the use of Cookies requires the unambiguous consent of the user. Unlike the provisions discussed above this requirements applies to any use of cookies and is therefore potentially relevant in the context of ECOSSIAN. Furthermore, it must also be understood that it is widely accepted that Cookie data constitutes personal data.[43] Therefore, both the *lex specialis* provisions contained in the E-Privacy Directive and the *lex generalis* provisions in the Data Protection Directive have applicability in the processing of this type of personal data.

Proposed Data Protection Regulation

xiv. Introduction

As previously stated, in 2012 European Commission adopted the Proposal for a regulation relating to the protection of individuals with regard to the processing of personal data and on the free movement of such data (Proposed General Data Protection Regulation). The most important characteristic of the draft regulation is the change in the regulatory instrument (i.e. the Regulation is replacing a Directive). This is a significant change as, if adopted, the proposed regulation should ensure a clearer and more harmonized application of the provisions by all States Member. In fact, complexity and juridical uncertainty create a cost which Europe must eliminate in order to present itself as a single market. Accordingly, a unique and uniform regulatory instrument, directly applicable to all 28 States Members, would be the most appropriate legal instrument to define the framework for the protection of personal data in the Union and contribute efficiently to the development of the internal market.[44] The proposal has been welcomed as it aims to reinforce the data subject's rights, enhance the obligations of the controllers and give more emphasis to the role of the supervisory authorities. Moreover, relevant changes concern the emphasis given to the social function of the right to personal data protection, the increasing role of the principle of reasonableness and the importance associated with the timescale.

In relation to the general principles to guarantee the lawfulness of personal data processing, the Proposed Regulation confirms the Directive's provisions (Article 5). The proposal highlights the transparency principle, providing that '*the personal data must be processed in a transparent manner in relation to the data subject*'; the data minimisation principle, providing that '*the personal data must be limited to the minimum necessary in relation to the purposes for which they are processed; they shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data*'

[43] See for example: Article 29 Working Party, 'Opinion 2/2010 on Online Behavioural Advertising adopted on the 22th of June 2010, 00909/10/EN WP 171

[44] See Explanatory Memorandum of the proposed Regulation, par. 3.1.

and finally, the responsibility and liability of the controller and processors, providing that '*the personal data must be processed under the responsibility and liability of the controller, who shall ensure and demonstrate for each processing operation the compliance with the provisions of this Regulation*'. Thus the general grounds allowing for the personal data collection and further processing, already examined for the Directive, remain under the proposed Regulation (Article 6). This is true, for example, for the data subject's consent and for the personal data processing based on a legal obligation or the public interest. However, in relation to consent, the proposed Regulation states that the consent must be explicit. As a consequence, this proposes to eliminate the legality of implicit consent.[45]

xv. Data subject's rights

The proposed Regulation strengthens the data subject's role in the data processing operation. The data subject is not a mere passive participant who suffers the decisions of controllers but rather an individual with an active and effective power of control over the collection and further processing of their personal data. In particular, the draft strengthens the right to access, including more information that the controller must provide to the data subject[46] and, more generally, requiring the implementation of quick and straightforward modalities for the exercise of this right. From this point of view, Article 11 of the proposal, significantly entitled 'Transparent information and communication', has a central role. This provision, after stating the controller's obligation to have transparent and easily accessible policies for the exercise of data subject's rights, points out the need to provide all information and communications relating to the processing of personal data to the data subject in an intelligible form, using clear and plain language, adapted to the data subject, with a particular attention to the personal data relating to children[47]. Moreover, the proposed Regulation provides that the controller has the obligation to respond to the data subject's request 'without undue delay', and at latest within one month of its receipt. With this in mind one must also consider Article 17 of the proposal which provides the right to erasure[48]. It is

[45] According to Article 4 (8) of the Proposal of the Regulation, data subject's consent is defined as 'any freely given specific, informed and *explicit* (italics added) indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed'. See also Article 7 related to the conditions for consent.

[46] According to Article 14 of the Proposal of the Regulation, data subject has the right to be informed by the controller about, apart from the information already stated by the Article 14 of the Data Protection Directive, the period for which the personal data will be stored and about his right to lodge a complaint to the supervisory authority.

[47] This provision is based on the Madrid Resolution on international standards on the protection of personal data and privacy, adopted by the International Conference of Data Protection and Privacy Commissioners on 5 November 2009.

[48] According to Article 17: 'The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child, where one of the following grounds applies:

(a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data;

(c) the data subject objects to the processing of personal data pursuant to Article 19;

(d) the processing of the data does not comply with this Regulation for other reasons'.

important to note that the first version of this provision was entitled *'Right to be forgotten and to erasure'* although its content only referred to the right to erasure.[49] The controller has the obligation to ensure erasure but also to inform third parties that are processing the data by means of links, copies or replications of the request of the data subject[50]. Nevertheless, no provision in the proposal makes it mandatory for third parties to comply with the data subject's request, unless they are also considered as controllers.[51] Another important right recognised by the data subject is the right to portability, provided by Article 18 of the draft Regulation. According to this provision, if personal data is processed by electronic means, the controller must, upon request of the data subject, provide a copy of such data to the data subject in an electronic and structured format, i.e. in a format which is commonly used and allows for further use by the data subject without hindrance from the controller of the personal data. This right will make it easier for individuals to transfer their personal data between service providers. Finally, according to Article 77 of the proposal, any person who has suffered damage as a consequence of an unlawful personal data processing has the right to receive adequate compensation from the controller or processor. As highlighted by the cited Opinion 01/2012 of the Article 29 Working Party, the proposal does not clarify if the word 'damage' only refers to a pecuniary loss or, as it should be reasonable, also to a non-economic damage.

xvi. Security of processing

The introduction of the principle of accountability in Article 22 plays a very important role in relation to value of data processing security.[52] In implementing this general principle it

It is important to note that the grounds that legitimize the exercise of this right are specific declinations of the more general principle of data minimization.

[49] The topic about the right to be forgotten is the core of a broad debate growing in significance following the recent decision by the Eu Court of Justice of 13 May 2014 (Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González - available at http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130d5b6c0ef0cfcc34664af65824af1275c09.e34KaxiLc3eQc40LaxqMbN4OaNmNe0?text=&docid=152065&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=433471) which has established that users can ask search engines to remove results linked to their name. See also a factsheet on ECJ's ruling about the right to forgotten, available at http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf. In the legal literature, see: GIUSELLA FINOCCHIARO, *La memoria della rete e il diritto all'oblio*, *Rivista di diritto dell'informazione e dell'informatica*, 3, 2010 p. 391 and VIKTOR MAYER-SCHONBERGER, *Delete. The virtue of Forgetting in the Digital Age*, Princeton University Press, 2009.

[50] See Article 29 Data Protection Working Party, Opinion 01/2012 on the data protection reform proposals, adopted on 23 March 2012, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp191_en.pdf.

[51] See Article 29 Data Protection Working Party, Opinion 01/2012 on the data protection reform proposals, adopted on 23 March 2012, p. 13.

[52] According to Article 22 (1-2-3) of the Proposal: 'The controller shall adopt policies and implement appropriate measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation.

The measures provided for in paragraph 1 shall in particular include:

(a) keeping the documentation pursuant to Article 28;

(b) implementing the data security requirements laid down in Article 30;

(c) performing a data protection impact assessment pursuant to Article 33;

(d) complying with the requirements for prior authorisation or prior consultation of the supervisory authority pursuant to Article 34(1) and (2);

(e) designating a data protection officer pursuant to Article 35(1).

becomes crucial for controllers to demonstrate that their processing activities take into account the concepts of the privacy by design and data protection by default, which constitute specific measures in ensuring an adequate level of data protection.[53] According to these principle, data protection safeguards should be built into the technical architecture, services and products from the earliest stage of development and that privacy-friendly default settings should be the norm. As such, the controller (and the processors), after a preliminary evaluation of the risks performed in light of the nature of the data, must implement appropriate technical and organisational measures to ensure an appropriate level of security. There will also be a mandatory obligation for controllers to inform the supervisory authority and any individuals adversely affected, without undue delay, of any data breaches. In particular, it is required that controllers notify if data is accidentally or unlawfully destroyed, lost, altered, accessed by unauthorized individuals. This is a significant proposal in the context of ECOSSIAN and as it moots the implementation of a notification requirement that was previously reserved only for the providers of communications networks. Finally, the controller has the obligation to maintain documentation of all processing operations under its responsibility. Article 28 indicates the information that are the focus of this obligation.

2.5.3. Comparative analysis

2.5.3.1 Directive 95/46/EC and Proposed Data Protection Regulation: differences

It is important to note that in comparing the Data Protection Directive and the proposed Regulation there are more additional elements than effective differences. Some of the major novelties of the proposed regulation will now be assessed.

i. Definitions: personal data, processing and controller

The proposal confirms the definitions (illustrated above) of personal data, processing and controller. In relation to the definition of personal data, it is important to note the need to

---

The controller shall implement mechanisms to ensure the verification of the effectiveness of the measures referred to in paragraphs 1 and 2. If proportionate, this verification shall be carried out by independent internal or external auditors.

(…)'.

[53] According to Article 23 of the Proposal: 'Having regard to the state of the art and the cost of implementation, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

The controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals.

The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures and mechanisms referred to in paragraph 1 and 2, in particular for data protection by design requirements applicable across sectors, products and services.

The Commission may lay down technical standards for the requirements laid down in paragraph 1 and 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2)'.

combine it with the definition of a data subject. Indeed, if personal data is defined as 'any information relating to a data subject'[54], 'data subject' is defined as:

> 'an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifiers or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person'[55].

Despite this, the draft Regulation introduces some significant additions to the basic definitions. Regarding the scope of ECOSSIAN, it is important to point out the definition of personal data breach as '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.' This definition was already stated by Article 2 (h) of the e-Privacy Directive. Moreover, it is also important to note the definition of biometric data as 'any data relating to the physical, physiological or behavioural characteristics of an individual which allow their unique identification, such as facial images, or dactyloscopic data'[56].

ii. Legal grounds for legitimate processing

As indicated *supra*, the Proposed Regulation confirms the general legal grounds for legitimate personal data processing. The six criteria indicated by the Data Protection Directive are reproduced *verbatim* in Article 6 of the proposal. A new element is represented in the formulation of Article 6(f), which states that in the balancing test between the legitimate interests of the controller and the data subject's right, more consideration should be taken in the case where the personal data relates to a child. Finally, as pointed out above, in relation to the consent of the data subject, the draft Regulation emphasises its requirements providing a specific definition. According to the Article 3(8) of the proposal, the data subject's consent means 'any freely given specific, informed and explicit indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed'.

iii. Lawful processing

Regarding the general principles relating to the data quality, the proposed Regulation does not contain substantial differences in comparison to the Data Protection Directive. As previously indicated, Article 5 of the Proposal confirms the principles according to which personal data may be processed only insofar as it is adequate, relevant and not excessive in relation to the purposes for which they are collected. Nevertheless, the proposal emphasises the importance of the data minimisation principle and the value of transparency for the data subject.

iv. Data subject's rights

[54] See Article 4 (2).
[55] See Article 4 (1).
[56] See Article 4 (11).

It is possible to state that in relation to the data subject's position the proposed Regulation contains the major novelties compared to the Data Protection Directive. Indeed, the proposal reinforces the position of the data subject, concretising the content of his right to informative self-determination. As stated *supra*, the proposal strengthens the data subject's right to access to their data, resulting in a more onerous controller obligation to provide the information about personal data processing to data subject. Moreover, the proposed Regulation introduces the right to erasure and the right to the portability of the data.

v. Security of processing

The draft Regulation emphasises, even in the preliminary definitions, the need to ensure the security of personal data processing. Indeed, Article 3(9) defines the risks connected to personal data processing are accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. In addition Article 22 introduces the fundamental principle of accountability. As indicated previously, this principle is closely associated with the concept of privacy by design and by default (Article 23). Also, even though these articles do not describe the concepts of data protection by design and by default, they require to the controller to 'implement appropriate technical and organisational measures and procedures' and to 'implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing (...)'. In this scenario, the controller becomes the subject of specific and detailed obligations and consequently its responsibilities are defined and circumscribed.

The provision stating the controller's obligation to maintain documentation of all decisions adopted in relation to personal data processing appears consistent with this approach. It is important to note that the controller's obligations persist throughout the entire personal data processing operation: they form continuing obligations that do not end at the time of personal data collection. This is confirmed by the requirement that the controller must inform the supervisory authority of any eventual data breaches that occurs during the processing. Finally, it is important to note that the proposal defines, more specifically compared to the Data Protection Directive, the powers and the independence requirements of the national supervisory authorities. Their opinion will be essential if Member States intend to adopt regulatory instruments that impact on the protection of personal data.

2.5.3.1 Impact of the Proposed Data Protection Regulation on the ECOSSIAN scenario

This final paragraph illustrates, in necessarily general terms, the impact of the Proposed Data Protection Regulation on the Project's scenario. An attack on the security of a critical infrastructure could lead to the loss or unauthorised access, destruction, use, modification or disclosure of personal data collected by the critical infrastructure involved. Considering the data protection framework illustrated above, although the attack comes generally from the outside (natural disasters or criminal attacks), if the result consist in a loss or other consequences that have a negative impact on the integrity, confidentiality and availability of personal data, the controller shall be liable for the failure to adopt the necessary technical and organisational security measures, as indicated by the law. In this scenario, it is evident that the Proposed of Data Protection Regulation, if adopted, could have a significant impact on the aspects related to the implementation of a critical infrastructure.

The introduction of the principle of privacy by design and by default will result in an obligation for the controller to adopt policies and implement appropriate measures to ensure that the processing of personal data is performed in compliance with the legal provisions. Thus, in relation to the state of the art and the cost of implementation, the controller should evaluate the risks for the personal data protection, and consequently adopt appropriate mechanisms for ensuring the respect of the minimisation principle, also considering the purpose of processing and the time of storage during the development stage. Hence, in this manner, in case of an attack to the infrastructures that leads i.e. to the loss of personal data, it is possible to state that the liability of the controller could be significantly mitigated. It is important to note that the obligation of the controller to notify the personal data breach to the supervisory authority is expected to have significant importance in the context of critical infrastructures. Therefore, it is no coincidence that the above mentioned Proposed NIS Directive evokes the need to tackle the personal data breaches resulting from incidents to guarantee the fundamental rights of the citizens relating to privacy and data protection.

The Proposed Police and Criminal Justice Data Protection Directive

It should also be acknowledged that the reform of the Data Protection Framework in the EU in not limited to the proposed Regulation but also encompasses the proposal[57] to replace the existing Framework decision covering personal data processing in the area of law enforcement and criminal justice.[58] The proposed introduction of this Directive aims at simplifying what was perceived by many critics a system that had failed to meet expectations.[59] As noted by de Hert and Papakonstantinou, the Commission had two options when deciding on the creation of a proposal for a new data protection framework; either combine the aims of the original Directive and Decision into one clear document or continue with the separation and provide modifications for both.[60] It is clear that the Commission has opted for the latter of these two options. 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.'[61]

[57] 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)

[58] Framework Decision 2008/977/JHA of November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.

[59] See: Paul de Hert and Vagelis 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.*

[60] Paul de Hert and Vagelis Papakonstantinou, The Polcie and Criminal Justice Data Protection Directive: Comment and Analysis, The IT Law Community, SCL Forum, http://www.vub.ac.be/LSTS/pub/Dehert/411.pdf

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

Article 2 defines the scope and 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'. Chapter 2 of the draft outlines the flexibilities permissible vis-à-vis the traditional standards for data processing (including sensitive data) in this context. The data subject rights are contained in Chapter 3 and Chapters 4, 6 and 7 refer to the enforcement mechanisms. Finally the conditions for international data transfer are regulated in Chapter 5. 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.

2.7 EU Level Conclusions

As seen through the analysis of the various instruments, there is a wide and diverse array of EU legislation relevant to the operations to be performed under the scope of ECOSSIAN. In its current state the protection of critical infrastructures at an EU level is focused on the coordination of classification and designation of European Critical Infrastructures. However, if adopted, the proposed NIS Directive could make substantive headway in the protection and security framework. In relation to the Privacy and Data Protection aspects it is significant to note the scope of application of the Data Protection Directive the resulting personal data security requirements. It is also important to highlight the potential changes regarding notification requirements for data breaches as contained in the proposed Data Protection Regulation. If adopted this would impose positive action on behalf of data controllers. As the current legislative framework has been adopted in the form of Directives it is now significant to assess the national implementation of these measures.

Chapter 3 Country Level Analysis

In order to successfully assess the impact of the privacy and data protection requirements on the operations to be undertaken as part of the ECOSSIAN project it is important to assess these requirements in the context of Critical Infrastructure Protection. With this in mind four particular questions have been selected as the means of assessing this impact. These are:

5. Regarding the detection and information sharing processes relating to the protection of Critical Infrastructures, what are the key variations in the national implementation of thresholds for the application of the Data Protection framework in the context of ECOSSIAN?
6. What are the key peculiarities of the relevant national provisions which ensure legal compliance legitimising the processes and operations which may be undertaken in relation to threat detection as a part of the activities to be performed by ECOSSIAN?
7. In the application of the national data protection framework to the specific parameters of the project, is the data controller subject to particular guarantees, liabilities or requirements (e.g. administrative/security) which deviate from those under the terms of the Directive and may affect the implementation of ECOSSIAN?
8. At its core ECOSSIAN aims to facilitate the sharing of information. Are there any specific concerns at a national level regarding public-private sector cooperation or vis-a-vis the transfer of data (and more specifically cross-border data transfer) in the context of the project?

The countries chosen to form part of this analysis are the following: the UK, Ireland. Italy, France, Portugal and Belgium. These countries have been selected based on the expertise on the partners but also due to contrasting nature of the adoption of the Critical Infrastructure legislative framework. For example neither the UK, Ireland nor France have adopted specific implementing measures to implement the Critical Infrastructure Directive. However, both the UK and France have a centralised system concentrated on the protection of national critical infrastructures (or the French equivalent) whereas Ireland has a decentralised approach dividing power across a variety of government departments and agencies. This decentralised option was also chosen by Belgium, however in contrast to Ireland, Belgium implemented the Critical Infrastructure Directive through specific legislation and accordingly has a much more transparent legislative footing. Similar to France and Belgium both Italy and Portugal implemented their Critical Infrastructure requirements through specific legislation. However, each of these contains its own unique take on this framework. Moreover the adoption and interaction of this legislation with the implementation of the Data Protection Framework varies in relation to each Member State. Despite this disparity it must be acknowledged that these 6 countries are merely a flavouring of the disparities that exist in the national implementing measures of the Critical Infrastructure Protection and Data Protection legislation. As such, in order to have a true assessment each of the 28 Member States would have to be assessed individually (something that is not possible under the terms of this deliverable). Accordingly the attention will now turn the various national implementing measures under the terms of the specified questions.

3.1 Country Report – United Kingdom

As noted in the interim review on the implementation of the Critical Infrastructure Directive some of the Member States ‘did not have any overarching national CIP laws in place, even

though they had internationally leading CIP programmes (e.g. the Netherlands, UK).' [62] In the UK, the Centre for the Protection of National Infrastructure (CPNI) is the Government authority responsible for giving security advice to businesses and organisations regarding critical infrastructure protection. The Security Services Act (1989) provides the basis under which the CPNI operates. The centre is interdepartmental in nature and relies on the resources of a number of Government departments and agencies as well as from the private sector (e.g. academia and industry). In particular, in relation to the sectors under the scope of the project (Transport, Energy and Finance) three particular agencies have responsibility.

- Transport - Department of Transport
- Energy – Department for Energy and Climate Change
- Finance – Her Majesty's Treasury

The CPNI is reliant on resources from the Security Service (MI5 - and is responsible to the Directorate General of the MI5) and CESG (the UK government's National Technical Authority for Information Assurance). The centre was the result of a merger between the National Infrastructure Co-ordination Centre and the National Security Advice Centre and operations began in February 2007. The Centre aims at reducing the threats against the UK's national infrastructure in order to maintain the essential services in particular sectors namely; communications, emergency services, energy, finance, food, government, health, transport and water services. Of clear importance to our current analysis are the respective operations in relation to the transport, energy and finance sectors. The CPNI acts as in the capacity of coordinator and this cooperates with a series of other agencies (namely the Cabinet Office, Office of Cyber Security, Cyber Security Operations Centre, Civil Contingencies Secretariat, Home Office (Minister of Interior), Serious Organised Crime Agency (SOCA), Office for Security and Counter-Terrorism (OSCT), Security Service (MI5) and essentially acts as the primary point of contact for all CIP issues.[63]

Given the high level of interdependency and cooperation it is obvious that there is also a broad overlap *vis-à-vis* the various UK government strategies and policies which come within the operational scope of these organisations and agencies.[64] However, a detailed discussion of this information does not come within the terms of this analysis and our focus must instead shift to an analysis of the CPNI operations and therefore CI Protection in the UK specifically. The Centre has produced a series of reports highlighting best practice guides and policy recommendations in addition to detailed guides on security planning.[65] Furthermore, the Centre also aids in the facilitation and operation of information exchanges.[66]

Aside from the CPNI it is also important to mention the government National Risk Assessments. These forms of assessment have been ongoing since 2005 and form the basis for the National Risks Register. The Register was first published in August 2008 and aims to

[62] Brussels, 28.8.2013 SWD(2013) 318 final COMMISSION STAFF WORKING DOCUMENT on a new approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures more secure Available at: ec.europa.eu/dgs/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure/docs/swd_2013_318_on_epcip_en.pdf

[63] Booz and Company (Italia) S.r.l. 'Study: Stock-Taking of Existing Critical Infrastructure Protection Activities', Final Report JLS/2007/D1/037, 16/10/2009. pp. 428.

