



## D7.7

### Information sharing policies in disaster situations Version 2

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

<b>Deliverable type:</b>	Report
<b>Deliverable reference number:</b>	SEC-607577 / D7.7/ 1.0
<b>Work package contributing to the deliverable:</b>	WP7
<b>Due date:</b>	MAY 2017 – M36
<b>Actual submission date:</b>	31 <sup>st</sup> May, 2017

<b>Responsible organisation:</b>	KUL
<b>Editor:</b>	Jessica Schroers
<b>Dissemination level:</b>	PU
<b>Revision:</b>	1.0

<b>Security    Sensitivity    Committee</b>	22 <sup>nd</sup> May, 2017
<b>Review performed on:</b>	
<b>Comments:</b>	N/A

<b>Abstract:</b>	This deliverable focuses on the legal framework related to the sharing of data for network and information security of Critical Infrastructure. It updates and extends the information provided in D7.3.
<b>Keywords:</b>	Information sharing, Disaster management, Critical Infrastructure Protection, Security.



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

**Editor**

Jessica Schroers (KUL)

**Contributors** (ordered according to beneficiary numbers)

Alessandra Spangaro, Giusella Finocchiato (UNIBO)

Erik Zouave, Plixavra Vogiatzoglou, Eline Dekyvere, Giancarlo Frosio, Damian Clifford (KUL)

## Executive Summary

Information sharing in disaster situations is potentially crucial for relief and the prevention of further damage. ECOSSIAN aims to develop prevention and detection tools that facilitate preventive functions like threat monitoring, early indicator and real threat detection, alerting, support of threat mitigation and disaster management in a privacy compliant manner. In order to adequately comprehend the legal implications of sharing information regarding the ECOSSIAN solution one must have a detailed understanding of information sharing in the broader context of disaster management. The purpose of this deliverable is to provide an update of the first version, outlining the requirements and policies associated with information sharing in the context of ECOSSIAN. This deliverable updates D7.3 “Information sharing policies in disaster situations – Version 1”, considering the important legislative changes during the last year, and includes more information regarding information sharing with law enforcement, notification obligations, classification as well as a specific deep analysis of Italian national legislation based upon the findings of D7.3.

# Contents

<b>Chapter 1</b>	<b>Introduction .....</b>	<b>1</b>
<b>Chapter 2</b>	<b>Critical Infrastructure and essential services .....</b>	<b>2</b>
2.1	Council Directive 2008/114/EC .....	2
2.2	The NIS Directive .....	3
<b>Chapter 3</b>	<b>Information sharing .....</b>	<b>6</b>
3.1	Access obligations of public authorities .....	6
3.2	Information sharing with Law Enforcement Authorities .....	7
3.3	Implementing Information Sharing .....	8
3.4	Information Sharing on Incidents .....	10
3.5	Information Sharing on Cybercrime .....	11
3.5.1	Competence in Criminal and Judicial Cooperation .....	12
3.5.2	Bodies with Law Enforcement Competence .....	12
3.5.2.1	<i>Spontaneous Information Sharing</i> .....	12
3.5.2.2	<i>Requests for Assistance</i> .....	13
3.5.2.3	<i>Harmonization of Evidentiary Sources</i> .....	13
3.5.2.4	<i>Procedure for Requests &amp; Sharing</i> .....	14
3.5.3	Bodies without Law Enforcement Competence .....	16
3.5.3.1	<i>Guidance for Bodies without Law Enforcement Competence</i> .....	17
3.6	Data Protection in Criminal & Judicial Cooperation .....	17
3.6.1	Automated Processing of Personal Data .....	19
3.6.1.1	<i>Definitions: Personal Data &amp; Automatic Processing</i> .....	19
3.6.1.2	<i>Obligations for Controllers</i> .....	19
3.6.1.3	<i>Automated Processing of Personal Data in the Police Sector</i> .....	20
3.6.1.3.1	Definitions: Personal Data & Data Processing .....	21
3.6.1.3.2	Recommendations for Police Authorities .....	21
3.6.1.3.3	Recommendations for Responsible Bodies .....	22
3.6.2	Data Protection & Mutual Assistance on Cybercrime .....	22
3.6.3	The Police & Criminal Authorities Directive .....	23
3.6.3.1	<i>Definitions: Personal Data &amp; Data Processing</i> .....	24
3.6.3.2	<i>Application to Controllers</i> .....	25
3.6.3.2.1	Appropriate Technical & Organizational Measures .....	26
3.6.3.2.2	Logging & Recording .....	27
3.6.3.3	<i>Application to Processors</i> .....	27
3.6.3.3.1	Lawfulness & Processing Under Contract .....	28
3.6.3.3.2	Record Keeping .....	29
3.6.3.4	<i>General Principles of Data Protection</i> .....	29
3.6.3.5	<i>Rights of the Data Subject</i> .....	31