[64] See for example the UK's Counter Terrorism Strategy and Cyber Security Strategy)

[65] http://www.cpni.gov.uk/advice/cyber/Good-practice-catalogue/

[66] See Question 4.

provide an assessment of the most significant potential threats to the UK and its citizens over a five year period. In essence, the register gives an overall picture and is designed to complement the Community based Risk Registers by providing a national level analysis.[67] The key piece of legislation behind this initiative is the Civil Contingencies Act 2004 which also provides a definition of emergencies and outlines the responsibilities of emergency responders. As noted by the Booz and Co report:

> 'Understanding the risks and determining their relative significance in terms of potential impact is the starting point for emergency planning. The key to turning this into useful planning information is remembering that it is not the risks themselves that people have to deal with when things go wrong, but their consequences. In an increasingly complex and interdependent society, emergencies can have increasingly complex knock-on effects. The Register identifies both direct and indirect consequences, many of which are common to several risks, and provides information on how to prepare for them.' [68]

The most recently available version (from 2013) provides a detailed analysis of the kinds of potential civil emergencies, outlines the risks associated with such emergencies while also assessing the proposed government responses.

In their assessment of risks the NRA combines historical and scientific data with expert opinions in order to provide an accurate analysis. This process involves three distinct steps: (1) The identification of risks, (2) An assessment of the likelihood of the risks occurring and the potential impact and (3) a comparison of the risks. Having outlined the UK national approach to Critical Infrastructure Protection our attention must now turn to the assessment of the application of this policy and operational framework in the context of privacy and data protection. The analysis in this section will assess the application of this framework in the context of ECOSSIAN through the analysis of the 4 questions chosen as the assessment means.

The Data Protection Directive was introduced into UK law through the Data Protection Act 1998 which came into force on the 1st of March 2000. This replaced the 1984 Data Protection Act which had been a reaction to the international pressures and obligations imposed on them by the Council of Europe Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data. Similar to its predecessor the 1998 Act sets out to implement the Directive 'in as minimal a fashion as possible'.[69] It is significant to note that data protection is a UK-wide matter and is reserved to Westminster. Nevertheless, Scotland has its own Information Commissioner who represents Scottish Data Protection interests in addition to monitoring the separate Scottish Freedom of Information system.

[67] Ie Scotland, Wales and Northern Ireland produce these Community Reports specific to the terms of the communities.
[68] Booz and Company (Italia) S.r.l. 'Study: Stock-Taking of Existing Critical Infrastructure Protection Activities', Final Report JLS/2007/D1/037, 16/10/2009, p.437.
[69] I. Lloyd, United Kingdom: International Encyclopaedia Of Laws: Cyber Law, (Ed.) Jos Dumortier (February 2004) Kluwer Law Series

Thresholds for the application of the Data Protection framework

Regarding the detection and information sharing processes relating to the protection of Critical Infrastructures, what are the key variations in the national implementation of thresholds for the application of the Data Protection framework in the context of ECOSSIAN?

In applying the UK implementation of the Data Protection Directive to ECOSSIAN there a few key variations which need to be highlighted. First, although the Data Protection Directive expressly refers to data subject privacy in Article 1, the term 'privacy' is not in the UK implementation. The 1998 Act defines personal data as:

> 'data which relate to a living individual who can be identified—
>
> (a) from those data, or
>
> (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,
>
> and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual;'

This definition stays substantially in line with the Directive. However, there a few clear differences. For example a distinction is made between 'data' and 'information'. Although this complicates the language somewhat there is no real material difference.[70] Furthermore, the UK act only relates to a living individual. Interestingly, there is also an important distinction in that under the terms of the Directive no reference is made as to whether the all information has to be in the possession of the data controller whereas the UK Act applies to data/information that is in or likely come into the possession of the Data Controller. In the definition of sensitive personal data with the words 'as to' replacing 'revealing' in the definition. Although this is a relatively small difference arguably it is more restrictive than the version found in the Directive.[71]

Accordingly, there is still doubt regarding the practical implications of this definition in UK law.[72] Significant in this regard is the *Durant v FSA* case from 2003 which significantly limited the definition of personal data in the UK. Auld J found that:

> 'Mere mention of the data subject in a document held by a data controller does not necessarily amount to his personal data. Whether it does so in any particular instance depends on where it falls in a continuum of relevance or proximity to the data subject as distinct, say, from transactions or matters in which he may have been involved to a greater or lesser degree.'[73]

[70] Douwe Korff; 'EC Study on Implementation of Data Protection Directive: Comparative Summary of National Laws (Study Contract ETD/2001/B5-3001/A/49)

[71] Douwe Korff; 'EC Study on Implementation of Data Protection Directive: Comparative Summary of National Laws (Study Contract ETD/2001/B5-3001/A/49)

[72] The ICO has issued guidance on the interpretation of personal data from both a technical and non-technical perspective see: http://ico.org.uk/for_organisations/data_protection/the_guide/~/media/documents/library/Data_Protection/Detailed_specialist_guides/PERSONAL_DATA_FLOWCHART_V1_WITH_PREFACE001.ashx and http://ico.org.uk/for_organisations/data_protection/the_guide/~/media/documents/library/Data_Protection/Detailed_specialist_guides/determining_what_is_personal_data_quick_reference_guide.ashx

[73] Durant v Financial Services Authority [2003] EWCA Civ 1746

The court further added that if the data was 'biographical in a significant sense, that is, going beyond the recording of the putative data subject's involvement in a matter or an event that has no personal connotations' then it is probable that it will be regarded as personal data. This was clearly a controversial interpretation which appears to contradict the opinion that was subsequently given by the Article 29 Working Party. This opinion identified three central concepts of data which render it personal – purpose, content and result and in contrast proffered a broad interpretation of the concept of personal data.[74]

The UK ICO has also issued technical guidance on the topic which recommended to broaden the interpretation of personal data to bring it more in line with the Working Party opinion and restrict *Durant*.[75] The UK Courts recently revisited this issue in the *Edam* case[76] and appear to have adopted the ICO recommendations and restricted the application of *Durant*. Essentially the court found that the biographical significance of focus tests should be restricted to factual scenarios judged on a case by case basis where the requested information is not 'obviously about' an individual or clearly 'linked to' them.[77] As noted by Aldhouse:

> Edem is another step in the direction of judicial sanity in refining the meaning of 'personal data'. The decision that names are personal data unless so common as to require supplemental information might be characterised as 'obvious'[78]

The court referred to the Court of Justice decisions of *Lindqvist*[79] and *Bavarian Larger*[80] and it appears that the decision clearly relies on these interpretations. In applying these developments to the project it appears that the convergence in interpretation of personal data brought about by *Edem* simply aligns the UK to the EU definitions and interpretations. Accordingly, if data falling under the EU interpretation and definition of personal or sensitive data is processed during the course of ECOSSIAN's operations then it will be classified accordingly in the UK. Finally, it should be noted cookies are dealt more specifically under the transposition of the E-Privacy Directive more specifically through the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011.

Legitimising the Processes and Operations - Threat Detection

What are the key peculiarities of the relevant national provisions which ensure legal compliance legitimising the processes and operations which may be undertaken in relation to threat detection as a part of the activities to be performed by ECOSSIAN?

[74] Article 29 Working Party, Opinion 4/2007 on the concept of personal data Adopted on 20th June 01248/07/EN WP 136 available at: ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf
[75] http://ico.org.uk/~/media/documents/library/Data_Protection/Detailed_specialist_guides/PERSONAL_DATA_FLOWCHART_V1_WITH_PREFACE001.ashx
[76] Edem v. The Information Commissioner and The Financial Services Authority [2014] EWCA Civ 92
[77] http://www.allenovery.com/publications/en-gb/Pages/Court-of-Appeal-endorses-Information-Commissioner-Office-Guidance-on-meaning-of-personal-data.aspx
[78] Francis Aldhouse, 'Edem v. The Information Commissioner and The Financial Services Authority [2014] EWCA Civ 92', Computer Law & Security Review Volume 30, Issue 3, June 2014, pp. 321–323
[79] C-101/01 Linqvist case Judgment of the Court 6th November 2003
[80] T-194/04 Bavarian Larger JUDGMENT OF THE COURT OF FIRST INSTANCE (Third Chamber) 8 November 2007

The CPNI disseminates a large amount of sector specific guidance and best practice recommendations on threat detection and the installation of appropriate safeguards. These provide valuable information for the operators of Critical Infrastructures. However, the CPNI does not offer the services needed to reply and process this type of attack but instead provides information on the industry service providers. These providers are certified by CPNI and CESG and essentially these Cyber Incident Response services are publicised by the CPNI. However, in the context of ECOSSIAN threat detection and incident management will be inbuilt in the response and therefore the processing of any personal data during this process must be considered in the light of the data protection framework.

Similar to the Directive the UK Act defines processing broadly essentially meaning that virtually all activities relating to personal data will satisfy the processing requirement under the Act. Furthermore, the fundamental data protection principles as provided for under Article 6 of the Directive are directly transposed into the UK Act in Part I of Schedule 1. In their implementation of the Data Quality principles the UK modified their application by providing fixed interpretations. For example, as noted in the technical analysis attached to the first Commission review of the implementation of the Directive:

> 'the law adds an interpretation of the first principle (that personal data must be processed fairly and lawfully), to the effect that personal data are always to be treated as having been obtained fairly if they were received from a person who was 'authorised by or under any enactment [law] to supply it', provided that the rules relating to the provision of information to the data subjects are complied with.'[81]

The corresponding interpretative provisions which expand upon principles 1, 2, 6, 7 and 8 are contained in Part II of Schedule 1. Essential amongst these in our current discussion on this question and a particular point of contrast and contention is the interpretation and variance found in the assessment of the first of these principles namely 'Fair Processing'. The UK provisions links this Fair Processing principle with the legitimate grounds for processing as stipulated in Article 7 of the Directive which is transposed in Schedule 2 Paragraph 1 of the Act. The additional requirements for the processing of sensitive personal data are contained in Schedule 3 of the Act.

The analysis will now turn to an examination of these conditions. As Edwards notes 'except in unusual circumstances such as litigation, the principal requirement for processing of sensitive data is likely to be 'explicit consent'.'[82] Similar to the Irish Act discussed *infra* the UK Act does not define consent. This definition was left out as it was believed to be a concept that was well understood in UK law. As such, it is understood that it is to be given its ordinary meaning and reference to the definition as found in the Directive can be made as the Act is a derivative of the provisions contained therein. As noted by Edwards,

[81] Analysis and impact study on the implementation of Directive EC 95/46 in Member States, available at: http://ec.europa.eu/justice/policies/privacy/docs/lawreport/consultation/technical-annex_en.pdf

[82] Lilian Edwards, 'Privacy and Data Protection Online: The Laws Don't Work', in *Law and the Internet* Lilian Edwards and Charlotte Waelde (eds.), *3rd Ed.* (Hart Publishing 2009).

> 'The ICO has, however, indicated in guidance that consent should be 'informed' and 'unambiguous'. The DPD definition of 'ordinary' consent should also be contrasted as something implicitly less rigorous than the (sometimes equally uncertain) requirement for 'explicit consent' for the processing of *sensitive* personal data.'[83]

This guidance reflect the UK's implementation and the decision to omit the informed element as provided for under Article 2(h) of the Directive from Schedules 2 and 3. There is clearly a slight difference between informed consent and consent and suggests a higher degree of user awareness.[84] This lack of a clear understanding of the concept of consent has led to a certain degree of ambiguity and disparity and this is reflected in the disparity between the interpretations of this term by the Article 29 Working Party and the one found in the original ICO opinion.

The implementation of the third ground namely where the processing is necessary to comply with a legal obligation, is also significant. In comparison to the Directive the UK act is more particular and specifies expressly that this provision does not apply to contractual obligations. For example, in the context of Critical Infrastructure Protection one should consider the application of provisions such as section 17 of the Anti-Terrorism, Crime and Security Act 2001. This allows for the disclosure of personal data under the statutory provisions specified in Schedule 4 for purposes connected with criminal investigation and prosecution, where such disclosures are proportionate. An additional example is found in the Civil Contingencies Act 2004 which provides a framework for modern civil protection mechanisms. As noted in the Government Guidance document on Data Protection and sharing in the context of emergencies:

> Though the key law governing data protection is the Data Protection Act 1998, clear legal power to share data is found in secondary legislation made under the Civil Contingencies Act 2004. The Civil Contingencies Act 2004 (through the regulations made under it) places a duty on Category 1 and 2 responders, on request, to share information relating to emergency preparedness/civil protection work with other Category 1 and 2 responders. This duty relates to the preparedness, response and recovery stages of an emergency.[85]

This is expressed in regulations 45-54 of the Act (and regulations 39-47 of the Scottish implementation). As such, it must be acknowledged that in applying this to Critical Infrastructure Protection the data controller may have legitimate grounds for processing under the terms of specific provisions outlining legal requirements.

Article 7(e) is also of particular importance and relates to processing in the public interest or in the exercise of an official authority and is implemented as the fifth ground in the UK Data Protection Act. It is important to mention this provision as the UK implementation varies somewhat from the Directive. The Act elaborates on the terms to include processing that is

[83] Lilian Edwards, 'Privacy and Data Protection Online: The Laws Don't Work', in *Law and the Internet* Lilian Edwards and Charlotte Waelde (eds.), *3rd Ed.* (Hart Publishing 2009).
[84] Andrew Murray, Information Technology Law: The law and Scoiety, (Oxford University Press, 2010) pp.479-483
[85] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60970/dataprotection.pdf

'necessary' for the administration of justice; for the exercise of 'any functions conferred on any person by or under any enactment [law]'; for the exercise of 'any functions of the Crown, a Minister of the Crown or a government department'; or for the exercise of 'any other functions of a public nature exercised in the public interest by any person'. This appears to have clear application in relation to Critical Infrastructure Protection regarding the detection and information sharing processes. Certainly, CPNI's operations, as a cross-departmental agency concentrated on the protection of public interests, would appear to come within the scope of this exemption provided their actions are proportional.

However, it must be acknowledged that although the CPNI helps through the development of best practice documentation and advisory positions, the sector specific service providers also hold responsibility in relation to threat detection and information sharing. Moreover, in the UK implementation authority is also given to those actions which are for the exercise of 'any other functions of a public nature exercised in the public interest by any person'. This appears to provide an exception for public sector processing for the protection of Critical Infrastructures. Nevertheless, this grounds for legitimate processing may be limited somewhat in that it involves an important balancing step in order to ensure that the processing is proportionate *vis-à-vis* the protection of public privacy and data protection. As such, broad level indiscriminate processing of personal data with the aim of detecting threats that does not respect the data protection principles will not come within the terms of this condition. However, it would appear to be an adequate ground to justify the processing of personal data following an attack.

Accordingly, given the nature of the activities of the project it is likely that one or more of the grounds for processing will be established. However, it must be understood that this gathering needs to be proportionate and must comply with the other data protection principles. For example, the implementation of the purpose specification principle is significant. In relation to this the UK uniquely specifies that the purpose of the processing must be specified 'in particular' in the information that is given to the data subject and in the processing notification given to the data protection authority. It is also important to analyse the implementation of the sixth of the data protection principles, namely the requirement that personal data can only be processed in accordance with the rights of the data subjects as established under the act. These rights are contained in Part II of the act which sets out the provisions provided under Articles 12-14 of the Data Protection Directive.

For the purposes of our current discussion it is the UK exemptions to these rights and the other requirements that necessitates a more detailed analysis. These have been created through the Act itself and a variety of SIs. The exemptions contained in the Act are found in Part IV (sections 28-36 and Schedule 7). As noted by Edwards:

> 'Some exemptions merely allow data controllers to ignore the fair processing and subject access rights provisions, while others exempt the data controller from almost all DPA obligations.'[86]

[86] Lilian Edwards, 'Privacy and Data Protection Online: The Laws Don't Work', in *Law and the Internet* Lilian Edwards and Charlotte Waelde (eds.), *3rd Ed.* (Hart Publishing 2009).

Of particular relevance to our current discussion is section 29 of the Act. Under this provision anyone (even private householders), who are processing personal information in order to prevent or detect a crime are exempt from the fair processing and subject access rules. In this context Edwards gives the example of a shop owner who sets up a security camera who does no need the consent of the data subjects in order to process information to prevent crime.[87] This has an obvious application in the context of ECOSSIAN and would appear to have general applicability. There is also an exemption based on national security as provided for under Section 28 of the Act. This will omit the gathered data from the application of the Act. However, this requires the issuing of a certificate by a Minister of the Crown indicating that the data is held for the purpose of national security. The decision to issue such a certificate is subject to an review as there is a right to issue proceedings in the format of a Tribunal by those who are 'directly affected' and this Tribunal has the power to quash the initial awarding of the certificate.[88]

Guarantees, Liabilities or Requirements

In the application of the national data protection framework to the specific parameters of the project, is the data controller subject to particular guarantees, liabilities or requirements (e.g. administrative/security) which deviate from those under the terms of the Directive and may affect the implementation of ECOSSIAN?

The CPNI provides a host of information detailing with data security and the protection of confidential and personal information. This information is presented in the form of a range of guidance documents and technical notes which focus on improving security protections.[89] The overall focus is split into three parts namely; Cyber Security, Personnel Security (i.e. threats emanating from members of staff) and Physical Security. Regarding the application of these recommendations to the context of personal data security it should be acknowledged that robust protection is required in order to allow the processing. This is provided for in the 7th data protection principle as per part 1 of schedule 1 which states that: 'Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.'

It is therefore left to the particular industry standards to define the parameters of the required protection. In the event of a data breach the ICO has issued guidance on the appropriate means of response and has recommended clear steps. This guidance focuses particularly on: Containment and Recovery; Assessing the risks, Notification of breaches, and Evaluation and response. In general there is no legal obligation for controllers. However, the Information Commissioner has stated that as a best practice serious breaches should be notified to the ICO. The classification of what a 'serious breach' amounts to is not made clear. Nevertheless, an ICO guidance document does make reference to two particular criteria; the potential detriment to data subjects, and the sensitivity of the data lost/released/corrupted.[90]

[87] Lilian Edwards, 'Privacy and Data Protection Online: The Laws Don't Work', in *Law and the Internet* Lilian Edwards and Charlotte Waelde (eds.), *3rd Ed.* (Hart Publishing 2009).
[88] See: Data Protection Tribunal (National Security Appeals) Rules 200 – SI 2000 No. 206.
[89] http://www.cpni.gov.uk/advice/cyber/Good-practice-catalogue/
[90] http://ico.org.uk/~/media/documents/library/data_protection/practical_application/breach_reporting.pdf

A specific case in which notification is mandatory relates to situations in which a breach occurs in an electronic communications service. This requirement was added to the Communications Act 2003 and has had effect since May 2011 (i.e. implementation of the requirement found in the E-Privacy Directive discussed in Chapter 2).

Although generally speaking the failure to notify the Information Commissioner of a breach is not an offence there are five different categories of offence in which the Commissioner can instigate proceedings that are notification related (i.e. processing without notification/supplying information – S30(1)-(2)), failure to comply with a notice (section 47); unlawful obtaining or procurement of data, requiring the provision of certain records (section 56), and obstructing or failing to assist a person in the execution of a warrant (schedule 9 para. 12). The majority of the offences contained in these categories are strict liability offences with a due diligence defence available. Although government departments are exempt from prosecution[91] a 'director, manager, secretary or similar officer' can be found guilty in addition to the data controller where the offence was committed with 'the consent or connivance of or to be attributable to any neglect on the part' of this person.[92] It is also significant to note that the processing of data without the consent of the data controller is also an offence. This has clear significance in relation to ECOSSIAN. However, there are a number of defences i.e. that the information was processed in the public interest or in order to prevent or detect a crime. Accordingly, it is unlikely to have any major impact on the operation of ECOSSIAN. The Information Commissioner has the power to issue enforcement notices under section 40 where he/she 'is satisfied that a data controller has contravened or is contravening any of the data protection principles'. Furthermore, through the adoption of Sections 55A and 55B the Commissioner has the capacity to impose fines.[93]

Facilitating Inforamtion Sharing

At its core ECOSSIAN aims to facilitate the sharing of information. Are there any specific concerns at national level regarding public-private sector cooperation or vis-a-vis the transfer of data (and more specifically cross-border data transfer) in the context of the project?

As mentioned in the initial analysis of the UK implementation the CPNI acts as the facilitator of certain information exchanges. As noted by the Booz & Co. EC report:

> 'The sharing of information about the risks facing networks is self evidently beneficial to both government and industry. If a mechanism can exist through which one company can learn from the experiences, mistakes, and successes of another, without fear of exposing company sensitivities to competitors and the media, then every participant can improve their level of assurance.'[94]

[91] Section 63(5)
[92] Section 61
[93] Inserted by the Criminal Justice and Immigration Act 2008.
[94] Booz and Company (Italia) S.r.l. 'Study: Stock-Taking of Existing Critical Infrastructure Protection Activities', Final Report JLS/2007/D1/037, 16/10/2009 p.442

According to their website the CPNI works with fourteen different industry specific exchanges.[95] There are some of these specific exchanges that are worth special mention in the context of ECOSSIAN. First, the Financial Services Information Exchange (FSIE) which is operated in cooperation with Her Majesty's Treasury and was launch in 2003. This aims to exchange information confidentially regarding electronic security threats, vulnerabilities incidents and solutions. The Transport Sector Information Exchange (TSIE) runs in cooperation with the Department for Transport. This exchange was formed in 2006 and has expanded to cover other major transport methods in addition to the aviation sector that it was initially established to cover.

Another Transport initiative is the Aerospace and Defence Manufacturers' Information Exchange which was also formed in 2006 to cover information relating to electronic security threats in the aerospace defence sector. Finally, the Department for Energy and Climate Change has also been involved in a specific initiative namely the SCADA and Control Systems Information Exchange (SCSIE) which was formed in 2003. It facilitates the sharing of information regarding electronic security threats, vulnerabilities, incidents and solutions specific to the sector. In their Code of Practice on Data Sharing the ICO note that there are two types of data sharing:

1. systematic, routine data sharing where the same data sets are shared between the same organisations for an established purpose; and
2. exceptional, one-off decisions to share data for any of a range of purposes.

In the context of ECOSSIAN it would seem that the data sharing in question would fall into the first category. It should be noted that the considerations vis-a-vis data sharing vary in respect of the public and private sector.

The public sector can have express and implied powers as well as an express obligation whereas private sector bodies have the capacity to share data provided it does not violate the Data Protection Act or other law. For example restrictions in the memorandum and articles of associations and also, in cases of private sector organisations carrying out functions of a public nature, the obligations under the Human Rights Act 1998 (implementation of the ECHR and more specifically Article 8)) should be considered. In the government guidance document on information sharing in the context of an emergency it is noted that this balancing also applies in relation to the common law duty of confidence.[96] Moreover, as noted in the Code of Practice;

> 'Private and third sector organisations should have regard to any industry-specific regulation or guidance about handling individuals' information as this may affect

[95] ADMIE - Aerospace and Defence Manufacturers Information Exchange, CIPSIE - Communications Industry Personnel Security Information Exchange, CNSSIE - Civil Nuclear Sector SCADA Information Exchange, FSIE - Financial Services Information Exchange, MSPIE - Managed Service Providers Information Exchange, NIXIE - Northern Ireland Cross-Sector Information Exchange. NSIE - Network Security Information Exchange, PIIE - Pharmaceutical Industries Information Exchange, SCSIE - SCADA and Control Systems Information Exchange, SPIIE - Space Industries Information Exchange, SRIE - Security Researchers Information Exchange, TSIE - Transport Sector Information Exchange, VSIE - Vendor Security Information Exchange, WSIE - Water Security Information Exchange - See more at: http://www.cpni.gov.uk/about/who-we-work-with/information-exchanges/#sthash.NmpVnvC3.dpuf

[96] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60970/dataprotection.pdf

> the organisation's ability to share information. They should also be aware of the legal issues that can arise when sharing personal data with public sector bodies. This becomes more of an issue as private and third sector bodies are carrying out a wider range of traditionally public sector functions.'[97]

Given the particular context of ECOSSIAN it is perhaps worth mentioning some of the grounds legitimising processing as highlighted by the Code of Practice regarding Data Sharing. As noted *supra* in the analysis of question two, consent is the normal legitimising ground to justify data processing but in reality in the application of the project the processing is more likely to be justified under the grounds of preventing or detecting a crime or the apprehension or prosecution of offenders. These grounds provide an exemption from the fairness requirements of the DPA, however this is limited 'only to the extent that applying these provisions would be likely to prejudice the crime... purposes.'[98] As such, the grounds provided for (as outline in detailed above) are applicable. In summary these grounds are: the third ground namely where the processing is necessary to comply with a legal obligation and the fifth ground processing in the public interest or in the exercise of an official authority found in Schedule 2 Paragraph 1; as well as the other exemptions found in both the act (see sections 28-36 and Schedule 7) and SIs.

It should also be noted that there is a certain level of cooperation internationally in the UK. Similar to the Irish Act (discussed below) the UK Data Protection provisions stipulate that transfers outside the EEA should not be allowed, 'unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.' This contrasts with the Directive which merely refers to transfers to third countries. The principle is accompanied by interpreting provisions in Schedule 1, Part II, paras 13-15 and by Schedule 4 (which illustrates situations where this principle is not applicable). The principle requires an assessment of 'adequacy' on country-by-country basis where the data controllers are obliged to notify the Commissioner of transfers to countries outside the EEA. The derogations are provided in Schedule 4 and implement Articles 26(1)-(2) of the Directive. The grounds provided for under Article 26(2) are implemented in 2 distinct procedural situations where the transfer:

1. 'is made on terms of a kind approved by the Commissioner' or
2. It 'has been authorised by the Commissioner'.

The assessment of adequate protection is therefore significant. However, in the context of ECOSSIAN it appears that all information processing is limited to within the EU. However, it should be noted given the global nature of the threats that for future development these conditions will need to be satisfied in order to legitimately transfer data.

Retention: In response to the invalidation of the Data Retention Directive at an EU level the UK government acting quickly and introduced emergency legislation after just 3 months. Although the initial implementation is still in force they are vulnerable to judicial review

[97] http://ico.org.uk/for_organisations/data_protection/topic_guides/~/media/documents/library/Data_Protection/Detailed_specialist_guides/data_sharing_code_of_practice.ashx
[98] http://ico.org.uk/for_organisations/data_protection/topic_guides/~/media/documents/library/Data_Protection/Detailed_specialist_guides/data_sharing_code_of_practice.ashx

following the CJEU decision. The recent impact assessment recognises that the amendments do not overcome all the stumbling blocks highlighted by the CJEU regarding the old provisions. Instead the Assessment notes that the judgement only addresses 'where possible' and 'to the extent practicable' the concerns raised by the CJEU judgement and with this in mind recognises the 'risk of being perceived of ignoring the... judgment.' [99]

3.2 Country Report – Italy

The Italian security legal framework is varied and complex. Since 1999 there have been a series of legislative measures implementing a national strategy for the safeguarding of Italian critical sectors. The inter-ministerial decree of the 21st of September 1999 established a working group made up of representatives from the Ministry of Communication, the Ministry of Justice and the Ministry of Internal Affairs. This group was tasked with assessing the network security and communications protection sector as a support to administrative and regulatory interventions. In 2003, through the inter-ministerial decree of the 14th of January, this working group was converted into the Permanent Observatory for Network and Communications Protection and Security, within the Ministry of Economic Development, with the task of taking into account the technological and regulatory evolution of the various aspects of the telecommunications sector.

In October 2001, the Technical Interdepartmental Committee of Civil Defence (Commissione Interministeriale Tecnica della Difesa Civile - CITDC) was established as a political unit supporting organ for the technical coordination of civil defence activities in crisis situations. In March 2003, the Ministry for Innovation and Technology established the Working Group on CIIP, involving representatives from ministries participating in critical infrastructure management (Interior, Infrastructure, Communication) and major private providers (ABI, Telecom Italia, WIND). In 2004 this Working Group elaborated the 'Report on Critical Information Infrastructure Protection: the Case of Italy'[100]. Legislative decree no. 155 (31st of May 2005) conferred jurisdiction to the Ministry of the Interior and identified the Postal and Communication Police as the unit responsible for law enforcement initiatives against cyber-attacks on critical information infrastructures. In 2006 the so called 'Tavolo PIC' was established (Inter Ministerial Coordination Platform) and was designated as the Contact Point for the sector of Critical Infrastructure Protection. Tavolo PIC assigned the CITDC the task of establishing the CI identification criteria and coordinating all the activities related to CI protection.

Significantly, in 2008 the Cybercrime Centre for the Protection of Critical Infrastructures (Centro Nazionale Anticrimine Informatico per la Protezione della Infrastrutture Critiche - CNAIPIC) was established. This Centre is a special unit within the Postal and

[99] http://www.parliament.uk/business/publications/business-papers/commons/deposited-papers/?fd=2014-07-09&td=2014-07-31&search_term=Home+Office#toggle-1053

[100] The source of this reconstruction is TENACE, *Protecting National Critical Infrastructures from Cyber Threats*, Center of Cyber Intelligence and Information Security - Università degli Studi di Roma 'La Sapienza', March 2014, available at *http://www.dis.uniroma1.it/~tenace/download/deliverable/Report_tenace.pdf*. TENACE is a research project funded by the Italian Ministry of University and Research.

Communication Police Service[101]. The CNAIPIC acts as a policy authority for all activities relating to prevention, repression and analysis of criminal actions committed against critical infrastructures. Within the realm of this activity the CNAIPIC maintains a dedicated telematic link with the critical infrastructures for the mutual and constant sharing of information. In 2009, the Inter Ministerial Coordination Secretariat for Critical Infrastructures Protection was established within the Italian Presidency of the Council of Ministers. The principal aim of the Secretariat is to ensure a high level of synergy between the initiatives of the various authorities.

In 2010, the Organisation for Crisis Management was established by a ministerial decree issued by the Prime Minister. This reorganised the crisis management system by creating new bodies such as the Inter-ministerial Cyber Crisis Unit (Nucleo interministeriale situazione e pianificazione - NISP)[102]. The principal purpose of the NISP is to monitor the national and international security situation to foresee and prevent possible crises (see Section 5 and Section 6 of the Decree). The European Directive on Critical Infrastructures (2008/114/EC) was transposed in Italy by legislative Decree no. 61 (11th of April 2011).[103] Section 4 of this Decree designates responsibility for the identification and designation of ECI to the NISP (see Section 6 for the ECI identification criteria). Furthermore, the decree designates responsibility for ECI protection to the relevant ministries, the Civil Protection Department and, at a local level, to the prefect with territorial jurisdiction.

Finally, there are two additional developments that are worth considering namely: law no. 133 (17th of August 2012)[104] and the ministerial decree from the 24th of January 2013 issued by the Prime Minister.[105] The latter of these outlines the National Cyber Architecture for Critical Infrastructure Protection. The decree lays the foundations for a comprehensive system: all the entities included in the National Cyber Architecture interact with each other in synergy, under the direct control of the Prime Minister. Furthermore, in December 2013 the 'National Cybersecurity Strategic Framework'[106] and the 'National Plan for Cyberspace Protection and ICT Security'[107] were adopted. The Prime Minister is supported in this endeavour by the Committee for the Security of the Republic (CISR) which may; propose the adoption of legislative initiatives; approve the guidelines to foster public-private partnerships, the policies for enhancing info-sharing arrangements and approves other measures to strengthen cybersecurity. The Committee for the Security of the Republic at Working Level (the so called 'Technical CISR') is in charge of the verification of the timely and correct implementation of the National Plan for cybersecurity, which complements the National Cybersecurity Strategic Framework. Supporting this political level is the national intelligence

[101] CNAIPC carries out its functions into distinct areas of intervention which include, aside from critical infrastructure protection: cyber terrorism; copyright; hacking; e-banking; analysis of emerging criminal phenomena and betting and gaming systems on line.
[102] D.p.c.m. 5 May 2010.
[103] D.lgs. no. 61, 11 April 2011, in http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2011;061.
[104] Lex no. 133, 17 August 2012, in http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2012;133.
[105] D.p.c.m. 24 January 2013, in http://www.gazzettaufficiale.it/eli/id/2013/03/19/13A02504/sg.
[106] Available at http://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-strategic-framework-for-cyberspace-security.pdf.
[107] Available at http://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-cyber-security-plan.pdf.

community. This contributes to the promotion of cybersecurity awareness. The Cybersecurity Unit is established within the Prime Minister Military Advisor's Office with the mandate of coordinating the various institutions that compose the national cybersecurity architecture, preventing and preparing for crisis situations.

The National Cybersecurity Strategic Framework sets out the aims which must be pursued through a joint effort and a coordinated approach of all key stakeholders of the National Cybersecurity Architecture. This Framework sets out a complex notion of information security that includes integrity, availability and privacy. The value of privacy must be considered as an essential element in relation to the implementation of a national cybersecurity architecture. As stated by the Committee on Civil Liberties, Justice and Home Affairs: 'the protection of critical information infrastructure requires an interdisciplinary approach that needs to include the important aspects of civil liberties, justice and home affairs such as internal security, personal data protection and the right to confidentiality and private life, thus enhancing security while respecting fundamental rights'.[108] Accordingly, it is crucial to outline the essential elements of the Italian data protection legislation.

The Data Protection Directive was implemented in Italy through Legislative Decree No. 196 (30th of June 2003) and has been in force since the 1st of January 2004 (following 'the Italian Data Protection Code'). The Code supersedes the Data Protection Act 1996 (lex no. 675/1996), which had come into effect in May 1997. The Italian Data Protection Code is founded upon the following key guiding principles: simplification, harmonisation and effectiveness. The Code is divided into three parts. The first part sets out the general data protection principles that apply to all organisations (public and private). The second part provides additional measures that will need to be undertaken by organisations in specific areas, for example, healthcare, telecommunications, banking and finance, or human resources. Finally, the third part sets out the sanctions and remedies. It is important to outline that the Italian Data Protection Code is not the only legal source in the field of personal data protection. In fact, this Code is complemented by the numerous general provisions issued by the Italian Data Protection Authority (DPA)[109].

The Italian Data Protection Code introduces the right to the protection of personal data and states that 'everyone is entitled to the protection of the personal data concerning him or her'. This right is to be distinguished from the right to privacy or confidentiality. The right to the protection of personal data relates to information about natural persons which is not necessarily relevant to the private or family life of the individual. In comparison, the right to privacy concerns the protection of an individual's private life. In this scenario and also

[108] Opinion of the Committee on Civil Liberties, Justice and Home Affairs of 22 March 2013 on Critical Infrastructures Protection. Achievements and next steps: towards global cyber - security (for the Committee on Industry, Research and Energy) Available at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A7-2012-0167+0+DOC+XML+V0//EN#top.

[109] The Italian Data Protection Authority is an independent authority set up to protect fundamental rights and freedoms in connection with the processing of personal data, and to ensure respect for individuals' dignity. The Authority was set up in 1997, when the former Data Protection Act came into force. It is a collegiate body including four members, who are elected by Parliament for a seven-year term.

considering the accepted notion of personal data (see the following section) the Italian Data Protection Code could be regarded as an act concerning the use of information: not limited to defining rules for confidential data, it deals also with the circulation of data in general. Data protection is granted in a broad sense and with a high level of protection. Therefore, it is appropriate to maintain that such a code practically operates as a stimulus to acquire a full understanding of the significance of information. This is clearly the case for public institutions, which often show little awareness of the huge deposits of information under their control. In conclusion, information is an asset to be aware of for companies and public administrations: it is a valuable resource to protect and defend using the instruments provided by the law.

Thresholds for the application of the Data Protection framework

Regarding the detection and information sharing processes relating to the protection of Critical Infrastructures, what are the key variations in the national implementation of thresholds for the application of the Data Protection framework in the context of ECOSSIAN?

In general, it is fair to assume that there are no major substantive differences between the Directive and the Italian Data Protection Code as it is considered to be a rigorous implementation of the European Directive. However, there are some subtle peculiarities which should be noted. As in other Member States, the definition of personal data is crucial to understanding the approach of the Italian implementation. According to Section 4(1)(b) of the Italian Data Protection Code, 'personal data shall mean any information relating to natural persons that are or can be identified, even indirectly, by reference to any other information including a personal identification number'. Without going into excessive detail, it can be surmised that similar to the other Member States analysed the Italian definition of personal data is also broad and includes all information directly or indirectly related to a natural person. The reference to data instead of documents and writings (i.e. the material supports where the data are stored) can be seen as an enhancement and a refinement when compared with previous Italian legislative implementation. That is not to say that in the past such a concept was not protected. However, the degree of awareness of the distinction between data as an intangible asset and the support where this is stored is a rather modern accomplishment.

Distinct from Directive 95/46/EC, the Italian Personal Protection Code defines anonymous data explicitly as 'any data that, in origin or after being processed, cannot be connected to an identified or identifiable person'. This definition has three key elements: the notion of data, the connection between the data and a person, and the identifiability of the latter. These elements reflect the essential components of the definition of personal data that is contained in the Directive 95/46/EC[110]. The essential element in the definition of anonymous data is the lack of a connection between this data and an identified (or identifiable) person. Indeed, the distinction between anonymous and personal data strictly depends on this connection. As previously indicated, according to the Italian law, the definition of personal data is wide and

[110] G. Finocchiaro, *Anonymity and the Law in Italy*, in Aa.Vv., *Lessons from the Identity Trail*, Kerr - Steeves - Lucock (edit by), Oxford University Press, 2009, 523.

generic. As such, this presents a problem in that according to the definition of personal data given by the Italian law, all possible links between a person and information can be considered as personal data and more subjects can be involved with multiple connections. For example, data concerning 'a graduated male living in Rome' would not be considered personal data, since it cannot be tied to a specific person even if a great amount of time and manpower is used. Vice versa, data referring to 'Mario Rossi law professor at the University of Rome' should certainly be considered as personal data, since the identification of the person is immediate even with negligible time and manpower. However, it would not be so clear-cut to decide whether data referring to 'a graduated male, living in Rome and working for a university' should be considered as personal data[111]. What is hard to evaluate is how many persons correspond to this description. Nevertheless, even if it merely one it is not so clear how much time and manpower is required to identify him.

In order to address problems like the one reported in previous example, the Article 29 Working Party opinion on the concept of personal data[112] should be consulted. Thus it is necessary to analyse each case on its own merits taking into account the factors highlighted by the Working Party namely: the intended purpose of data processing, the way the processing is structured, the advantage expected by the controller, the interests at stake for the individuals, as well as the risk of organisational dysfunctions and technical failures. The identification process is dynamic and 'should consider the state of the art in technology at the time of the processing and the possibilities for development during the period for which the data will be processed'. The concept of reasonableness is used to assess identifiability. This concept is commonly used in the legal system as a criterion to measure how easily a data subject can be linked to the data. This approach highlights the fact that anonymity is a relative concept, and its evaluation requires taking into account the particular context at the time of processing. The degree of anonymity cannot be predetermined: in fact, anonymity may depend on the circumstances and factors perhaps even including the will of the data subject. The concept of anonymity, however, assumes a special weighting I importance of the principle of data minimisation (provided for in Section 3 of the Italian Data Protection Code) which will be discussed in the following section.

Another point to be highlighted is the sensitive data definition stipulated by the Italian implementation. According Section 4(1)(d) of the Italian Data Protection Code, 'sensitive data shall mean personal data allowing the disclosure of racial or ethnic origin, religious, philosophical or other beliefs, political opinions, membership of parties, trade unions, associations or organizations of a religious, philosophical, political or trade-unionist character, as well as personal data disclosing health and sex life'. The core of this notion is the expression 'allowing' i.e. not only data that discloses directly (for example) religious beliefs of an individual is considered sensitive, but also data that can disclose indirectly this information. In this scenario a recent decision of the Italian Supreme Court (no. 19365, 22/09/2011) has a particular relevance. This decision has stated that data about the health of

[111] See: S. Mascetti - A. Monreale - A. Ricci - A. Gerino, *Anonymity: a Comparison between the Legal and Computer Science Perspectives*, in Aa.Vv., *European Data Protection: Coming of Age*, Springer, 2013, 92.
[112] See: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf.

a child is also considered as 'sensitive data' of the child's parents: therefore parents in this situation have their own enforceable rights.

Legitimising the Processes and Operations - Threat Detection

What are the key peculiarities of the relevant national provisions which ensure legal compliance legitimising the processes and operations which may be undertaken in relation to threat detection as a part of the activities to be performed by ECOSSIAN?

Similar to the European Directive, the Italian Data Protection Code defines 'data processing' broadly as 'any operation, or set of operations, carried out with or without the help of electronic or automated means, concerning the collection, recording, organisation, keeping, interrogation, elaboration, interconnection, blocking, communication, dissemination, erasure and destruction'. All activities relating to personal data must observe the data processing general principles indicated by Sections 3 and 11 of Italian Data Protection Code. As stated *supra*, Section 3 of the Italian Data Protection Code introduces the principle of data minimisation. This principle encourages organisations to make use of non-personal data whenever possible. According to this provision:

> 'information systems and software shall be configured by minimising the use of personal data and identification data, in such a way as to rule out their processing if the purposes sought in the individual cases can be achieved by using either anonymous data or suitable arrangements to allow identifying data subjects only in cases of necessity, respectively'.

This provision must be interpreted in conjunction with Section 11 which sets out the general rules applying to all processing operations. These rules provide that personal data must be processed lawfully and fairly; collected and recorded for specific, explicit and legitimate purposes and used in further processing operations in a way that is not inconsistent with said purposes; accurate and, when necessary, kept up to date; relevant, complete and not excessive in relation to the purposes for which they are collected or subsequently processed; kept in a form which permits identification of the data subject for no longer than is necessary for the purposes for which the data were collected or subsequently processed. It is important to outline that these rules are mandatory in nature. Hence, any personal data processed in contrary to any of them breaches the personal data protections under the Italian framework.

Having outlined the general rules applying to all personal data processing, our attention must now turn to the analysis of the additional rules that in the Italian Data Protection Code are different depending on the nature of the data controller. If the data controller is a public entity, only data necessary to reach its institutional tasks shall be processed. In processing data, a public entity shall guarantee the prerequisites and limitations set out in Sections 3 and 11. Consideration must also be given to the different features of the data as well as any additional laws and regulations. Processing of sensitive data shall only be allowed where it is expressly authorised by a law (or by internal regulation) specifying the categories of data that may be processed and the categories of operations that may be performed. Similar to the Irish Act and the UK Act, the Italian Data Protection Code does not define consent but indicates its specific requirements. Consent shall be express (not implicit), given freely,

specifically with regard to a clearly identified processing operation, documented in writing and informed. In case of sensitive data, consent shall be given in writing.