3.6.4	The Right to Privacy in Information Sharing .....	34
3.6.4.1	<i>Interferences with Privacy</i> .....	34
3.6.4.2	<i>Interferences for Detecting &amp; Preventing Crime</i> .....	35
3.6.4.3	<i>Safeguards in Access to Data for Crime Detection &amp; Prevention</i> .....	35
3.6.4.4	<i>Effective Guarantees against Abuse</i> .....	36
3.6.4.5	<i>Scope of Interference</i> .....	37
3.7	ICT specific legal frameworks .....	38
3.7.1	Breach notification obligations.....	38
<b>Chapter 4</b>	<b>Legal barriers to information sharing .....</b>	<b>49</b>
4.1	Data protection requirements.....	49
4.2	Requirements in intellectual property and unfair competition law .....	54
4.2.1	Copyright and Database Right .....	56
4.2.1.1	<i>Ordinary and Database Copyright</i> .....	57
4.2.1.2	<i>Database Sui Generis Right</i> .....	58
4.2.1.3	<i>Exceptions</i> .....	59
4.2.2	Unfair Competition and Trade Secrets .....	61
<b>Chapter 5</b>	<b>Classification and confidentiality obligations .....</b>	<b>63</b>
5.1	EU classification rules/strategy .....	63
5.1.1	National classification rules .....	66
5.1.2	Technical and organizational requirements as a hurdle.....	67
5.1.3	ECOSSIAN .....	67
<b>Chapter 6</b>	<b>Italian Analysis .....</b>	<b>69</b>
6.1	Introduction to the Italian legal framework .....	69
6.2	Disaster Management.....	69
6.2.1	Critical Infrastructure Framework .....	69
6.2.1.1	<i>ITALY</i> .....	71
6.2.1.2	<i>MILESTONES in ITALY</i> .....	75
6.2.2	Italian CI Information Sharing Platforms .....	82
6.2.3	Italian Civil Protection.....	83
6.2.4	Public-Private Partnerships (PPP).....	85
6.2.5	Disaster Management and Italian CIP Mechanisms .....	87
6.3	Legal Framework for Information Sharing .....	88
6.3.1	Criminal law - Implications for data sharing in disaster situations .....	88
6.3.2	ICT Specific Legal Frameworks.....	88
6.4	Legal Barriers to Information Sharing .....	90
6.4.1	Data Protection Requirements .....	90
6.4.2	Requirements in Intellectual Property Law .....	90

6.4.3 Confidentiality obligations .....	92
6.5 Impact on ECOSSIAN.....	93
6.5.1 About the Italian Demo.....	93
<b>Chapter 7 Impact on ECOSSIAN/Evaluation .....</b>	<b>95</b>
<b>Chapter 8 Guidelines.....</b>	<b>98</b>
8.1 Human operator guidelines .....	99
<b>Chapter 9 Conclusion.....</b>	<b>100</b>
<b>Chapter 10 List of Abbreviations .....</b>	<b>101</b>
<b>Chapter 11 Bibliography.....</b>	<b>103</b>
11.1 Primary sources .....	103
11.1.1 Legislation.....	103
11.1.2 Case law .....	105
11.2 Secondary Sources .....	106
11.3 Other .....	109