Given the nature of the activities of the project, it is clear that the rules for personal data processing will find application. In brief, we can say that an architecture based on the collection, detection and information sharing must ensure (according to the Italian law) the following general rules. Only (personal) data necessary to one or more specific purpose shall be processed; if it is possible to use anonymous data or suitable arrangements to allow identifying data subjects only in cases of necessity, this processing mode is to be preferred, although more costly and burdensome; the personal data processing must ensure, in any its phase, quality of information and consequently the data subject's rights. In this scenario, it can be understood that, although specific rules are established by Section 53 for personal data processed by the Data Processing Centre at the Public Security Department or by the police and by Section 58 for personal data processing finalized to State defence and security, the processing data also in these cases (finalized to the public interest) must observe the general rules indicated by Section 3 and 11 of the Italian Code. Several provision have been taken by the Italian Data Protection Authority concerning the difficult balance between the value of privacy and the need for public safety. Among the most recent are the DPA Opinion from the 5th of June 2014.[113] In this the DPA expressed a favourable opinion on a draft decree on the organisational arrangements for the Central Direction of the Criminal Police Department of Public Safety.[114]

Guarantees, Liabilities or Requirements

In the application of the national data protection framework to the specific parameters of the project, is the data controller subject to particular guarantees, liabilities or requirements (e.g. administrative/security) which deviate from those under the terms of the Directive and may affect the implementation of ECOSSIAN?

Similar to the Data Protection Directive the Italian Data Protection Code also stipulates that there is no privacy without data security. The 'controller' ('titolare' under the Italian legislation) and the 'processor' ('responsabile') are defined as the subjects in charge with reference to that issue. Section 4(1)(f) of the Italian Data Protection Code defines the 'titolare' as 'the natural or legal person, public administration, and any other body, association, entity which alone or jointly with others determines the purposes, the means and the instruments of the processing of personal data, including the security-related aspects'. Section 4(1)(g) of the 'responsabile' is defined as 'the natural or legal person, public administration and other body, association, entity which processes personal data on behalf of the "titolare"'.

[113] available at http://www.garanteprivacy.it - doc. web n. 3246681

[114] DPA Provision of 31 July 2014, available at http://www.garanteprivacy.it - doc. web n. 3471761: In this the Italian DPA indicated to the Public Security Department of the Ministry of Interior specific provisions in order to guarantee a high security level of the database ('N-S.i.s.') and of information flows of the unit ('S.i.re.n.e').

According to the Italian Data Protection Code, security is not only a computer system-related matter. A truly effective and successful way to manage information security implies an integrated approach: technical, legal and organisational. This clarifies that security depends on a variety of factors, all tightly interconnected, of technical, organizational, computer-based, logistic and procedural nature (see, among other norms, Section 31 of Italian Data Protection Code). Section 31 provides that:

> 'having also regard to the state of the art, to the nature of the data and to all the specifics of the processing, the personal data under processing shall be kept and controlled in such manner as to reduce to the minimum, by the adoption of appropriate and preventive security measures, the risk of destruction or loss of the data, even by chance, the risk of unauthorised data access or processing, and the risk of a processing inconsistent with the purposes of the collection'.

These provisions must be co-ordinated with those of an organisational and technical nature set forth in Annex B to Italian data Protection Code. Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected. In other words, data security is not to be considered just a competence of the information system manager, but many different professional areas of expertise must co-operate in order to attain an adequate level of security. This appears all the more true as the trend is towards the development of devices allowing potentially privacy-invasive capabilities.

Under the Italian Data Protection Code, data controllers (both public and private) are only required to notify the Italian Data Protection Authority when processing higher-risk categories of data. These include, in particular, genetic and biometric data, data processed for the purpose of analysing or profiling individuals, and credit-related information (see Section 37). It is important to outline the 2013 Data Protection Authority General Provision relating to measures on the notification of a personal data breach.[115.] This provision states that the providers of publicly available electronic communications services are required to:

- give an initial, albeit summary, notification to the DPA of any personal data breach suffered by them within 24 hours from the time they become apprised of such breach, and to make available additional information, if any, by 3 days from the initial notification;
- specify, in the notification to the DPA, the reasons why the breach was not detected immediately along with the measures that were or are intended to be taken in order to prevent this from occurring again, if the breach was not detected at the time the relevant event occurred;
- provide to the DPA already in the initial notification of any personal data breach the following information: information necessary to identify the provider; a short description of the breach; information relating to the date (including the estimated date) when the breach occurred and the time when the breach was detected; specification of the place where the data breach occurred, including whether the

[115] Italian Data Protection Authority General Provision 'Implementing Measures with Regard to the Notification of Personal Data Breach - 4 April 2013'Available at http://www.garanteprivacy.it - doc. web n. 2414592.

breach occurred following the loss of mobile devices or media; specification of the nature and type of the data that are (presumably) affected; finally, a short description of the processing or storage systems used for the affected data, including their location;

- notify the contracting parties or other individuals the personal data affected by the breach relate to by 3 days from the time the said providers become apprised of the breach.

A template to be used for the notification to the Italian DPA is attached to this general provision. It is important to outline that also the use of cookies falls under the scope of notification obligations pursuant to Section 37(1)(d), of the Code if it is aimed at 'profiling the data subject and/or his/her personality, analysing consumption patterns and/or choices, or monitoring use of electronic communications services except for such processing operations as are technically indispensable to deliver said services to users'[116]. In relation to the use of cookies, in March 2014 the Italian DPA adopted the general provision relating to the use of cookies and the obtaining of informed consent.[117] This provision distinguishes technical cookies and profiling cookies. Technical cookies are those used exclusively with a view to 'carrying out the transmission of a communication of an electronic communication network, or insofar as this is strictly necessary to the provider of an information society service that has been explicitly requested by the contracting party or user to provide the said service'. The prior consent of data subject is not necessary to install these cookies, whilst information indicated by Section 13 of the Italian Code has to be provided.[118] On the other hand, explicit as well as specific data subject consent is necessary to install profiling cookies.

Facilitating Inforamtion Sharing

At its core ECOSSIAN aims to facilitate the sharing of information. Are there any specific concerns at national level regarding public-private sector cooperation or vis-a-vis the transfer of data (and more specifically cross-border data transfer) in the context of the project?

The Italian Data Protection Code transposed the norms regarding data transfer in Articles 42 - 44 without notable deviations from the European provisions. The rules for legitimising transfers to non-EU countries can be found in Section 43 and include consent, meeting contractual obligations, public interest requirements, safeguarding life/health, investigations by defence counsel, and the use of publicly available data. Additional provisions for legitimising transfers are indicated in Section 44 and include transfers to countries deemed to

[116] The use of cookies was exempted from notification obligations by a decision of the Italian DPA of 31 March 2004 whereby notification was ruled out with regard to processing 'that is related to the use of electronic markers or similar devices whether installed or temporarily stored, in a non-persistent manner, on an user's terminal equipment, as consisting exclusively in the transmission of session IDs pursuant to the applicable regulations for the sole purpose of facilitating access to the contents of Internet sites' (decision No. 1 of 31 march 2004 as published in the Official Journal No. 81 of 6 April 2004).

[117] 'Simplified Arrangements to Provide Information and Obtain Consent Regarding Cookies' Available at http://www.garanteprivacy.it - doc. web n. 3118884.

118 It should be recalled that the failure to provide information or the provision of inadequate information, carry administrative sanctions consisting in payment of a fine ranging from six thousand to thirty-six thousand Euro (Section 161 of the Code).

have adequate protections implemented by the European Commission, the adoption of contractual safeguards, and the use of binding corporate rules. Data subjects are entitled to lodge non-compliance complaints with the said contractual/corporate safeguards. Moreover, the Italian DPA issued specific authorisations to enable data controllers (both public and private) to transfer personal data to third countries that have been found by the European Commission to provide 'adequate' data protection safeguards. Accordingly, to prevent data controllers from having to apply for ad-hoc authorisations, Article 40 of the Italian Data Protection Code provides that 'general authorisations' may also be issued by the Italian DPA. Where a data controller complies in full with the provisions made in the relevant general authorisation, no ad-hoc authorisation will be required for the data transfer. The Italian DPA reserves the right to investigate the processing arrangements and, where appropriate, block or ban the data transfer.

The Italian Data Protection Code has implemented the provisions contained in the e-Privacy Directive 2002/58/EC as well as in the Data Retention directive (2006/24/EC) (see Title 10, Part 2 of the Code). One of the main principles is relating to data retention. Communications service providers (CSPs) are permitted to retain traffic data for only a six-month period in order to deal with disputes over billing and subscriber services (see Section 123). CSPs are also required to retain traffic data for longer in connection with law enforcement purposes; the retention periods are currently set at twenty-four months (telephone traffic data) and twelve months (electronic communications traffic data), irrespective of the given offence at issue (see Section 132). Following ratification of Council of Europe's Cybercrime Convention (via Act no. 48/2008, which amended Section 132 of the Italian Data Protection Code), police authorities were enabled, under specific circumstances, to order IT and/or Internet service providers and operators to retain and protect Internet traffic data - except for content data- for no longer than ninety days, in order to carry out pre-trial investigations or else with a view to the detection and suppression of specific offences. The order issued by police authorities must be notified to and validated by the competent public prosecutor. Following the CJEU decisions from 4th April 2014 (in Joined Cases C-293/12 and C-594/12) which found the Data Retention Directive, the Italian DPA issued a press statement indicating that the judgment promotes a stronger protection of rights. According to the Italian DPA, traffic data are not neutral information and could reveal much about an individual's life. Therefore, an undifferentiated retention of this data for long periods could result in substantial risks.

3.3 Country Report - Ireland

Critical infrastructure Protection in Ireland has been adopted in a rather vague decentralised manner which focuses more on emergency planning in general rather than CI protection in particular. No specific legislation or statutory instrument was adopted in the implementation of the Critical Infrastructure Directive. As per the 2012 Natioanl Risk Assessment;

> At national level critical infrastructure includes airports (including Air Traffic Control), ports, power and communications networks, transport networks, water supply etc. It is the responsibility of each Department to manage its risks and to

ensure that the Agencies or Bodies that fall within its remit have robust risk management systems in place.[119]

As such, several government departments and agencies hold responsibilities in relation to their emergency planning functions. In the event of an emergency the most relevant Government department takes the lead role where they have statutory responsibility and they are assisted if necessary by the other State bodies. The various structures for emegency planning and response were coordinated in 2001 through the creation of the Government Task Force on Ememrgency Planning, the National Coordination Group and the Office of Emergency Planning. The Government Task force is chaired by the Minister for Defence and is comprised of other senior officials from the other Government departments, the Defence Forces, An Garda Siochana (Irish Police Force) and other public authorities with a role in emergency planning. The task force is responsible for the development of top level policy development and coordination in relation to emergency planning.

The National Cordination Group (led by the relevant Minister or the Government as illustrated in fig. 1) is responsible for the national level coordination and management of the national-level response and is located in the National Emergency Co-ordination Centre (NECC) which is a communications centre with meeting rooms and a crisis centre. This crisis centre was established in 2007. According to the guidelines on Emergency Planning its functions include:

- Gathering reports and information, evaluating the emergency/crisis situation from a national perspective and identifying key issues;
- Coordinating the national level response, and linking with the frontline response services as appropriate;
- Ensuring the dissemination/sharing of information (inter-department and agency);
- Setting objectives and identifying priorities in support of the objectives;
- Deciding the efficient allocation of available resources, and seeking additional resources (including international assistance) if required;
- Making decisions in relation to operational cross-cutting issues arising, where appropriate
- Developing and making recommendations in relation to any longer-term policy issues arising;
- Developing a public information strategy (in consultation with the GIS and GPO);
- Agreeing post-emergency review of the response arrangements;
- Other such functions as deemed necessary by the Group.

The Office of Emergency Planning (OEP) is responsible for supporting the Government task force and reports to the Minister for Defence and essentially chairs the Government Task Force Subgroup on Emergency Planning. The OEP also assists in the dissemination of guidelines[120] and risk assessments as they are developed,[121] through their website.[122] In

[119] http://www.emergencyplanning.ie/media/docs/A%20National%20Risk%20Assessment%20for%20Ireland%20Published.pdf
[120] http://www.emergencyplanning.ie/media/docs/Guidelines%20for%20Coordinating%20a%20national%20level%20emergency%20crisis%20response%20Version%202%202013%2003.15.pdf

essence the OEP supports and facilitates in emergency situations. In December 2012, the OEP issued a National Risk Assessment for Ireland, although this document recognised the importance of Critical Infrastructure Protection the focus of the document in relation to their protection focuses on their protection and the potential disruption in relation to natural disasters/extreme weather conditions as opposed to concerted attacks which are dealt with separately as risks in themselves.[123]

This separation reflects the decentralised manner of protection and raises a clear difficulty where two government departments may have the lead in relation to one incident. For example a loss of a critical infrastructure in the transport sector dues to a cyber attack would involve both the departments of Transport and Communications Energy and Natural Resources (as well as a potential whole host of other departments e.g. Justice, Equality and Law Reform, Foreign Affair, Defence). The guidelines for coordinating a National-level Emergency/Crisis Response outlines the initial steps to be taken at the outset of an emergency and more specifically also specifies how the relevant lead government department can be identitified. In this regard it appears to be simply sector specific and in the above example the Department of Transport would take the lead. Having outlined the structure of Critical Infrastructure Protection in Ireland in detail it is now time to see how this emergency planning policy and framework impacts upon the data protection legislation in Ireland. The analysis in this section will assess the application of this framework in the context of ECOSSIAN through the analysis of the 6 questions chosen as the assessment means.

The legislative protection of privacy is provided for under the terms of the Irish Constitution. Although, not expressly provided for, the right to privacy is protected as an unenuerated right as extrapulated from the guarantee of personal rights under Article 40.3. This right has developed through a series of cases originating with the seminal Supreme Court judgement in *McGee v Attorney General*. The Data Protection Act was introduced in 1988 in order to incorporate the 1988 Council of Europe Data Protection Convention into Irish Law. The act aimed to implement Ireland's international commitments and stayed quite close to the original wording of the Convention. This legislative act was the first Data Protection step and provided the foundation for the modern framework. The adoption of the Data Protection Directive necessitated the amendment of the 1988 Act. This resulted in the adoption of the European Communitites (Data Protection) Regulations 2001 (which came into force in 2002).[124] These were subsequently replaced by the Data Protection (Amendment) Act 2003. With the adoption of the 2003 Act Ireland trasposed the parts of the Directive that were not covered by the 1988 Act. The combination of the 1988 and 2003 Acts constitutes the current Data Protection Framework in Ireland. As provided for under s. 23(2) of the 2003 Act these are referred to collectively as the Data Protection Acts 1998 and 2003 and are construed as one.

[121] http://www.emergencyplanning.ie/media/docs/A%20National%20Risk%20Assessment%20for%20Ireland%20Published.pdf
[122] www.emergencyplanning.ie
[123] http://www.emergencyplanning.ie/media/docs/A%20National%20Risk%20Assessment%20for%20Ireland%20Published.pdf
[124] Si No. 626 of 2001

Thresholds for the application of the Data Protection framework

Regarding the detection and information sharing processes relating to the protection of Critical Infrastructures, what are the key variations in the national implementation of thresholds for the application of the Data Protection framework in the context of ECOSSIAN?

In order to adequately assess the application of the Irish implementation of the Data Protection framework in relation to CIP and thus the project, it is necessary to assess some of the key variations. The definition of personal data is key to understanding the scope of the Irish legislation. Article 2(a) provides that:

> '"personal data' means data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller;",

This is a broad definition however it does differ slightly from the one provided for under the Directive. A clear distinguishing feature is that the Irish Act is limited to protecting the data of living persons. A further distinguishing feature is that the Irish Act does not contain the criteria through which an individual may become identifiable. As noted by McDonagh and Crowley, this more 'open ended approach' renders the Irish definition 'potentially broader in scope'.[125] A third difference relates to the fact that under the terms of the Directive it is irrelvant who is in possession of the data which might lead to the indirect identification whereas under the terms of the Irish definition the information must be in the possession of the data controller.

The definition of sensitive data also varies slightly from that outlined in the Directive. The version in the Act is slightly broader in that it includes two additional categories that are not contained in the Directive namely: personal data as to 'the commission or alleged commission of any offence by the data subject'; and personal data related to 'any proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings'. These definitions and the distinction thereof is of extreme importance in the interpretation of both the Act and the Directive. The question of whether particular data sets may identify a particular individual can be a controversial and divisive issue. A particularly apt example in this regard is the debate as to whether IP addresses should be classified as personal data. This confusion is reflected at a fundamental level in Court decisions. In *EMI & Ors v Eircom Ltd,*[126] Charleton J in the Irish High Court concluded that IP addresses do not amount to personal data.

In contrast, one year later the CJEU in *Scarlet v Sabam* found that IP addresses are classified as personal data as they allow users to be directly identified.[127] The Article 29 Working Party have clearly and repeatedly stated that IP addresses amount to personal data

[125] Maeve McDonagh and Louise Crowley, Ireland: International Encyclopaedia Of Laws: Cyber Law, (Ed.) Jos Dumortier (February 2004) Kluwer Law Series
[126] EMI & Ors v Eircom Ltd [2010] IEHC 108.
[127] Case C-70/10, Scarlet v Sabam, November 24, 2011

under the terms of the Directive as they can be traced to a natural person with the cooperation of the internet provider.[128] It is clear that with the development of increasingly powerful processing mechanisms the identity of users can often be ascertained through analysing of large quantities of data linked to IP addresses and other seemingly anonymous data.[129] The Irish Act does not define anonymous data or the process of anonymisation. However, the Act implicitly implies that it does not apply to anonymised data and the Data Protection Commissioner has confirmed this view in a series of opinions.[130]

Accordingly, it appears that the Irish position is somewhat unclear regarding the classification of IP addresses as personal data. However, it must be acknowledged that Charleton J's opinion in the High Court came before the Court of Justice opinion and given that the Irish Data Protection Commmissioner's opinion is in line with the Article 29 Working Party and the Court of Justice. Accordingly, it would seem that the processing activities envisaged by ECOSSIAN will come under the application of the Data Protection legislation in Ireland if IP addresses are processed. It should be noted that this deviation only applies to one particular data type. Hence, given that the processing may involve additional specifically identifying information the processing in ECOSSIAN will come under the application of the Act. Finally, in relation to Cookies these are specifcally dealt with the implementation provided for under E-Privacy Regulations 2011 (S.I. 336 of 2011).

Legitimising the Processes and Operations - Threat Detection

What are the key peculiarities of the relevant national provisions which ensure legal compliance legitimising the processes and operations which may be undertaken in relation to threat detection as a part of the activities to be performed by ECOSSIAN?

The fragmented nature of the Irish cyber security and Critical Infrastructure Protection ecosystem results in a decentralised operator specific threat detection structure. The government strategy has largely omitted to provide any particular guidance on this matter at an industry level. Recommendations and policies have focused on the protection of users and business from fraud rather than on concerted cyber attacks. Attack responses have been aligned to criminal investigative powers. As noted by Buckenham:

> 'Ireland's work in combating cyber-crime is led by the Computer Crime Investigation Unit (CCIU), which sits within the Fraud Investigation Division of An Garda Síochána. CCIU employs approximately fifteen full-time staff of Detective Garda grade or higher, as well as a small number of detectives on secondment from the Paedophile Investigation Unit (PIU). CCIU provides forensic and

[128] Article 29 Working Party, 'Opinion 1/2008 on data protection issues related to search engines' Adopted on 4 April 2008 00737/EN WP 148

[129] Article 29 Working Party, 'Opinion 1/2008 on data protection issues related to search engines' Adopted on 4 April 2008 00737/EN WP 148

[130] See example relating to Health Care Data: http://www.dataprotection.ie/docs/The-Medical-and-Health-Sector/245.htm

investigative support to local policing units and has responsibility for investigating high-tech crime in Ireland.'[131]

The CCIU is aided by the Centre for Cybersecurity and Cybercrime Investigation at University College Dublin. The UCD CCI staff provide training and additional support to the CCIU and the CCIU sits on the European Cyber-crime Training and Education Group board.[132] Therefore, it is clear that these initiaitives are focussed more on post-attack investigation by authorities rather than threat detection. However, in the policy description on the Department of Communications Energy and Natural resources it is noted that '[t]he establishment of a Cyber Security Centre, which relates particularly to the protection of critical infrastructure'[133], is an area that the Communications division is focussing on developing. Aside from the above there have been some private initiatives developed in Ireland that are important to mention given the overall lack of a public structure. Most important in this regard is the Irish Reporting and Information Security Service that provides best practice guides to members on how to prevent security breaches and detect threats. During this threat detection and incident response process personal data may be processed and it is hence import to consider the application of the national data protection implementation in this regard.

Section 2(1) of the Irish Data Protection Act outlines the fair obtaining and processing principle. This stipulates that data controllers are obliged to ensure that personal data should be obtained and processed fairly. This is an implementation of Articles 6(1)(a) and (b) of the Directive. The 2003 Act built upon this foundation by implementing Articles 10 and 11 of the Directive in Section 2D of the Act thus incorporating the fair information principles into Irish law. Data 'processing' is another key concept of the Act and this definition was kept close to that provided for in the Directive. The 2003 amendment introduced a detailed definition that appears to include 'all possible activities involving data.'[134] In order to ensure the lawfulness of the processing of personal data under the terms of the Irish Act one is required to comply with the data quality principles (as provided for under Section 2) and at least one of the conditions provided for under Section 2(A)(1). This section seeks to transpose Article 7 of the Directive by outlining 10 conditions for the legitimate processing of personal data. Section 2(A) permits the processing of data where at least one of the conditions is met. The Irish legislation refers to consent without any qualifying adjective which contrast sharply to Article 7 of the Directive which requires 'unambiguous' consent. It is also significant to note that in comparison to the Directive (in Article 2(1)) there is no definition of what is meant by consent in the Irish Act.

[131] Paddy Buckenham, Cybersecurity: European and domestic responses Briefing paper, The Institute of International and European Affairs, (April 2013).

[132] *Feasibility Study for a European Cybercrime Centre*, Rand Corporation, 2012, http://www.rand.org/content/dam/rand/pubs/technical_reports/2012/RAND_TR1218.pdf

[133] http://www.dcenr.gov.ie/Corporate+Units/Minister/Ministers+Brief/Communications.htm

[134] Maeve McDonagh and Louise Crowley, Ireland: International Encyclopaedia Of Laws: Cyber Law, (Ed.) Jos Dumortier (February 2004) Kluwer Law Series

Although from an intial glance the remaining conditions appear to differ (i.e. numercially there are twice as many), in substance the provisions of the Act stick close to those as provided for under the terms of the Directive. For example as noted by McDonagh and Crowley:

> 'While the condition cocerning the administation of justice in section 2A has no direct counterpart in Article 7, it can be accommodated within the scope of Article 7(e)... or Article 7(f)... .'[135]

In relation to the processing of sensitive data, the Act stipulates that in addition to the provisions set out in Section 2 and Section 2(A) the Data Controller is also required to comply with at least one of the conditions in Section 2(B). This section essentially transposes the requirements found in Article 8 of the Directive. Nevertheless, it is also important to mention the implementation of two of the other principles namely the purpose limitation and the data minimisation principles.

The purpose specification princple in incorporated in Section 2(1)(c)(i) which states that data 'shall have been obtained only for one or more specified, explicit and legitimate purposes'. In addition, Section 2(1)(c)(ii) further clarifies that the data 'shall not be further processed in a manner incompatible with that purpose or those purposes'. The terms explicit and speicifed are not not defined in the Act. Section 2(1)(c)(iii) of the Act is identical to the wording of Article 6(1)(c) of the Directive and essentially implements the sufficiency principle. This stipulates that data 'shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they were collected or are further processed'. This Section links to the time principle as provided for under Section 2(1)(c)(iv) which essentially states that data should not be kept for longer than is necessary as per Article 6(1)(e) of the Directive. Accordingly, in commercial practice the processing of personal information is significantly curtailed through the application of these principles. However, the context of Critical infrastructure protection encompasses a broader public consideration.

In this regard the Irish Act contains a number of provisions that are not expressly provided for under the terms of the Directive and presumably were 'intended to fit within the category of 'substantial public interest' as provided for under Article 8(4).' More specifically this relates to: processing related to the administration of justice, for the performance of a function conferred on a person by or under an enactment and for the performance of a function of the Government or a Minister of the Government; for the performance of any other function of a public nature performed in the public interest by a person. In contrast to the Directive, the Irish Act also develops upon the scope of vital interests of the Data Subject to include serious loss caused by damage to property (in addition to health of the data subject and others as per the Directive). As such, in applying these grounds to ECOSSIAN (and to the protection of Critical Infrastructures more generally) it appears that the associated processing could fall under the legitimate ground of in the adminstration of justice or for the performance of any other function of a public nature performed in the public interest by a person. Nevertheless, it must be understood that any use of such a grounds must be a proportionate to the interests of the data subject and hence precludes indiscriminate monitoring through the processing of personal data.

[135] Maeve McDonagh and Louise Crowley, Ireland: International Encyclopaedia Of Laws: Cyber Law, (Ed.) Jos Dumortier (February 2004) Kluwer Law Series

Guarantees, Liabilities or Requirements

In the application of the national data protection framework to the specific parameters of the project, is the data controller subject to particular guarantees, liabilities or requirements (e.g. administrative/security) which deviate from those under the terms of the Directive and may affect the implementation of ECOSSIAN?

The security of personal data is dealt with in Section 2(1)(d) of the Irish Act. This requires Data Controllers to ensure that 'appropriate security measures shall be taken against unauthorised access to, or unauthorised alteration, disclosure or destruction of, the data, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.' From Section 2(2) it is clear that this applies to both controllers and processors. The 1988 Act failed to give adequate detail in comparison to the requirements provided for under the terms of the Directive and accrodingly the Amendment Act introduced new provisions into the Irish Data Protection Act in order to comply with the security provisions. Section 2C implements these changes by providing guidance to Data Controllers and Processors in relation to how to comply with the security requirements. Subsection (1) provides that when determining the appropriate security measures the data subject should consider: the state of technological development and the cost of implementing the measures. In addition, the data controller is also required these measures are appropriate via-a-vis '(i) the harm that might result from unauthorised or unlawful processing, accidental or unlawful destruction or accidental loss of, or damage to, the data concerned, and (ii) the nature of the data concerned.'

Subsection (2) stipulates that the date processors and controllers take all reasonable steps to ensure that their employees are aware of and comply with the security measures. As noted by McDonagh and Crowley:

> This provision is interesting insofar as it imposes obligations on data controllers in respect of the activities, not only of their employees and contractors, but also of anyone who might happen to be at their premises. The directive, by contrast, does not explicitly impose obligations on data controllers with respect to the activities of employees or such other persons who happen to be at their place of work.[136]

Finally, subsection (3) outlines the requirements for Data Controllers where they employ the services of a Data Processor. The provision stipulates that Data Controllers are obliged to:

> ensure that the processing is carried out in pursuance of a contract in writing or in another equivalent form between the data controller and the data processor and that the contract provides that the data processor carries out the processing only on and subject to the instructions of the data controller and that the data processor complies with obligations

[136] Maeve McDonagh and Louise Crowley, Ireland: International Encyclopaedia Of Laws: Cyber Law, (Ed.) Jos Dumortier (February 2004) Kluwer Law Series

> equivalent to those imposed on the data controller by section 2(1)(d) of this Act,

In addition the Data Controller is also obliged to guarantee that the Data Processor provides 'sufficient guarantees' relating to the technical security and organisational measures governing the processing and finally that the Controller is required to take all 'reasonbale steps' in order to ensure compliance with the measures. The Irish Data Protection Commissioner has given detailed guidelines on best practices to ensure data security.[137] This focueses on issues such as: access control, access authentication (i.e. via strong password creation etc), encryption, anti-virus software and firewalls. Of particular interest in our current analysis is the Code of Practice relating to Personal Data Security Breaches which was adopted on the 29th of July 2011.[138]

This Code developed due to the recommendations established by the Data Protection Review Group which was established in 2009 by the Minister for Justice, Equality and Law reform. The group examined whether changes were required to address data breaches with a particlar emphasis on mandatory reporting. The group issues recommendations in May 2010 which included inter alia:

- Legislation should provide for a general offence by a data controller of deliberate or reckless acts or omissions in relation to the data protection principles – including contraventions of the security principle in relation to data breach incidents. This would complement the existing offence under the Data Protection Acts of failure to comply with an Enforcement Notice issued by the Data Protection Commissioner (DPC) - including an Enforcement Notice directing a data controller to inform individuals of a data breach affecting them
- The reporting obligations of data controllers in relation to data breaches should be set out in a statutory Code of Practice, as provided for under the Data Protection Acts. The Code, broadly based on the current guidelines from the DPC, should set out the circumstances in which disclosure of data breaches is mandatory. Failure to comply with the disclosure obligations of the Code could lead to prosecution by the DPC
- The Code should be reviewed on a regular basis by the DPC and amendments submitted to the Minister as necessary to keep the legislation current
- The DPC should continue to develop his investigation and audit activities in a targeted way, with a particular focus on organisations that hold sensitive personal data, in compliance with emerging risk-based approaches to enforcement
- Legislation should provide for the timely publication of the outcome of such DPC audits, as an aid to good practice and in the interests of transparency
- The DPC should continue to develop public awareness activities in this area[139]

As indicated *supra* the result of these recommendations was the development of the Code of Practice relating to Personal Data Security Breaches. This Code does not apply to providers of publicly availble electronic communications networks or services (i.e. activities which come under the scope of the E-Privacy Directive). According to paragraph 2:

[137] http://www.dataprotection.ie/viewdoc.asp?DocID=1091
[138] http://www.dataprotection.ie/docs/Data_Security_Breach_Code_of_Practice/1082.htm
[139] http://www.justice.ie/en/JELR/Pages/Ahern%20Publishes%20Data%20Review%20Report

> 'This Code of Practice addresses situations where personal data has been put at risk of unauthorised disclosure, loss, destruction or alteration.The focus of the Office of the Data Protection Commissioner in such cases is on the rights of the affected data subjects in relation to the processing of their personal data.'

Essentially the Code focusses on the measures around and obligations of the data controllers and processors relating to incident reporting. It provides the steps to be aware of in the treatment of data breaches. The Code outlines the importance and indeed obligation of informing the data subjects (except where law enforcement agencies have requested a delay)[140] and the Commissioner of the breach and where relvant relevant authorities such as An Garda Siochana (the Irish Police force). As summarised by the ENISA report on data breach notifications in the EU, 'Once the DPA is notified of a breach, the regulator can decide if the data subjects should be notified. If the data controller resists, the DPA can issue an enforcement notice.'[141]

The Code also outlines the mitigating effect of the encryption of data and the presence of adequate security measures. Paragraph 8 of the Code specifies the potential requirement for the data controller to provide a detailed report of the incident. This report 'should reflect careful consideration of the following elements:

- the amount and nature of the personal data that has been compromised;
- the action being taken to secure and / or recover the personal data that has been compromised;
- the action being taken to inform those affected by the incident or reasons for the decision not to do so;
- the action being taken to limit damage or distress to those affected by the incident;
- a chronology of the events leading up to the loss of control of the personal data; and
- the measures being taken to prevent repetition of the incident.'

It is clear that the Code applies in the application of Irish Law in the context of ECOSSIAN. However, it should be noted that this is a best practice self-regulating guide which does not alter the obligations and requirements under the data protection framework. Instead it merely provides guidance and not obligations vis-à-vis incident reporting. Given the aim of ECOSSIAN, the requirements to inform the data subjects immediately of the breach may be mitigated given the investigative nature (as outlined above). However, the steps of informing the Commissioner and the relevant authority i.e. the Police are of clear significance.

Facilitating Inforamtion Sharing

At its core ECOSSIAN aims to facilitate the sharing of information. Are there any specific concerns at national level regarding public-private sector cooperation or vis-a-vis the transfer of data (and more specifically cross-border data transfer) in the context of the project?

[140] As noted in the endnote of the Code: ' Even in such circumstances consideration should be given to informing affected data subjects as soon as the progress of the investigation allows.'
[141] https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/dbn

Currently the law in Ireland relating to the public-private partnerships and transfers of data between these sectors is rather vague. As per Section 2A(1)(b)(iii) the data controller has legitimate grounds to process information 'for compliance with a legal obligation to which the data controller is subject other than an obligation imposed by contract'. Accordingly, it appears relatively clear that given that these attacks would be considered as criminal offences there would be an obligation to disclose information to the national Police force under the Crimnal Justice Act 2011. Any such information would then be sent to the Computer Crime Investigation Unit for investigation. In relation to the finance sector it is significant to note that '[t]he Unit participates in an information-sharing and analysis forum with retail banks based in Ireland and internet service providers, and is in the process of developing a similar forum for telecommunications stakeholders.'[142] It is therefore clear that in the context of ECOSSIAN there appears to be a basis for the public-private sharing of data.

However, this positive obligation does not apply to the transfer of data relating to mere threat detection. There appears to be no formally established threat detection information sharing ties in the transport, energy and finance sectors. Nevertheless, it should be acknowledged that in the transport and energy sectors large portions of the respective market are dominated by state owned (semi-state) corporations and accordingly the divide between the public and private sectors is accordingly not as acute. In the private sector the Irish Reporting and Information Security Service provides incident reporting, alerts and warning services to their clients. Hence, in relation to this sharing of information it is important to acknowledge that if it contains personal data one of the grounds for legitimate processing will need to be satisfied. These have already been discussed (see *supra*) and relate to processing for: the adminstration of justice, the performance of a function in the public interest or for a function approved by the Government through an enactment. In the context of ECOSSIAN the grounds for legitimising the sharing of threat/attack information could be found in one of the grounds indicated above. However, it should be noted that any such sharing would need to be proportionate to the data subjects rights.

The Irish Act transposes the provisions regarding data transfer (as contained in Articles 25-26 of the Directive) in Section 11. The Irish Act refers to countries outside of the European Economic Area whereas the Directive simply refers to third countries. Thus the Irish Act, in contrast to the Directive, does not view these countries as third countries but includes them in the same category as the EU MSs.[143] From Section 11(2)(a) – (b) it is expressly provided for that the assessment of the level of protection in the third country is dependant on the Commission finding an 'adequate level of protection'. As noted by Korff:

> As far as the first derogation mentioned in the Directive is concerned, the Irish law fails to stipulate that 'consent' for a transfer to a country without 'adequate' protection must be 'unambiguous'; and that law also (as in respect of processing

[142] Paddy Buckenham, Cybersecurity: European and domestic responses Briefing paper, The Institute of International and European Affairs, (April 2013).

[143] Maeve McDonagh and Louise Crowley, Ireland: International Encyclopaedia Of Laws: Cyber Law, (Ed.) Jos Dumortier (February 2004) Kluwer Law Series

of 'sensitive data', discussed above, at 7.2) extends the derogation concerning transfers needed to protect the 'vital interests' of data subjects (Art. 26(1)(e) of the Directive) to transfers which are 'necessary to prevent injury or other damage to the health of the data subject or serious loss of or damage to property of the data subject or otherwise to protect his or her vital interests', in cases in which 'seeking [the data subject's] consent to the transfer is likely to damage his or her vital interests'.[144]

This area is particularly relevant given the recent referral by the Irish High Court to the CJEU regarding the legality of the US safe harbour agreement.[145] However, despite the small differences in the implementation the transfering of data will occur within the EEA and therefore no additional obligations need to be satisfied.

The Data Retention Directive was implemented in Ireland by the Communications (Retention of Data) Act 2011. Although not precisely the same, the Irish implementation does closely follow the scope and effect of the Directive. Following the referral by the Irish High Court and the subsequent CJEU decision, which found the Directive contrary to the protections provided for under the Charter of Fundamental Rights of the European Union, it is clear that the Irish implementation suffers from the same defects. However, despite the ruling the Irish implementation remains unaffected and the CRDA will remain in force until it is amended or repealed by the Irish legislator. Accordingly, the position will remain unclear until a definitive decision is made and it would be inadvisable to rely on the terms of the current legislation.

3.4 Country Report - France

Critical Infrastructure Protection and Policy is coordinated in France in centralised manner through the defence and national security agency (SGDSN) under the authority of the Prime Minister. More generally the protection of Critical Infrastructures is based on Decree No. 2006-212 and is now part of the defence code under Article R. 1332-1 to R. 1332-42 (which are based on Article L. 1332-1 to 1332-7 of this Code). These provisions are contained in title 3 (economic defence) chapter 2 (the protection of amenities of vital importance). Interestingly, the French implementation of measures for the protection of Critical Infrastructures pre-dates EU level legislative action and refers instead to '[La] Protection des installations d'importance vitale' (the protection of amenities of vital importance).

However, it must be understood that this includes Critical Infrastructures. Indeed, according to the recent inter-ministerial instruction issued by the SGDSN, the existing provisions implement the Directive adequately.[146] This provides the legislative framework for the development and application of measures against attacks on publically or privately held critical infrastructures. These provisions heavily modified and unified the previously existing provisions that were applicable to 'amenities of vital importance' (Ordonnance No. 58-1371

[144] Douwe Korff; 'EC Study on Implementation of Data Protection Directive: Comparative Summary of National Laws (Study Contract ETD/2001/B5-3001/A/49)
[145] Schrems v Data Protection Commissioner (No. 2) [2014] IEHC 351
[146] Premier Ministre, Secretariat General de la Defense et de la Securite Nationale, ‚Direction Protection et Sécurité de l'Etat: Instruction Generale Interministerielle Relative a la Securite des Activites d'importance vitale' N°6600/SGDSN/PSE/PSN du 7 Janvier 2014 N° Nor : PRMD1400503J

29 December 1958) and sensitive points and networks (Instruction générale interministérielle N° 4600 – 8th February 1993). The PSE (State Protection and security division) of SGDSN deals with the security planning in more detail and the CIP unit falls under this division.

In particular, it is important to note that the documents reference the protection of the security of activities of vital importance (SAIV) and that these activities fit more broadly into the Vigipirate plan framework. This plan is France's national alert mechanism that was established in 1978 and has since been updated several times most recently in 2014. The Vigipirate plan essentially creates a centralised alert system that allows for the warning of interested parties in both the public and private sector in addition to outlining appropriate detection measures. In addition to this it is also worth mentioning Article L.2151-4 of the defence relating to the service and national security code. Under this provision the operators of critical infrastructures must put in place plans relating to continuity and the re-establishment of the service following an attack. The PSE aims at integrating CI protection into this overall framework.

In addition the national agency for the security of information systems (ANSSI) is also of significance. This was created through Decree no. 2009-834 and is the agency with national competence for the protection of Critical Infrastructures. The creation of the ANSSI was inspired by the recommendations made in the 2008 White Paper on defence and national security. The French ISS Operational Centre (COSSI) ensures the implementation of the authority given to ANSSI and is responsible for:

- The analysis of threats
- Identification of the weaknesses of the system and current tools
- The on-going research and classification of attacks
- Defining adequate attack response protocols
- Aiding in the application of urgently required corrective measures

COSSI also hosts CERT-fr (originally CERTA), France's Computer Emergency Response Team. The team aims at detecting the system vulnerabilities, leading the resolution of incidents (with an international cooperation element if necessary), helping establish mechanisms countering future incidents, and establishing a network for confidential sharing of information.

In Articles R. 1332-2 *et seq.* of the Defence Code, (as modified by Chapter 4 of the *Loi de Programmation Militaire*) the sectorial responsibilities are outlined.[147] More specifically the Ministerial order from the 2nd of June 2006, as modified by the order from the 3 of July 2008, sets out the 12 sectors of activity that are of vital importance and the designation of the relevant ministries. In relation to the context of ECOSSIAN of particular importance are Energy (the Minister with the responsibility for Energy), Finance (the Minister with the responsibility for the economy and finance) and Transport (the Minister with the responsibility for Transport). As noted in the recent inter-ministerial instruction issued by the SGDSN, in

[147] As modified by Chapter 4 of the Loi de Programmation Militaire (18th of December 2013) which has added specific provisions relating to security measures).

relation to the sectors covered by the Directive (Transport and Energy) the identification and designation of a European Critical Infrastructure is coordinated by the relevant minister in cooperation with the operator through the application of the SGDSN methodology.[148] European Critical Infrastructures are normally chosen from those selected as amenities of vital importance. Where the ECI is not first classified as an amenity of vital importance the designated infrastructure must at least be covered by an Operator Security plan that which follows the industry standard.

Having overviewed the French approach to Critical Infrastructure Protection our attention must now turn to the assessment of the application of this policy and operational framework in the context of privacy and data protection. The analysis in this section will assess the application of this framework in the context of ECOSSIAN through the analysis of the 4 questions chosen as the assessment means. The Data Protection is covered by the 1978 French Data Protection Act (FDPA). The FDPA was modified to implement the changes brought about by the Data Protection Directive and these entered into force on the 6th of August 2004. There have been a few additional subsequent amendments namely: Law no. 2011-334 of the 29th of March 2011, Ordinance no. 2011-1012 of the 24th of August 2011, Law no. 2013-907 of the 11th of October 2013 and Law no. 2014-344 of the 17th of March 2014.

Thresholds for the application of the Data Protection framework

Regarding the detection and information sharing processes relating to the protection of Critical Infrastructures, what are the key variations in the national implementation of thresholds for the application of the Data Protection framework in the context of ECOSSIAN?

Données à caractère personnel or personal data under the French legislation was modified by the 2004 modification implementing the Data Protection Directive. Article 2 of the FDPA provides that:

> 'Personal data means any information relating to a natural person who is or can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to him. In order to determine whether a person is identifiable, all the means that the data controller or any other person uses or may have access to should be taken into consideration.'[149]

Although this definition stays broadly in line with the Directive there are two differences that are worth highlighting as a comparison with the Directive. First, the FDPA does not mention any of the specific factors that are mentioned 'in particular' the Directive. Second, the final sentence of the French implementation which relates to how to determine whether a person is identifiable is not contain in the corresponding provision of the Directive but instead relates more to the contents of Recital 26. According to Korff:

[148] Premier Ministre, Secretariat General de la Defense et de la Securite Nationale, ‚Direction Protection et Sécurité de l'Etat: Instruction Generale Interministerielle Relative a la Securite des Activites d'importance vitale' N°6600/SGDSN/PSE/PSN du 7 Janvier 2014 N° Nor : PRMD1400503J

[149] All references to the act in English are taken from the official translation available at: http://www.cnil.fr/fileadmin/documents/en/Act78-17VA.pdf

> 'This suggests that, under the Law, the concept of 'personal data' is relative: data can be 'personal' for a controller or another person who has access to the data if that controller or other person has the means to identify the person, but not if the controller or other person does not have those means.'[150]

The French Data Protection Authority, the CNIL interpreted this definition, and thus the concept of personal data, broadly.[151] However, this additional detail relating to identifiability suggest that anonymised data do constitute personal data for the person who has the key to re-identify the data.[152]

There have also been a number of contrasting judgements on the scope of the French implementation vis-à-vis the status of IP addresses which potentially have some impact on ECOSSIAN. As an example of this one can consider the decision of the Paris Court of Appeal that concluded the collection of IP addresses did not constitute the processing of personal data as IP addresses did not fall into the classification.[153] This was also the view taken by the Criminal Chamber of the *Cour de Cassation*. More specifically the Court found that the collection of IP addresses during the process of identifying those committing illegal activities did not amount to data processing and does not fall within the scope of the FDPA.[154] This was later confirmed by the Paris Court of Appeal which further noted that IP addresses were not personal data.[155] It must be understood however, that all of the above decisions relate to the detection of the downloading of illegal materials from the internet and copyright infringement. Furthermore, in contrast to the above the Constitutional Court in its judgement assessing the Hadopi process decided that the collection of data allowing for the identification of a person did amount to the processing of personal data.[156] As such the matter is somewhat confused at the national level but in the current context it is likely that IP addresses will be viewed as personal data. Finally in relation to cookies, the provisions under the E-Privacy Directive were implemented through ordonnance n°2011-1012 (24th of August 2011).