## List of Figures

Figure 1: Directive 2008/114/EC and some of its specific applications .....	70
Figure 2: Public actors of the emergency system before DPCM 17 <sup>th</sup> February 2017 .....	81
Figure 3: Public actors of the emergency system after DPCM 17 <sup>th</sup> February 2017 .....	82

## List of Tables

Table 1: CI protection and the disaster management framework .....	5
Table 2: Criminal law - Implications for data sharing in disaster situations.....	38
Table 3: EU notification legislation.....	42
Table 4: National notification obligations .....	47
Table 5: ICT specific frameworks requirements .....	48
Table 6: Intellectual Property .....	57
Table 7: Requirements in IP .....	62
Table 8: Confidentiality obligations .....	68
Table 9: Comparison Directive 2008/114/EC with Legislative Decree April 11th, 2001 No. 61 .....	74
Table 10: Overview Italian IP legislation .....	92
Table 11: Limitation of IP rights in Italian legislation .....	92
Table 12: Applied Requirements Table I.....	96
Table 13: Applied Requirements Table II.....	97
Table 14: Guidelines .....	98

## Chapter 1 Introduction

Information sharing in disaster situations is potentially crucial for relief and the prevention of further damage. ECOSSIAN aims to develop prevention and detection tools that facilitate preventive functions like threat monitoring, early indicator and real threat detection, alerting, support of threat mitigation and disaster management in a privacy compliant manner. In order to adequately comprehend the legal implications of sharing information regarding the ECOSSIAN solution one must have a detailed understanding of information sharing. The first deliverable focused on disaster situations, however, as the ECOSSIAN system aims for information sharing also outside of disaster situations for improved network and information security of Critical Infrastructures, this update has a slightly broader scope and includes for example also information sharing with law enforcement. This deliverable should be distinguished from D7.6 “Legal evaluation of the ECOSSIAN system and recommendations”, which assesses the compliance of the developed ECOSSIAN system with the requirements provided in D7.2 “Legal requirements”. D7.7 also assesses the requirements specified in D7.3 “Information sharing policies in disaster situations – Version 1”, however, as they mostly relate to the actual organisational implementation, most of them cannot be assessed from a technical point of view and therefore recommendations are provided.

The analysis will be divided as follows: Chapter 2 will first examine the current legislative framework in the context of Critical Infrastructures, including the Council Directive 2008/114 and the new NIS Directive (‘Critical infrastructure and essential services’). Chapter 3 will focus on the legal framework for information sharing (‘Information sharing’), including a section on information sharing with law enforcement. Chapter 4 will assess the barriers to information sharing (‘Legal barriers to information sharing’). An additional Chapter 5, focusing on classification of information (‘Classification and confidentiality obligations’) and Chapter 6, providing an complete analysis from a national point of view (‘Italian analysis’) have been added to the scope of the previous deliverable. The analysis provided in the previous Chapters will then be applied in Chapter 7 to the context of ECOSSIAN (‘Impact on ECOSSIAN’). The application to ECOSSIAN will maintain these distinctions as they highlight the policy basis for action, the legislation requiring information sharing and finally the legal frameworks imposing restrictions on any such sharing. Chapter 8 will provide guidance on the implementation of the identified requirements and finally Chapter 9 will conclude the analysis.



## Chapter 2 Critical Infrastructure and essential services

### 2.1 Council Directive 2008/114/EC

Council Directive 2008/114/EC<sup>1</sup> 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.<sup>2</sup> Each Member State (MS) of the EU has the responsibility for the identification of their Critical Infrastructures. However, 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 (ECI). 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.*

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 (MSs) include definition of Critical Infrastructure based on defence strategies, national emergency management and long term national traditions. Following identification each MS is required to inform the other MSs ‘which may be significantly affected by a potential ECI about its identity and the reasons for designating it as a potential ECI.’ and subsequently engage in bilateral or multilateral negotiations (where appropriate) with the other potentially affected MS(s). 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.

---

<sup>1</sup> Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection [2008] OJ L345/75.

<sup>2</sup> See Annex 1 of the Directive

In the review<sup>3</sup> for a new European Programme for Critical Infrastructure Protection (EPCIP), the Commission finds that less than 20 European Critical Infrastructures have been designated and consequently very few new Operator Security Plans have been produced and some Critical Infrastructures such as main energy transmission networks are not included.<sup>4</sup> Some disadvantages of the Directive are that not a real European forum for cooperation has been created and that the sector focused approach does not align with the reality where criticalities are not necessarily confined to sectoral boundaries.<sup>5</sup> They conclude that “Operators of Critical Infrastructures including those operating in the energy and transport sector, would, moreover, fall under the risk management and incident reporting requirements of the proposed Directive on network and information security”.<sup>6</sup>

Accordingly, we will now turn our attention to the new NIS Directive.

## 2.2 The NIS Directive

The Directive ‘concerning measures for a high common level of security of network and information systems across the Union’<sup>7</sup> (previously referred as network information security Directive and therefore shortened NIS Directive) was adopted and entered into force in 2016. The new NIS Directive aims at EU wide improvement of cybersecurity, with a focus on essential services and specific digital services. As a directive Member States will have 21 months (until 9.5.2018) to transpose the Directive into their national legislative framework. The NIS Directive aims to achieve a high common level of security of network and information systems within the European and in order to achieve this specifies certain obligations for Member States. Member States must adopt a national strategy on the security of network and information systems, designate one or more national competent authorities, CSIRTs and a national single point of contact.

Furthermore, they must identify operators of essential services in their territory.

### Operators of essential services:

‘Operators of essential services’ are public or private entities in the sectors energy, transport, banking, financial market infrastructure, health sector, drinking water supply and distribution and digital infrastructure which fulfil three criteria:

- 1) they provide a service that is essential for the maintenance of critical societal and/or economic activities,

---

<sup>3</sup> Commission Staff Working Document on a new approach to the European Programme for Critical Infrastructure Protection - Making European Critical Infrastructures more secure, Brussels, 28.8.2013, SWD(2013) 318 final.

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

<sup>5</sup> Commission Staff Working Document on a new approach to the European Programme for Critical Infrastructure Protection - Making European Critical Infrastructures more secure, Brussels, 28.8.2013, SWD(2013) 318 final, p.4.

<sup>6</sup> Commission Staff Working Document on a new approach to the European Programme for Critical Infrastructure Protection - Making European Critical Infrastructures more secure, Brussels, 28.8.2013, SWD(2013) 318 final, p.5.

<sup>7</sup> Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016.

- 2) the provision of their services depends on network and information systems, and
- 3) an incident would have a significant disruptive effect on the provision of that service.

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

#### Information sharing:

The NIS Directive also includes some approaches to increase and improve information sharing. The Cooperation Group and the CSIRTs network are two groups established by the NIS Directive, which should increase exchange of information. The Cooperation Group is composed of representatives of the Member States, the Commission and ENISA and has a more strategic role, focusing on exchanging information regarding best practice e.g. on the exchange of information related to incident notification. On the other hand, the CSIRT network consists of representatives of the Member States' CSIRTs and CSIRT-EU. The aim of the network is to exchange information on CSIRTs' services, operations and cooperation capabilities, exchange and discuss non-commercially sensitive information (at the request of a representative of a CSIRT), exchange and make available on a voluntary basis non-confidential information concerning individual incidents. As becomes visible from the restrictions the sharing is purely voluntary and it is provided that Member State's CSIRTs may refuse to contribute to discussions if there is a risk of prejudice to the investigation of an incident, and the sharing only involves non-confidential information and non-commercially sensitive information.