Legitimising the Processes and Operations - Threat Detection

What are the key peculiarities of the relevant national provisions which ensure legal compliance legitimising the processes and operations which may be undertaken in relation to threat detection as a part of the activities to be performed by ECOSSIAN?

[150] Douwe Korff, 'Comparative Study On Different Approaches To New Privacy Challenges, In Particular In The Light of TechnOlogical Developments Contract nr: JLS/2008/C4/011 – 30-CE-0219363/00-28 Country Studies: A.3 – France LRDP Kantor Ltd (Leader) In association with Centre for Public Reform (Final edit – May 2010)
[151] http://www.cnil.fr/documentation/questionsreponses/?faq%5buid%5d=48
[152] Douwe Korff, 'Comparative Study On Different Approaches To New Privacy Challenges, In Particular In The Light of TechnOlogical Developments Contract nr: JLS/2008/C4/011 – 30-CE-0219363/00-28 Country Studies: A.3 – France LRDP Kantor Ltd (Leader) In association with Centre for Public Reform (Final edit – May 2010)
[153] Anthony G. / SCPP Cour d'appel de Paris, 13ème chambre, section B Arrêt du 27 avril 2007 http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=1954
[154] Cour de cassation Chambre criminelle Arrêt du 13 janvier 2009: www.legalis.net/spip.php?page=breves-article&id_article=2563
[155] Cour d'appel de Paris 12ème chambre, pôle 5 Arrêt du 1er février 2010: www.legalis.net/spip.php?page=breves-article&id_article=2852
[156] Décision n° 2009-580 DC du 10 juin 2009: www.conseil-constitutionnel.fr/decision/2009/decisions-par-date/2009/2009-580-dc/decision-n-2009-580-dc-du-10-juin-2009.42666.html

As stated *supra* the SGDSN's efforts to protect Critical Infrastructures is set in the context of the VIGIPIRATE architecture. This involves a series of intervention plans which cover many aspects of threat detection/prevention and mitigation. The Booze and Co. report notes 8 in particular:

- Intelligence and/or detection
- Threat identification
- Alert and preparation
- Governmental organisation management, inter-agency crisis centre activation & communication
- Law enforcement and first responders pre-positioning
- Mitigation / intervention plan activation
- Specific measures activation
- Secondary attack prevention[157]

These goals reflect the involvement of the operators as in order to effectively achieve them a high degree of coordination with public authorities is necessary. The government, through the VIGIPIRATE strategy, guides the risk assessment programme for the relevant sectors. This results in the development of the National Security Directive and this defines the sectors or sub-sectors, those responsible, the processes and issues and the outlines the security needs. The Directive defines the planned and graduated detection, prevention and reaction measures and essentially acts as the frame in which the Operator security Plan is developed.

Hence, unlike the UK, Ireland and Belgium the French authorities play much more of an active role in the implementation of methods to enable threat detection in the relevant infrastructures. Their activities are not limited to the issuing of best practice guides and recommendations. Indeed, CERT-FR has direct involvement in the implementation of measures which aim at preventing and detecting future attacks. More generally as indicated *supra*, this is the one of the operational mission objectives of the ANSSI. This agency also issues detailed analysis of potential threats and in their typology of information security attacks issued detailed information on the specific genres of attack and vulnerabilities that are common. However, threat detection is very much a shared public and private issue due to close supervisory role the public sector plays in the protection of the country's Critical Infrastructures.[158] This is clearly evident in the modifications to the Defence Code provided through the *Loi de Programmation Militaire*. As noted in Art. L. 1332-6-1, the rules relating to the creation of security systems outlined in Articles 21-25 (discussed in more detail under the next question), proscribe the creation of threat detection systems. These systems are operated in France by service providers qualified in information systems security, the national authority system security information or other state services designated by the Prime Minister. Having noted the high level of State involvement it is now appropriate to examine the specific data protection concerns.

Similar to the other MS implementations 'Data Processing' is given a broad definition under the terms of the FDPA which reflects the definition in the Directive. The Data Quality provisions as contained in Article 6 of the Directive are almost directly transposed in the

[157] Booz and Company (Italia) S.r.l. 'Study: Stock-Taking of Existing Critical Infrastructure Protection Activities', Final Report JLS/2007/D1/037, 16/10/2009 p.142
[158] Loi de Programmation Militaire 18th of December 2013.

French Act however slight modifications have been made. For example, in relation to the first data quality ground, data must not only be processed fairly and lawfully but must also be obtained with respect to the same criterion. This specification was in any case perhaps assumed under the Directive. However, despite the slight variations in wording the same substantive criteria are in force. The slight variations in implementation are also evidenced in the grounds for legitimate processing. In comparison to the Directive and the UK and Ireland implementation, consent is used as the primary criterion for the legitimate processing of personal data and all other grounds are implicitly treated as secondary.

Indeed as provided for by the FDPA:

'Processing of personal data must have received the consent of the data subject or must meet one of the following conditions:

1. compliance with any legal obligation to which the data controller is subject;
2. the protection of the data subject's life;
3. the performance of a public service mission entrusted to the data controller or the data recipient;
4. the performance of either a contract to which the data subject is a party or steps taken at the request of the data subject prior to entering into a contract;
5. the pursuit of the data controller's or the data recipient's legitimate interest, provided this is not incompatible with the interests or the fundamental rights and liberties of the data subject.'

Similar to the Irish and UK acts consent is not defined in the French implementation. In addition the above provision refers simply to the consent of the data subject and thus there is no mention of 'unambiguous consent'. It was envisaged that consent was to be given its ordinary meaning under in Civil law. The CNIL has a strict interpretation of this requirement. As observed by Korff: 'The list of remaining criteria in the Law also suggests a certain hierarchy, with the 'better' grounds for processing without consent being listed first.'[159] Of particular relevance to ECOSSIAN are conditions 1, 3 and 5.

The latter of these is the vaguest of the 3 which are applicable. However it is conceivable that it could be used as the protection of the operational integrity of the Critical Infrastructure is of clear importance for the legitimate interests of the data controller. Condition 3 appears to be directed towards public sector bodies in their fulfilment of public tasks and extending merely to the disclosure of data by private/public sector bodies in the fulfilment of that task. Accordingly this could provide a grounds for the sharing of information in the operation of Critical Infrastructures. However, it is important to note that the first condition may also have applicability and as discussed in more detail under the next question this sharing can be required under the Specific Protection Plan. In relation to the processing or sensitive personal data (as specified in Article 8(1)) there are some differences. In particular the FDPA also covers data which indirectly reveals the information listed and this has the clear effect of broadening the scope of the prohibition as the Directive merely refers to data 'revealing' this information.

[159] Douwe Korff; 'EC Study on Implementation of Data Protection Directive: Comparative Summary of National Laws (Study Contract ETD/2001/B5-3001/A/49)

Regarding the grounds legitimising the processing of sensitive data aside from the explicit consent ground and the other specific exceptions, one should consider Article 8(3) which states:

> 'If the personal data mentioned in Section I are, within a short period of time, to be subject to an anonymisation procedure which the CNIL has earlier approved as complying with the provisions of this Act, the Commission may authorise certain categories of processing according to the conditions stipulated in Article 25 (authorisation by the CNIL), taking their purpose into consideration. The provisions of Chapter IX (processing of personal data for the purpose of medical research) and Chapter X (processing of personal medical data for the purposes of evaluation or analysis of care and prevention practices or activities) shall not apply.'

Of particular importance to ECOSSIAN is Article 9 of the Act which states that:

> 'Processing of personal data relating to offences, convictions and security measures may be put in place only by:
>
> 1. the courts, public authorities and legal entities that manage public services, within the framework of their legal remit;
> 2. the representatives of the law for the strict needs of the exercise of the functions granted to them by the law;
> 3. [Provisions considered contrary to the Constitution by decision No. 2004-499 DC of 29 July 2004 of the Constitutional Court];
> 4. the legal persons mentioned in Articles L321-1 and L331-1 of the Intellectual Property Code, acting by virtue of the rights that they administer or on behalf of victims of infringements of the rights provided for in Books I, II and III of the same Code, and for the purposes of ensuring the defence of these rights.'

This provision, and Article 9(1) in particular, appears to legitimise the imposition of security measures as approved by the relevant authorities in the context of Critical Infrastructure Protection as described above in detail. Following a data breach there is no general requirement under French law to report the incident (either to the CNIL or the data subjects concerned). However, given the level of State involvement in the security operations any penetration of the security measures of a critical infrastructure necessitates the sharing with the relevant Critical infrastructure Protection authorities due to the reporting requirements contained in the *Loi de Programmation Militaire* (see next question).

Guarantees, Liabilities or Requirements

In the application of the national data protection framework to the specific parameters of the project, is the data controller subject to particular guarantees, liabilities or requirements (e.g. administrative/security) which deviate from those under the terms of the Directive and may affect the implementation of ECOSSIAN?

There is a high level of State involvement in the assessment of operator security plans in France. The operators of designated infrastructures are required to conduct a risk assessment in order to evaluate threats and vulnerabilities. Following this assessment the operator must develop an operator security plan and a list of all key assets. This plan must contain inter alia: Threat scenarios, Risk assessment and Risk management, security targets, security measures and the list of key assets. The Ministry responsible for the Critical Infrastructure must approved the Security Plan and the list of key assets before the SGDSN confirms the validity of the overall document. As part of the Security Plan a liaison officer must be created for the infrastructure and one of each of its key assets. However, operator responsibility does not stop there as they are also required to develop Specific Protection Plans (which are linked to the Vigipirate plans). Following the creation of this plan the department prefect approves the Specific Protection Plan and creates an External Protection Plan in conjunction with the security representative of the infrastructure and in cooperation with a general officer in the zone of security and defence. Essentially, the External Protection Plan defines the parameters in which the public sector interacts with the private operator and the public sector response to potential threats. This is discussed thoroughly from the mobilisation of man and technical power to the formalisation of the exchange of information (discussed further in the following question).

The Specific Protection Plan must be issued within 2 years and relies on two important aspects in its design:

1. The National Security Directive which corresponds to the relevant sector in which the Infrastructure operates.
2. The Operator Security Plan

Furthermore, it must conform to the standard plan developed by ministerial order. This is developed by the SGDSN with the aim of maintaining some level of coherence between the specific security plans and acting as a guide. In the situation where the operator discovers that it is impossible to fulfil certain criteria or if certain criteria are found to be absent the operator can overcome these difficulties as long as the relevant department prefect approves these differences (the prefect can order changes under Article R. 1332-26 of the Defence Code in consultation with the Zonal Commission for defence and security). The implementation of these plans are for the operator to arrange.

As noted in the recent inter-ministerial report there is a certain level of overlap with some sector specific codes exist and these indicate an automatic equivalence between the specific security plan and the sector specific one found in particular legislation (for example see Articles R. 321-19 and R. 321-26 of the Maritime Ports Code). It depends on the opinion of the prefect of the relevant department in conjunction with the Inter-ministerial Commission on Defence and Security to decide on the total or partial equivalence of security plans taken under such regulations. As noted in the Inter-ministerial Report certain schemes should be noted for example: Article R. 213-1-1 of the Civil Aviation Code, the law on the Modernisation of Civil Security (N° 2004-811 from the 13th of August 2004) and security plans that are elaborated in and apply with international agreements.

Specifically the *Loi de Programmation Militaire* outlines certain specific provisions in Article 22 relating the implementation of security measures to protect information systems. Article L. 1332-6-1 states that the Prime Minister has the power to specify the necessary security measures. These measures are to be implemented at the cost of the Public or Private body. Thus the level of State involvement in the protection of Critical Infrastructures is significant. However, it must be understood that specific Data Protection provisions relating to personal data security also have applicability if the Critical Infrastructure is processing personal data. These requirements aim to ensure that the security measures are up to industry standard. However, given the high level of state involvement in the protection of the IT integrity of the national Critical Infrastructures it is clear that these requirements will likely be fulfilled. Nevertheless, given the key importance of the implementation of these measures in French law it is necessary to analyse them in detail. As noted in the French Guide to the Security of Personal Data, the FDPA:

> 'requires that organisations implementing data processing or holding data files guarantee their security. Data security should be understood as all 'useful precautions, with regard to the nature of the data and the risks of the processing, to preserve the security of the data and, in particular, prevent their alteration and damage, or access by non-authorised third parties' (Art. 34 of the DPA Act). This security must be considered for all the processes applied to this data, whether it is its creation, its use, its backup, its archiving or destruction and concerns its confidentiality, its integrity, its authenticity and their availability.'

Accordingly the FDPA essentially imposes a general requirement to ensure that all measures that should be taken are part of the operator's legal requirements. In this regard one should consider the application of Article 9 of the FDPA as discussed above and more particularly Article 9(1).

In its Guide to the Security of Personal Data the CNIL outlines some best practices in relation to the sharing of information containing personal data. However, much of this is relatively basic best practice advice regarding the 'dos and don'ts' of information transfer and the value of properly encrypting personal data to ensure its security during the exchange. However, as the transfer of data will be one of the clear functionalities of the ECOSSIAN system it is important to analyse the legal structures for sharing information in the context of Critical Infrastructures and with respect to data protection and privacy in more detail.

Facilitating Inforamtion Sharing

At its core ECOSSIAN aims to facilitate the sharing of information. Are there any specific concerns at national level regarding public-private sector cooperation or vis-a-vis the transfer of data (and more specifically cross-border data transfer) in the context of the project?

As has been made clear from the discussion thus far, Critical Infrastructure Protection in France is extremely reliant on a high level of cooperation between the public and private sectors. This cooperation forms part of the entire risk management process. It is clear that in the approval of the various security plans the public sector (SGDSN and the departmental prefect) must approve and therefore review security operations. The External Protection Plan

arranges the sharing of information during a crisis situation, however CERT-FR has clear involvement in the sharing of risk and threat information in a real time way through the creation of network of confidence.[160] All relevant information necessary in the application of the protection of these infrastructures are classified (*Confidentiel Défense*) and are thus required to comply with the rule defined in the general inter-ministerial instruction on the protection of national defence secrets (N° 1300/SGDSN/PSE/PSD 30th of November 2011): Where the operator does not want to share information which it judges is just too sensitive to share, it must instead make reference to the documents which outline the protection measures.

However, the *Loi de Programmation Militaire* specifies in Article L. 1332-6-2 that operators are required to promptly inform the Prime Minister of incidents affecting the operation or security of information systems mentioned. Therefore, despite the fact that there is no general requirement to provide notification of data breaches under the Data Protection Framework this specific Article enunciates a clear sector specific obligation to share information in order to coordinate responses. In relation to other data protection issues, the FDPA transposes the requirements under Article 25 and 26 of the Directive in Chapter XII of the law. This transposition follows the rules enunciated under the Directive closely and essentially legitimises the transfer of personal data within the EU. This contrasts somewhat with the UK and Ireland implementations which has broadened this to the transfer within the EEA, however in the context of ECOSSIAN this does not appear to have an immediate impact. Accordingly transfers to third countries, the requirements they have to satisfy regarding the adequacy of the protections as contained in Articles 68 and 69. It is also worth noting the transposition of the Data Retention Directive. At a national level this was transposed into National law in Articles L. 34-1 of the Postal and Electronic Commuincations Code. This transposition can however be challenged before the Conseil Consitutionel by way of a preliminary decision proceeding question resulting from a pending court case. Until then, the national implementation remains valid and in place.[161]

3.5 Country Report – Portugal

As is the case in almost all European Union countries, we have witnessed in Portugal a gradual increase at the level of critical infrastructures, a direct and necessary consequence of the country's social and economic progress. Although nowadays no country is immune from destructive actions (deliberate or not), natural disasters and other types of threats, the protection of critical infrastructures is of vital significance. At the moment the national plan is being drafted; it is a dynamic process after the identification and classification procedure. The first step was taken in 1984 with the setting up of the *Conselho Nacional de Planeamento Civil de Emergência (CNPCE)*, by Decree Law DL 279/84.[162] However, it was only in 2011 that the *Sistema Nacional de Planeamento Civil de Emergência* (D.L. 62/2011[163]) was firmly established. This legislation transposes the Critical Infrastructure

[160] http://www.cert.ssi.gouv.fr/cert-fr/certfr.html
[161] J Scherer and C Heinickel, 'European Court of Justice Declares Data Retention Directive Invalid', Client alert April 2014 available at: www.bakermckenzie.com/files/Publication/fcf2ef80-c7f6-4361-a782-660857c40248/Presentation/PublicationAttachment/cac82cb1-74a4-4451-bef6-6829c1ecf1c5/ALGermanyPublicLawApril2014.pdf
[162] http://digestoconvidados.dre.pt/digesto/pdf/LEX/39/15129.PDF
[163] http://www.imarpor.pt/pdf/isps/dl_62.pdf

Directive into Portuguese Law. Although it focuses on European Critical Infrastructures (ECI), the same provisions provide for the application of the same procedures in the context of national critical infrastructures. However, application is limited to the energy and transportation sectors.

Moreover, the *Conselho Nacional de Planeamento Civil de Emergência* transferred its powers to the *Autoridade Nacional de Proteção Civil.* This authority is tasked with the mission, at national level and in partnership with entities of a number of areas, to define, update and implement civil emergency planning policies and was established through Decree Law - DL nº 73/2012.[164] This approves the organic structure of the Authority, establishes the tasks regarding civil emergency planning and states in article 2 (1) that:

> 'The mission of the National Civil Protection Authority is to plan, coordinate and implement the civil protection policy, namely to prevent collective risks and the occurrence of serious accidents or resulting disasters, to rescue and assist people and to oversee the fire fighting activity, as well as secure the planning and coordination of national needs as regards civil emergency planning in response to situations of crisis or war.'

1 — The procedure for the identification and designation of European Critical Infrastructures (ECIs) provided for in this Decree Law shall apply to the energy sector, namely:

a) Infrastructures and plants for the generation and transmission of electricity;

b) Infrastructures for oil production, refining, treatment, storage and transmission by pipelines; and

c) Infrastructures for gas production, refining, treatment, storage and transmission by pipelines and terminals for liquefied natural gas (LNG).

2 — The procedure for the identification and designation of European Critical Infrastructures (ECIs) provided for in this Decree Law shall also apply to the transportation sector, namely:

a) Road transport;

b) Rail transport;

c) Air transport;

d) Inland waterway transport;

e) Sea transport, including short sea shipping, and sea ports.

Notwithstanding the fact that the Portuguese State is currently assuming the lead role in ensuring the normal functioning of a large part of critical infrastructures, there is an increasing need to seek the involvement of the private sector not only to achieve this objective, but also as regards emergency planning and response with a view to facing potential hazards which could jeopardize vital sectors of society. Our attention must now turn to the implementation of the Privacy and Data Protection edifice in the Portugal. The Data Protection Directive was been implemented by Law 67/98 of the 26th of October on personal data protection. This act came into force on the 1st of November 1998 and its enforcement is monitored by the 'National Commission for the Protection of Data' also known as the 'CNPD'. Moreover, the *Constituição da República Portuguesa* [Constitution of the Portuguese Republic] recognises data protection as a *sui generis* right. This is contained in Article 35 which specifically highlights the Constitutional importance of Data Protection in Portugal.

[164] http://www.proteccaocivil.pt/Documents/DL%20n%C2%BA%2073-2012%20-%20ANPC.pdf

Accordingly, data protection has a particular constitutional setting within Portugal that is similar to Article 8 of the Charter of Fundamental Rights of the European Union.[165]

Thresholds for the application of the Data Protection framework

Regarding the detection and information sharing processes relating to the protection of Critical Infrastructures, what are the key variations in the national implementation of thresholds for the application of the Data Protection framework in the context of ECOSSIAN?

As with the assessments of the previous Member States it is important to assess the implementation of the concept of personal data. Article 3(a) provides that:

> "Personal data" shall mean any information of any type, irrespective of the type of medium involved, including sound and image, relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an indication number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

This definition stays substantively in line with the one provided for in the Directive however it does define what is meant by 'any information'. Despite this there is really no material difference between the definitions. Similar to the UK the deciphering of whether data is personal following anonymisation depends on the whether there is access to unlocking and identifying the person, thus the definition in Portugal is relative.[166] In relation to the status of IP addresses as personal data, there appears to be no particular discussion around this issue as it appears clear cut that IP addresses are considered as personal data.[167] Significantly Article 35 (3) of the specifically refers to "sensitive data":

> "Information technology may not be used to treat data concerning philosophical or political convictions, party or trade union affiliations, religious faith, private life or ethnic origins, save with the express consent of the data subject, or with an authorization provided for by law and with guarantees of non-discrimination, or for the purpose of processing statistical data that are not individually identifiable."

In relation to the status of cookie data Act 46/2012, of August 29, 2012 transposed Directive no. 2009/136/EC thus implementing the changes to the E-Privacy Directive.

Legitimising the Processes and Operations - Threat Detection

What are the key peculiarities of the relevant national provisions which ensure legal compliance legitimising the processes and operations which may be undertaken in relation to threat detection as a part of the activities to be performed by ECOSSIAN?

In view of the steady increase of transnational threats it is imperative to address globalisation-related phenomena. One of the key instruments that regulates this issue is Act

[165] Douwe Korff; 'EC Study on Implementation of Data Protection Directive: Comparative Summary of National Laws (Study Contract ETD/2001/B5-3001/A/49)

[166] Karen McCulagh, 'A study of data protection: harmonisation or confusion?' 21st BILETA Conference: Globalisation and Hormonisation in Technology Law April 2006, Malta available at: www.bileta.ac.uk/content/files/conference%20papers/2006/Data%20protection%20-%20harmonisation%20or%20confusion.pdf

[167] http://www.timelex.eu/frontend/files/userfiles/files/publications/2011/IP_addresses_report_-_Final.pdf

Lei 109/2009.[168] **This piece of legislation** approves the Cyber-Crime Act and transposes the national legislation the Council Framework Decision no. 2005/222/JHA[169] thus adapting national legislation to the Council of Europe Convention on Cyber-Crime. The National Security Office is a central service under the administration of the State endowed with administrative autonomy, subordinated to the Prime Minister, whose mission is to guarantee the security of classified information, both at national level and within the scope of international organisations to which Portugal is party. Furthermore, the office acts as a clearing authority for people and companies in relation to the accessing and handling of classified information.

Decree Law 69/2014, of May 9, 2014 established the Cyber Security National Centre. The Centre's mission is to contribute to the use of cyberspace in a free and secure way, as well as to monitor anticipation, detection, and incident response regarding cyber attacks. The mission of the Portuguese Criminal Police - Polícia Judiciária (PJ) - is to assist the judicial and prosecuting authorities in investigations, to develop and foster preventive, detection and investigative actions, falling within their jurisdiction or the actions which Polícia Judiciária is entrusted in association with the competent judicial and prosecuting authorities. Within the scope of cyber-crime and cyber terrorism, PJ must be immediately informed of any crimes that are being prepared or executed. The Cyber Crime Office, set up by order of the Attorney General, is the key authority in the internal coordination of the Public Prosecution Service as far as this crime area is concerned. The Office is also involved in the development of scientific training and the creation of communication channels, in particular between criminal police bodies and communication network access service providers, thus enabling criminal investigation cooperation.

Nevertheless despite all these considerations it must be understood that any personal data processing during any threat detection operation will need to satisfy the certain key principles. According to Article 3(b):

> "Processing of personal data" ("processing") shall mean any operation or set of operations which is performed upon personal data, whether wholly or partly by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

The data quality principles are contained in Article 5 and this is a strict implementation of these provisions and therefore the same considerations as discussed *supra* are also valid in the Portuguese implementation. Furthermore, similar to France, the Portuguese implementation of the grounds for legitimate processing consent is also given an elevated status with the additional grounds ranking in order of importance behind this key requirement. This is implemented in Article 6 of the Act which provides:

> 'Personal data may be processed only if the data subject has unambiguously given his consent or if processing is necessary:
>
> (a) for the performance of a contract or contracts to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract or a declaration of his will to negotiate;
>
> (b) for compliance with a legal obligation to which the controller is subject;

[168] http://www.cnpd.pt/bin/legis/nacional/LEI109_2009_CIBERCRIME.pdf
[169] Council Framework Decision no. 2005/222/JHA, of February 24, 2005, on attacks against information systems

(c) in order to protect the vital interests of the data subject if the latter if physically or legally incapable of giving his consent;

(d) for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed;

(e) for pursuing the legitimate interests of the controller or the third party to whom the data are disclosed, except where such interests should be overridden by the interests for fundamental rights, freedoms and guarantees of the data subject.

Clearly Article 6(b), (d) and (e) are of key importance in the context of ECOSSIAN. More specifically one must also consider the potential impact of Article 8(2) which refers to processing concerning suspicion of illegal activities, criminal and administrative offences. This states that:

'The processing of personal data relating to persons suspected of illegal activities, criminal and administrative offences and decisions applying penalties, security measures, fines and additional penalties may be authorized by the CNPD, subject to observance of the rules for the protection of data and the security of information, when such processing is necessary for pursuing the legitimate purposes of the controller, provided the fundamental rights and freedoms of the data subject are not overriding.'

This is similar to Article 7(2) which provides a grounds for the processing of sensitive data:

'The processing of the data referred to in the previous number shall be permitted by a legal provision or by the authorisation of the CNPD when, on important public interest grounds, such processing is essential for exercising the legal or statutory rights of the controller or when the data subject has given his explicit consent for such processing, in both cases with guarantees of non-discrimination and with the security measures provided for in Article 15.'

These provisions appear to add a specific potential justification for the processing operations in the context of ECOSSIAN. Accordingly, there appears to be potential grounds for the operations to be performed under ECOSSIAN if personal data is indeed processed. However these are still required to respect the data quality principles and thus all operations are required to be proportionate vis-à-vis the personal data protection rights of the data subjects.

Guarantees, Liabilities or Requirements

In the application of the national data protection framework to the specific parameters of the project, is the data controller subject to particular guarantees, liabilities or requirements (e.g. administrative/security) which deviate from those under the terms of the Directive and may affect the implementation of ECOSSIAN?

It is clear from the transposition of the Critical Infrastructure Directive that Portuguese operators of Critical Infrastructures are required to implement an adequate Operator Security Plan in order to ensure the security and integrity of their infrastructure. However, if personal data is processed then there is also the overlap with the Data Protection framework implementation and the requirement to adequately ensure the security of the personal data contained therein. Article 14 of the Portuguese implementation of the Data Protection Directive provides that the:

"…controller must implement appropriate, technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental

> loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network…"

Hence, the rather vague requirements for security as enunciated by the Directive are maintained and essentially the form and means of the security protections are left for the Controller to decide upon. There are also more specific security provisions that are outlined in Article 15. These provisions are applicable in scenarios described in Articles 7(2) and 8. Article 7(2) was discussed above but in summary relates to an express legal authority to process on the grounds of public interest or other specific situations highlighted *supra.* Article 8 (1) provides as follows:

> "Central registers relating to persons suspected of illegal activities, criminal and administrative offences and decisions applying penalties, security measures, fines and additional penalties may only be created and kept by public services vested with that specific responsibility by virtue of the law establishing their organisation and functioning, subject to observance of procedural and data protection rules provided for in a legal order, with the prior opinion of the CNPD".

In the absence of an entity responsible for issuing codes of conduct, the CNPD sends binding resolutions and guidance to operators who are responsible for their observation and transmission. The additional measures are required to:

> '(i) prevent unauthorised access to the premises used for processing such data; (ii) prevent data media from being read, copied, altered or removed by unauthorised persons; (iii) prevent unauthorised input and/or control over inputs; (iv) prevent unauthorised use of processing equipment; (v) prevent unauthorised access to data; (vi) confirm the details of the persons to whom the data is transmitted; (vii) keep an audit trail of all inputs; and (viii) protect information while it is being transmitted (which at the CNPD's direction may include encryption). Furthermore, the systems used must guarantee the logical separation between data relating to health and sex life, including genetic data, and other personal data.'[170]

Following any breach of these security systems there is no particular requirement to provide notification either to the data subject or the CNPD (with the obvious exception as provided in the transposition of the E-Privacy Directive).

Facilitating Inforamtion Sharing

At its core ECOSSIAN aims to facilitate the sharing of information. Are there any specific concerns at national level regarding public-private sector cooperation or vis-a-vis the transfer of data (and more specifically cross-border data transfer) in the context of the project?

In order to promote cyber security at the national level, particularly in the context of critical infrastructure protection, the Foundation for National Scientific Computing established the Portuguese Computer Emergency Response Teams (CERT.pt). This has been encouraging a national network of Computer Security incident Response Team (CSIRT), in specifically related critical infrastructure sectors namely: Communications, Energy, Transport, Banking and Public Administration.

As noted by the Booz & Co. report: 'The roles of the CERT.PT include:

[170] https://clientsites.linklaters.com/Clients/dataprotected/Pages/Portugal.aspx#nra

- Offering technical support to computer users in resolving security incidents, advising on best-practices, analysing artefacts, and coordinating actions with the parties involved.
- Gathering and disseminating information about security vulnerabilities and recommended solutions.
- Gathering from accredited sources information related to security vulnerabilities, and working with the community to minimise their impact at the National level.
- Promoting the creation of new CERT/CSIRTs in Portugal, and raising awareness of security issues for computer users.'

Accordingly, one of the main objectives of the CSIRT National Network is to create a cooperation and mutual assistance in handling incidents and sharing of good security practices environment, between privates and public agencies.

However, where such transfers involved personal data certain provisions contained in the national data protection framework must be satisfied. Article 18 of the Portuguese Act states that: "Without prejudice to the tax or customs decisions of the Community, personal data may move freely between Member States of the European Union". Hence, this provision sticks close to the one provided for under the Directive. If the transfer is to country outside the EU the CNPD has the responsibility of deciding whether there is an adequate level of protection. However, as the transfers in the context of ECOSSIAN are within the EU these considerations are of little concern. Finally, it is also worth noting the transposition of the requirements under the Data Retention Directive were implemented through Law n.º 32/2008 from the 17th of July.

3.6 Country Report – Belgium

Unlike the UK, Ireland and France the Belgian government similar to Italy thought it necessary to introduce an implementing measure to adopt the Critical Infrastructure Directive[171]. The implementation of the Directive resulted in the Belgian law on the security and protection of critical infrastructures of 1 July 2011[172] as amended by the Law of 25 April 2014[173]. Despite the clarity that the Belgian Law brings in relation to the legal grounds establishing critical infrastructure protection, it is significant to note that this legislation followed a decentralised approach on sector-level and thus no particular agency has full authority over the issue (Art. 5,-). Instead, similar to Ireland, each government sector holds responsibility for their own sector or competence.

The implementing measures are broader than Directive 2008/114/EC and include, in addition to the Energy and Transport, the Financial and Electronic communications sectors under the scope of the legislation (Art. 4, §4). In relation to the sectors relevant for ECOSSIAN the following departments have competence (Art. 3, 3°, as amended by the Law of 25 April 2014):

- For Transport: the Minister with Transport as part of her portfolio or a chosen delegate from the administration;

[171] 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, *OJ* 23 December 2008, L 345, 75-82.
[172] Belgian Law of 1 July 2011 on the security and the protection of critical infrastructures, *B.S.* 15 July 2011.
[173] Belgian Law of 25 April 2014, *B.S.* 7 May 2014.

- For Energy: the Minister with Energy as part of her portfolio or a chosen delegate from the administration;
- For Finance: the National Bank of Belgium.

It is also significant to note that this initial implementation has been further elaborated upon by certain sector specific legislation, which supplement the original adoption. More specifically these relate to Air[174], Port[175] and Energy sector Critical Infrastructures.[176] However, the Government Crisis and Coordination Centre does help in the overall management and reporting responsibilities to the Commission and the EPCIP (European Programme for Critical Infrastructure Protection).[177] In addition to the organs described above the Belgian Federal Government has also established the Federal Cyber Emergency Team (CERT)[178]. This Emergency Team was set up in 2009 and is operated by Belnet (the Belgian National Research Network)[179] on behalf of Fedict (the Federal Public Service for Information and Communication Technology)[180]. The Belgian CERT's responsibilities cover three particular objectives, namely to:

1. Coordinate organisations in the event of cyber incidents;
2. Advise organisations about finding a solution when cyber incidents arise;
3. Support organisations to prevent these security incidents occurring.

CERT.be recommends a series of sector specific guidelines on threat detection and mitigation. The service helps to tackle and resolve incidents as quickly as possible. They do not sell solutions but instead provide best practice guidance and advice on appropriate solutions. The service offers a whole range of advisories on network gear, operating systems and software. Accordingly CERT.be does not offer the services it recommends vis-à-vis threat detection and mitigation but instead offers a platform on which best practices and potential threat information can be shared in confidence.

Article 22 of the Belgian Constitution determines that everyone has the right to respect for his/her private life. Since 1992 a Belgian Law has ensured the protection of individuals in relation their personal data in particular.[181] This Law establishes the rules for the use of personal data, the obligations for data controllers, and the rights of the data subjects. After Directive 95/46/EC[182] was introduced, the Belgian Law of 8 December 1992 was amended to implement the EU rules for personal data protection by the Law of 11 December 1998[183]. Following this initial implementation several modification have been made, including those of the Law of 26 February 2006[184].

[174] Belgian Royal Decree of 2 December 2011 on critical infrastructures in the sector of air, *B.S.* 27 December 2011.
[175] Belgian Royal Decree of 29 January 2014 on the security and protection of critical infrastructures in the sector of ports, *B.S.* 19 February 2014.
[176] Belgian Royal Decree of 11 March 2013 on the security and protection of critical infrastructures in the sector of energy, *B.S.* 29 March 2013.
[177] See: http://crisiscentrum.be/nl/inhoud/kritieke-infrastructuur-0.
[178] See: https://www.cert.be/nl/wie-zijn-we.
[179] See: http://www.belnet.be/nl.
[180] See: http://www.fedict.belgium.be/nl/.
[181] Belgian Law of 8 December 1992 on the protection of the private life of individuals in relation to the processing of personal data, *B.S.* 18 March 1993.
[182] European Parliament and Council, Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *OJ* 23 November 1995, L 281, 31-50.
[183] Belgian Law of 11 December 1998, *B.S.* 3 February 2011.
[184] Belgian Law 26 February 2006, *B.S.* 26 June 2003.

Thresholds for the application of the Data Protection framework

Regarding the detection and information sharing processes relating to the protection of Critical Infrastructures, what are the key variations in the national implementation of thresholds for the application of the Data Protection framework in the context of ECOSSIAN?

The Belgian Data Protection Law of 8 December 1992 is considered as a rather strict implementation of Directive 95/46/EC. The Law protects the individuals against the unlawful processing of their personal data. The Law does not distinguish Belgian citizens from other individuals. However, it is required that the individual is a natural person. Companies and organisations are not protected by data protection law. Personal data is any information relating to an identified or identifiable natural person (called data subject)(Art. 1(1) Belgian DP Law). The notion of 'personal data' is very broadly interpreted and may cover different types of information, including a person's name, an image, a telephone number, an e-mail address, sound recordings, etc. The only requirement is that the data subject is identifiable through the personal data. This has to be assessed objectively: information should be considered as personal data as long as *someone* is reasonably able to identify the data subject. As such is information still personal data if someone else is reasonably able to use means that identify the individual. For this reason is in Belgium an identification number such as IP address from a computer that is connected to the Internet considered as personal data.[185]

Also the definition of 'processing personal data' is explained broadly. Processing means any operation or set of operations performed on personal data (Art. 1, §2 Belgian DP Law). These operations include the collection, storage, use, modification and disclosure of data. The Belgian DP Law is applicable from the moment personal data are processed by automatic means. However, even when no computer technology, telematics or telecommunication networks are used for the processing, the Belgian DP Law is applicable in cases where the data are part of (or are intended to become part of) a manual file, i.e. an aggregate of data that can be accessed according to certain criteria. It is most likely that the security solution developed during the ECOSSIAN project lifetime will process the personal data of individuals in Belgium (or on whom the Belgian DP Law is applicable).

Legitimising the Processes and Operations - Threat Detection

What are the key peculiarities of the relevant national provisions which ensure legal compliance legitimising the processes and operations which may be undertaken in relation to threat detection as a part of the activities to be performed by ECOSSIAN?

The Belgian DP Law establishes the requirements for the legitimate processing of personal data of individuals. The data controller is responsible for the lawful processing of the data. The controller is the person who determines the purposes and the resources of the processing. In contrast to the data subject, the data controller is not always a natural person, but he can also be a legal person, an un-associated organisation or a public authority.

The controller has to notify the Privacy Commission, prior to the start of the automatic processing operation. An electronic notification form is directly accessible on the Privacy Commission's website: http://www.privacycommission.be. A paper form can be requested on the website, by phone or in writing. The notification is not intended to request authorisation or

[185] Parl. St. Kamer 1997-98, nr. 1566/1, 12; see: J. Dumortier, ICT-recht, Acco, Leuven, 2014, 272.

permission, but is, except from very exceptional cases, a necessity to lawfully process personal data under Belgian Law. Asides from the description of the processing the notification contains also e.g. the name of the processing, the purposes of the processing, the categories of data being processed, the legal basis for the processing, the categories of recipients to whom the data may be disclosed, the safeguards for disclosure to third parties, the technical and organisational security measures to protect the data, etc. For manual operations no prior notification is required. However, Royal Decree of 13 February 2001 excludes a list of automatic processing operations from the requirement of prior notification.[186] These operations include e.g. operations relating to accounting, operations in relation to customer or supplier management and operations carried out by a company with a view to personnel management. It is rather unlikely that the processing operations by the ECOSSIAN solution will fall under one of the exemption categories from the Royal Decree.

Personal data may only be processed for a specified and legitimate purpose. In addition only processing operations that are compatible with the initial purposes are allowed. The extent to which the compatibility reaches depends on reasonability. For example, a fitness club that sells the list of its members to a diet company exceeds what is reasonably expected in this situation. While it is perfectly lawful for a club to keep records of its members, it is not reasonable to disclose this information to third parties. Similarly, issues regarding private-public information sharing in a critical infrastructures context might potentially raise legal issues. However, personal data may be processed if the processing is required by law, decree or ordinance (Art. 5© Belgian DP Law), or when the processing is necessary to perform a task of public interest or a task which is part of the exercise of public authority (Art. 5€ Belgian DP Law) or when the processing is necessary to safeguard a legitimate interest of the controller or of a third party, provided that it is not overridden by the data subject's rights or interests (Art. 5(f) Belgian DP Law). The latter will occur when the controller's interest in the processing is greater than the data subject's interest in *not* processing the personal data.

Further the Belgian Law was amended after EU Directive 95/46/EC was adopted in order to implement all legal requirements for the processing of personal data and to align the Belgian legal framework with the European standards for processing.[187]

Guarantees, Liabilities or Requirements

In the application of the national data protection framework to the specific parameters of the project, is the data controller subject to particular guarantees, liabilities or requirements (e.g. administrative/security) which deviate from those under the terms of the Directive and may affect the implementation of ECOSSIAN?

In principle individuals and operators of critical infrastructures are obliged to organise software security measures on their own behalf. Government involvement is limited to the dissemination of information via the CERT website. The Law of 1st of July 2011 ensures the cyber safety and protection of critical infrastructures. This law forces critical infrastructure operators to indicate a point of contact and to develop a security plan to prevent, mitigate and neutralise the risks of service interruption or infrastructure destruction.

Section 3 of the Belgian implementing measures outlines provisions relating to the internal security measures that an operator must be aware of when protecting a Critical Infrastructure. Article 12 stipulates that the operator of the CI is required to appoint a security

[186] Royal Decree of 13 February 2001, *B.S.* 13 March 2001.
[187] Belgian Law 11 December 1998, *B.S.* 3 February 1999.

contact (who will act as the point of contact for the sectorial authority, the DGCC, the Mayor and the police) and to communicate this information to the sectorial authority within 6 months of being designated as a Critical Infrastructure (the same applies for every update). The information for this point of contact must be publically available. Furthermore, Article 13 states that each CI is required to have an operator security plan which aims at preventing and neutralising the risks associated with an interruption of service or the destruction of the CI (this must be created and implemented within 1 year of the notification of designation as a CI). This Plan must include at a minimum:

1. Permanent internal security plans applicable in all circumstances
2. Gradual internal security measures that apply depending on the level of the threat.[188]

Moreover, the operator security plan must include at a minimum certain key steps, namely:

1. An inventory and location of all parts of the infrastructure that if attacked could cause an interruption to its functioning or its destruction.
2. A risk analysis consisting of the identification of the principal potential threat scenarios caused by intentional acts with the aim of interrupting the functioning or destroying a critical infrastructure.
3. An analysis of the vulnerabilities of the critical infrastructure and the potential impact caused by the interruption of service or destruction based on particular chosen scenarios.
4. In relation to each scenario of the risk analysis, the identification, selection and designation in order of priority of the internal security measures.

However, the particular form that this Operator Security Plan is to take is left to this discretion of the operator. As stated *supra* CERT.be recommends particular security protocols and standards which aim at mitigating the threats posed by cyber-attacks. It should also be acknowledged that certain if personal information is involved then there are certain security provisions under the Data Protection framework that also need to be considered. This complements the data security principle provided by Article 16 of the Belgian DP Law. Article 16(4) states that the data controller must take the appropriate organisational and technical measures to safeguard the personal data being processed. More specifically, the appropriate level of protection must be assessed, taking into account the technical state of the art and the costs of the measures, on the one hand, and the nature of the personal data and the likely risks that relate thereto, on the other.

Facilitating Inforamtion Sharing

At its core ECOSSIAN aims to facilitate the sharing of information. Are there any specific concerns at national level regarding public-private sector cooperation or vis-a-vis the transfer of data (and more specifically cross-border data transfer) in the context of the project?

Sharing between public-private sectors is a crucial element in the fight against cybercrime and to guarantee the quality of any cybercrime policy. There are many actors, and most critical infrastructures are private. Therefore, the State must rely on information sharing with other involved private actors. There is currently no systematic information-sharing system available in Belgium. Although the CERT has access to a worldwide system to share information, this platform is not yet used sufficiently by organisations and government institutions.

[188] Article 13(2)

According to Belgian law the transfer of lawfully processed personal data to another EU country is permitted (Art. 21, §1 Belgian DP Law). However, outside the European Union, and more broadly outside the European Economic Area, personal data may only be transferred to countries ensuring an adequate level of protection equivalent to that in the Member States of the European Union. The adequacy of the level of protection in countries outside of the EU, will be assessed by the European Commission (art. 21, §2 Belgian DP Law). If the country of final destination for a data transfer is not included in the European Commission list, the transfer is still possible if the adequate level of protection is ensured by means of a contract. In Belgium such a contract needs to be authorised by Royal Decree, following the opinion of the Belgian Data Protection Authority (Art. 22 Belgian DP Law).

In addition, multinationals can also provide sufficient safeguards for data protection through internal codes of conduct. Those Binding Corporate Rules have to be ratified by the different national DPAs involved in the data flows. Finally, even in the absence of an agreement, Article 22, 1°-6° Belgian DP Law provides 6 exemptions which allow lawful transfer of personal data to third countries. For example, when data subject gives their unambiguous consent to transfer the data to a third country or if the transfer is necessary to perform a contract with the data subject. Finally it is also worth noting the implementation of the Rata Retention Directive. The Belgian legislator established the general framework for data retention obligations in the Belgian Law from the 30th of July 2013.[189] The Royal Decree of 19th September 2013[190], which determines the details of the retention, finalised the implementation. The Belgian implementation is broader than the EU Directive as electronic communications providers are to retain significantly more information than required under the EU Directive.

3.7 Country Level Analysis Conclusions

As has been made clear from the analysis set out above there is a high degree of disparity in the application of a security framework amongst the chosen Member States. Moreover, despite compliant implementation of the Data Protection Framework subtleties in implementation exist. Hence, this examination has highlighted the specific need for an awareness of the variance in implementation at a national level. This has a specific impact not only on the rules for the implementation of ECOSSIAN at an O-SOC and N-SOC level but also on the selection of country in which the E-SOC as a data subject will be located. This is an issue which should be weighted carefully.

[189] Belgian Law 30 July 2013 amending Articles 2, 126 and 145 of the Electronic Communications Act of 13 June 2005 and Article 90decies of the Code of Criminal Procedure, *B.S.* 23 August 2013.
[190] Royal Decree 19 September 2013 on Article 126 of the Electronic Communications Act of 13 June 2005, *B.S.* 8 October 2013.

Chapter 4 Conclusion

This deliverable has outlined the current EU approach and highlighted in variance in adoption at a national level through an assessment of the implementation in the UK, Italy, Ireland, France, Portugal and Belgium. In the EU level analysis the current and proposed legislative framework has been assessed in detail in relation the application of the Critical Infrastructure Protection mechanisms and the Privacy and Data Protection Framework. The National level assessment has provided an insight into the variance in application of the national level implementations. This assessment provides an insight into the considerations that will be necessary to consider in the implementation of the ECOSSIAN solution. This initial Deliverable will form the basis of the future Deliverables and in particular D7.2 (Legal Requirements) and D7.3 (Information Sharing Policies).

Chapter 5 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 6 Bibliography

6.1 Primary Sources

Legislation

xvii. EU

Council of Europe Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data

European Convention of Human Rights

Charter of Fundamental Freedoms of the European Union

European Parliament and Council, Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *OJ* 23 November 1995, L 281, 31-50.

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

Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws

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)

Framework Decision 2008/977/JHA of November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.

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, *OJ* 23 December 2008, L 345, 75-82.

Resolution 2011/2284(INI) on Critical Information Infrastructure Protection - achievements and next steps: towards global cyber security

Directive 2005/65/EC of the European Parliament and of the Council of 26 October 2005 on enhancing port security

Regulation (EC) No 725/2004 of the EP and of the Council of 31 March 2004 on enhancing ship and port facility security

Regulation (EC) No 2320/2002 of the European Parliament and the Council of 16 December 2002 establishing common rules in the field of civil aviation security; and its implementing regulations and amendments

Regulation (EC) No 300/2008 of the EP and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002

Regulation (EC) No 2096/2005 of 20 December 2005 laying down common requirements for the provision of air navigation services

Regulation (EC) No 550/2004 of the EP and of the Council of 10 March 2004 on the provision of air navigation services in the single European sky

Regulation (EC) No 1315/2007 of 8 November 2007 on safety oversight in air traffic management and amending Regulation (EC) No 2096/2005

xviii. UK

Data Protection Act 1984

Data Protection Act 1998

The Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011.

Data Protection Tribunal (National Security Appeals) Rules 200 – SI 2000 No. 206.
Criminal Justice and Immigration Act 2008.

Security Services Act (1989)

Civil Contingencies Act 2004

Anti-Terrorism, Crime and Security Act 2001

Civil Contingencies Act 2004

Human Rights Act 1998

xix. Italy

Legislative decree no. 155 (31st of May 2005)

Legislative Decree No. 196 (30th of June 2003)

D.p.c.m. 5 May 2010.

D.lgs. no. 61, 11 April 2011, in http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2011;061.

Lex no. 133, 17 August 2012, in http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2012;133.

D.p.c.m. 24 January 2013, in http://www.gazzettaufficiale.it/eli/id/2013/03/19/13A02504/sg

xx. Ireland

The Data Protection Act was introduced in 1988

European Communitites (Data Protection) Regulations 2001

E-Privacy Regulations 2011 (S.I. 336 of 2011).

Crimnal Justice Act 2011

Statutory Instrument No. 626 of 2001

xxi. France

Defence code

Law no 2013-1168 Loi de Programmation Militaire 18 décembre 2013

Ordonnance No. 58-1371 29 December 1958) and sensitive points and networks (Instruction générale interministérielle N° 4600 – 8th February 1993

Decree no. 2009-834

1978 French Data Protection Act (FDPA) - All references to the act in English are taken from the official translation available at: http://www.cnil.fr/fileadmin/documents/en/Act78-17VA.pdf

Law no. 2011-334 of the 29th of March 2011,

Ordinance no. 2011-1012 of the 24th of August 2011,

Law no. 2013-907 of the 11th of October 2013

Law no. 2014-344 of the 17th of March 2014.

Ordonnance n°2011-1012 (24th of August 2011).

Civil Aviation Code,

The law on the Modernisation of Civil Security

Postal and Electronic Commuincations Code.

xxii. Portugal

Decree Law DL 279/84, of August 13.

D.L. 62/2011, de 09 de May

Decree Law - DL nº 73/2012

Lei 67/98

Constituição da República Portuguesa [Constitution of the Portuguese Republic]

Act 46/2012, of August 29, 2012

Lei 109/2009

Decree Law 69/2014, of May 9, 2014

xxiii. Belgium

Belgian Law of 1 July 2011 on the security and the protection of critical infrastructures, *B.S.* 15 July 2011.

Belgian Law of 25 April 2014, *B.S.* 7 May 2014.

Belgian Royal Decree of 2 December 2011 on critical infrastructures in the sector of air, *B.S.* 27 December 2011.

Belgian Royal Decree of 29 January 2014 on the security and protection of critical infrastructures in the sector of ports, *B.S.* 19 February 2014.

Belgian Royal Decree of 11 March 2013 on the security and protection of critical infrastructures in the sector of energy, *B.S.* 29 March 2013.

Belgian Law of 8 December 1992 on the protection of the private life of individuals in relation to the processing of personal data, *B.S.* 18 March 1993.

Belgian Law of 11 December 1998, *B.S.* 3 February 2011.

Belgian Law 26 February 2006, *B.S.* 26 June 2003.

Royal Decree of 13 February 2001, *B.S.* 13 March 2001.

Belgian Law 11 December 1998, *B.S.* 3 February 1999.

Belgian Law 30 July 2013 amending Articles 2, 126 and 145 of the Electronic Communications Act of 13 June 2005 and Article 90decies of the Code of Criminal Procedure, *B.S.* 23 August 2013.

Royal Decree 19 September 2013 on Article 126 of the Electronic Communications Act of 13 June 2005, *B.S.* 8 October 2013.

Case law

C-101/01 Linqvist case Judgment of the Court 6th November 2003

T-194/04 Bavarian Larger JUDGMENT OF THE COURT OF FIRST INSTANCE (Third Chamber) 8 November 2007

BGH, 28. 10. 2014, >> Az. VI ZR 135/13) see:juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=pm&Datum=2014&Sort=3&nr=69184&pos=0&anz=152

EU Court of Justice of 13 May 2014 (Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González

xxiv. United Kingdom

Durant v Financial Services Authority [2003] EWCA Civ 1746
Edem v. The Information Commissioner and The Financial Services Authority [2014] EWCA Civ 92

xxv. Ireland

EMI & Ors v Eircom Ltd [2010] IEHC 108.
Case C-70/10, Scarlet v Sabam, November 24, 2011
Schrems v Data Protection Commissioner (No. 2) [2014] IEHC 351

xxvi. Italy

Italian Supreme Court (no. 19365, 22/09/2011)

xxvii. France

Anthony G. / SCPP Cour d'appel de Paris, 13ème chambre, section B Arrêt du 27 avril 2007 http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=1954

Cour de cassation Chambre criminelle Arrêt du 13 janvier 2009: www.legalis.net/spip.php?page=breves-article&id_article=2563

Cour d'appel de Paris 12ème chambre, pôle 5 Arrêt du 1er février 2010: www.legalis.net/spip.php?page=breves-article&id_article=2852

Décision n° 2009-580 DC du 10 juin 2009: www.conseil-constitutionnel.fr/decision/2009/decisions-par-date/2009/2009-580-dc/decision-n-2009-580-dc-du-10-juin-2009.42666.html

Secondary Sources

xxviii. Opinions/Reports/Best Practice Documentation

Analysis and impact study on the implementation of Directive EC 95/46 in Member States, available at: http://ec.europa.eu/justice/policies/privacy/docs/lawreport/consultation/technical-annex_en.pdf

Article 29 Working Party, Opinion 4/2007 on the concept of personal data, adopted on 20 June, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf.

Article 29 Working Party, working document on data protection issues related to RFID technology, adopted on 19 January, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp105_en.pdf.

Article 29 Working Party Opinion 4/2007 on the concept of personal data Adopted on 20th June 01248/07/EN WP136

Article 29 Working Party 'Opinion 2/2010 on online behavioural advertising Adopted on 22 June 2010, 00909/10/EN WP 171

Article 29 Working Party, Working document, Privacy on the Internet - An integrated EU Approach to On-line Data Protection, adopted on 21 November 2000, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2000/wp37_en.pdf.

Article 29 Working Party, Opinion 1/2010 on the notion of controller and processor, adopted on 16 February 2010, available at https://www.cbpweb.nl/downloads_med/med20100219_C.03%20DC-DP_Opinion_ADOPTED.pdf.

Article 29 Working Party, Opinion 6/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, adopted on 9 April, available at http://www.cnpd.public.lu/fr/publications/groupe-art29/wp217_en.pdf.

Article 29 Working Party, Opinion 15/2011 on the definition of consent, adopted on 13 July 2011, available at http://ec.europa.eu/research/participants/data/ref/fp7/89736/article-29_en.pdf.

Article 29 Working Party, Opinion 3/2013 on purpose limitation, adopted on 2 April, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

Article 29 Working Party, Opinion 01/2012 on the data protection reform proposals, adopted on 23 March 2012

Article 29 Working Party, 'Opinion 1/2008 on data protection issues related to search engines' Adopted on 4 April 2008 00737/EN WP 148

Brussels, 28.8.2013 SWD(2013) 318 final COMMISSION STAFF WORKING DOCUMENT on a new approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures more secure Available at: ec.europa.eu/dgs/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure/docs/swd_2013_318_on_epcip_en.pdf

Booz and Company (Italia) S.r.l. 'Study: Stock-Taking of Existing Critical Infrastructure Protection Activities', Final Report JLS/2007/D1/037, 16/10/2009. pp. 428

Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, 2013, p3, http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security.

European Commission, Communication 245 on a Digital Agenda for Europe, 2010, http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52010DC0245

European Commission Communication 639-2010 from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Energy 2020 A strategy for competitive, sustainable and secure energy, http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52010DC0639

European Commission Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions A Digital Agenda for Europe, Brussels, 19.5.2010 COM(2010)245 eur-lex.europa.eu/legal-content/EN/TXT/PDF/?Uri=CELEX:52010DC0245&from=EN

ENISA, Threat Landscape Responding to the Evolving Threat Environment [Deliverable – 2012-09-28]

ENISA, Incentives and Barriers to Information Sharing in the Context of Information and Network Security.

Douwe Korff, 'EC Study on Implementation of Data Protection Directive: Comparative Summary of National Laws (Study Contract ETD/2001/B5-3001/A/49)

Douwe Korff, 'Comparative Study On Different Approaches To New Privacy Challenges, In Particular In The Light of TechnOlogical Developments Contract nr: JLS/2008/C4/011 – 30-CE-0219363/00-28 Country Studies: A.3 – France LRDP Kantor Ltd (Leader) In association with Centre for Public Reform (Final edit – May 2010)

Opinion of the Committee on Civil Liberties, Justice and Home Affairs of 22 March 2013 on Critical Infrastructures Protection. Achievements and next steps: towards global cyber - security (for the Committee on Industry, Research and Energy) Available at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A7-2012-0167+0+DOC+XML+V0//EN#top.

Feasibility Study for a European Cybercrime Centre, Rand Corporation, 2012, http://www.rand.org/content/dam/rand/pubs/technical_reports/2012/RAND_TR1218.pdf

Position Paper of the TNCEIP on EU Policy on Critical Energy Infrastructure Protection (November 2012) at:
ec.europa.eu/energy/infrastructure/doc/20121114_tnceip_eupolicy_position_paper.pdf

Premier Ministre, Secretariat General de la Defense et de la Securite Nationale, ‚Direction Protection et Sécurité de l'Etat: Instruction Generale Interministerielle Relative a la Securite des Activites d'importance vitale' N°6600/SGDSN/PSE/PSN du 7 Janvier 2014 N° Nor : PRMD1400503J

TENACE, *Protecting National Critical Infrastructures from Cyber Threats*, Center of Cyber Intelligence and Information Security - Università degli Studi di Roma 'La Sapienza', March 2014, available at *http://www.dis.uniroma1.it/~tenace/download/deliverable/Report_tenace.pdf*.

Safe Harbor Privacy Principles and annexed Frequently Asked Questions approved by European Commission with decision 2000/520/CE, 26 july 2000, available at http://eur-lex.europa.eu.

xxix. Books/Articles

Francis Aldhouse, 'Edem v. The Information Commissioner and The Financial Services Authority [2014] EWCA Civ 92', Computer Law & Security Review Volume 30, Issue 3, June 2014, pp. 321–323

Paddy Buckenham, Cybersecurity: European and domestic responses Briefing paper, The Institute of International and European Affairs, (April 2013).

BUTTARELLI, in *Concise. European IT Law*, BULLESBACH - GIJRATH - POULETT - PRINS (ed.), Second Edition, 2010, Kluwer Law International

Paul de Hert and Vagelis 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.*

Paul de Hert and Vagelis Papakonstantinou, The Polcie and Criminal Justice Data Protection Directive: Comment and Analysis, The IT Law Community, SCL Forum, http://www.vub.ac.be/LSTS/pub/Dehert/411.pdf

J. Dumortier, ICT-recht, Acco, Leuven, 2014, 272.

Myriam Dunn, 'Understanding Critical Information Infrastructures: An Elusive Quest' in Myriam Dunn and Victor Mauer (eds.) International CIIP Handbook 2006 Vol. II Analyzing Issues, Challenges, And Prospects (2006 Center for Security Studies) pp. 27-53.

Lilian Edwards, 'Privacy and Data Protection Online: The Laws Don't Work', in *Law and the Internet* Lilian Edwards and Charlotte Waelde (eds.), *3rd Ed.* (Hart Publishing 2009).

GIUSELLA FINOCCHIARO, *La memoria della rete e il diritto all'oblio*, *Rivista di diritto dell'informazione e dell'informatica*, 3, 2010 p. 391 and VIKTOR MAYER-SCHONBERGER, *Delete. The virtue of Forgetting in the Digital Age*, Princeton University Press, 2009.

G. Finocchiaro, *Anonymity and the Law in Italy*, in Aa.Vv., *Lessons from the Identity Trail*, Kerr - Steeves - Lucock (edit by), Oxford University Press, 2009, 523.

KOTSCHY, *Concise. European IT Law*, BULLESBACH - GIJRATH - POULETT - PRINS (edit by), Second Edition, 2010, Kluwer Law International, p. 55.

KUNER, *European Data Privacy Law and Online Business*, 2003, Oxford University Press, p. 52.

I. Lloyd, United Kingdom: International Encyclopaedia Of Laws: Cyber Law, (Ed.) Jos Dumortier (February 2004) Kluwer Law Series

S. Mascetti - A. Monreale - A. Ricci - A. Gerino, *Anonymity: a Comparison between the Legal and Computer Science Perspectives*, in Aa.Vv., *European Data Protection: Coming of Age*, Springer, 2013, 92.

Karen McCulagh, 'A study of data protection: harmonisation or confusion?' 21st BILETA Conference: Globalisation and Hormonisation in Technology Law April 2006, Malta available at: www.bileta.ac.uk/content/files/conference%20papers/2006/Data%20protection%20-%20harmonisation%20or%20confusion.pdf

Maeve McDonagh and Louise Crowley, Ireland: International Encyclopaedia Of Laws: Cyber Law, (Ed.) Jos Dumortier (February 2004) Kluwer Law Series

Andrew Murray, Information Technology Law: The law and Scoiety, (Oxford University Press, 2010) pp.479-483

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/

Christer Pursiainen (2009), The Challenges for European Critical Infrastructure Protection, Journal of European Integration, vol. 31:6, 721-739, November 2009.

J Scherer and C Heinickel, 'European Court of Justice Declares Data Retention Directive Invalid', Client alert April 2014 available at: www.bakermckenzie.com/files/Publication/fcf2ef80-c7f6-4361-a782-660857c40248/Presentation/PublicationAttachment/cac82cb1-74a4-4451-bef6-6829c1ecf1c5/ALGermanyPublicLawApril2014.pdf

AA.VV., *Concise. European IT Law*, BULLESBACH - GIJRATH - POULETT - PRINS (edit by), Second Edition, 2010, Kluwer Law International.

xxx. Websites

http://ec.europa.eu/energy/infrastructure/critical_en.htm

http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

http://europa.eu/rapid/press-release_IP-12-1389_en.htm

http://www.cpni.gov.uk/advice/cyber/Good-practice-catalogue/

http://ico.org.uk/for_organisations/data_protection/the_guide/~/media/documents/library/Data_Protection/Detailed_specialist_guides/PERSONAL_DATA_FLOWCHART_V1_WITH_PREFACE001.ashx

http://ico.org.uk/for_organisations/data_protection/the_guide/~/media/documents/library/Data

_Protection/Detailed_specialist_guides/determining_what_is_personal_data_quick_reference_guide.ashx

http://ico.org.uk/~/media/documents/library/Data_Protection/Detailed_specialist_guides/PERSONAL_DATA_FLOWCHART_V1_WITH_PREFACE001.ashx

http://www.allenovery.com/publications/en-gb/Pages/Court-of-Appeal-endorses-Information-Commissioner-Office-Guidance-on-meaning-of-personal-data.aspx

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60970/dataprotection.pdf

http://www.cpni.gov.uk/advice/cyber/Good-practice-catalogue/

http://ico.org.uk/~/media/documents/library/data_protection/practical_application/breach_reporting.pdf

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60970/dataprotection.pdf

http://ico.org.uk/for_organisations/data_protection/topic_guides/~/media/documents/library/Data_Protection/Detailed_specialist_guides/data_sharing_code_of_practice.ashx

http://ico.org.uk/for_organisations/data_protection/topic_guides/~/media/documents/library/Data_Protection/Detailed_specialist_guides/data_sharing_code_of_practice.ashx

http://www.parliament.uk/business/publications/business-papers/commons/deposited-papers/?fd=2014-07-09&td=2014-07-31&search_term=Home+Office#toggle-1053

http://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-strategic-framework-for-cyberspace-security.pdf

http://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-cyber-security-plan.pdf

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf

http://www.garanteprivacy.it

http://www.emergencyplanning.ie/media/docs/A%20National%20Risk%20Assessment%20for%20Ireland%20Published.pdf

http://www.emergencyplanning.ie/media/docs/Guidelines%20for%20Coordinating%20a%20national%20level%20emergency%20crisis%20response%20Version%202%202013%2003.15.pdf

http://www.emergencyplanning.ie/media/docs/A%20National%20Risk%20Assessment%20for%20Ireland%20Published.pdf

www.emergencyplanning.ie

http://www.emergencyplanning.ie/media/docs/A%20National%20Risk%20Assessment%20for%20Ireland%20Published.pdf

http://www.dcenr.gov.ie/Corporate+Units/Minister/Ministers+Brief/Communications.htm

http://www.dataprotection.ie/viewdoc.asp?DocID=1091

http://www.dataprotection.ie/docs/Data_Security_Breach_Code_of_Practice/1082.htm

http://www.justice.ie/en/JELR/Pages/Ahern%20Publishes%20Data%20Review%20Report

https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/dbn

http://www.arthurcox.com/publications/data-retention-directive-declared-invalid-eu-court-justice/

http://www.cnil.fr/documentation/questionsreponses/?faq%5buid%5d=48

http://crisiscentrum.be/nl/inhoud/kritieke-infrastructuur-0.

https://www.cert.be/nl/wie-zijn-we.

http://www.belnet.be/nl.

http://www.fedict.belgium.be/nl/

http://www.cert.ssi.gouv.fr/cert-fr/certfr.html

http://www.timelex.eu/frontend/files/userfiles/files/publications/2011/IP_addresses_report_-_Final.pdf