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

Further information the NIS Directive in consideration of different specific contexts can be found in the next chapters: Information sharing with Law enforcement in Chapter 3 section 3.2, notification obligations in section 3.7.1 and confidentiality obligations in Chapter 5.

D7.3 specified three requirements for Critical Infrastructure protection:

Req. number	Description	Importance* (M/O)	Relevant for Level			Comment
			O-SOC	N-SOC	E-SOC	
GReq. 1.1	The ECOSSIAN solution must be able to be integrated with the already existing Operator Security Plan.	M	X	X	X	Article 5 and Annex II Critical Infrastructure Protection Directive
GReq. 1.2	National implementations of Directive 2008/114/EC must be consulted as they may (for example France) have	M	X	X	X	

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

\*M – mandatory; O – optional

\*\* Work Packages where this requirement should be implemented

Table 1: CI protection and the disaster management framework

From the above analysis, it becomes clear that on an European level there are not many Operator Security Plans required, however, on a national level Member States might require their national Critical Infrastructure operators to implement comparable plans. As the ECOSSIAN solution is technological flexible and can be integrated in different ways, it should be possible to include it in different Critical Infrastructures and align it with existing Operator Security Plans. In the analysis no specific technical restrictions have been identified, however, with the currently ongoing legislative changes including the national implementation of the NIS Directive, the above requirements will stay applicable for a potential implementation of an ECOSSIAN system from an organisational point of view and will require further discussion and analysis.

## Chapter 3 Information sharing

### 3.1 Access obligations of public authorities

D7.3 showed that the Member States interpretations and implementations regarding the public sector bodies' rights and obligations in relation to making "public information" available upon request (but also encouraging proactive release) to the general public vary significantly. This is an issue which remains in the sole competence of the Member States thus facilitating clear disparities.<sup>8</sup>

Accordingly, in general access to public sector information is dictated by national law with no precise framework at an EU level. As noted in D7.3, there are two exceptions in relation to environmental and spatial data, which are however of limited relevance for ECOSSIAN.

Regarding Public Sector Information (PSI) re-use, D7.3 gave an overview on the PSI Directive (Directive 2003/98/EC)<sup>9</sup> and Directive 2013/37/EU (Member States are required to implement the changes by the 18th of July 2015). Considered as especially relevant were the interaction between intellectual property rights and the PSI framework and that the re-use of PSI cannot breach the data protection legislation. Theoretically, when e.g. the N-SOC or E-SOC are public sector bodies, the PSI Directive could provide a common framework for the rights of re-use.<sup>10</sup> However, in the current context of information sharing in disaster situations the information needed to be shared and re-used would often be security sensitive and will therefore be unlikely to be made available for re-use. Therefore the impact of this legislation will most likely be limited.

This does however not withhold that information access legislation might provide a "psychological barrier" to information sharing for CI providers, as has been found in the Netherlands where members of the National Detection Network were reluctant to share information with a governmental body for the fear of the Dutch Freedom of Information legislation (Wet openbaarheid bestuur). In the Netherlands this issue was solved by classifying the information at a confidentiality level where the legislation does not apply.<sup>11</sup> Therefore, considering the different organisational forms the different SOC's might take, it can be useful to ensure that information shared within the ECOSSIAN can indeed not be accessed under EU or national access legislation, in order to increase trust in information sharing.

---

<sup>8</sup> For more see: <http://journalism.cmpf.eui.eu/maps/freedom-of-information/>

<sup>9</sup> Directive 2003/98 of November 17, 2003 on the re-use of public sector information [2003] OJ L345/90.

<sup>10</sup> ENISA, 'A flair for information sharing- encouraging information exchange between CERTs' (2011) accessed on 01/03/2015 at: <http://www.enisa.europa.eu/activities/cert/support/fight-against-cybercrime/legal-information-sharing>

<sup>11</sup> see Ch. 5 forthcoming book Florian Skopic et al., "Collaborative Cyber Threat Intelligence – Creating, Sharing and Processing Security-relevant Information on National Level".

### 3.2 Information sharing with Law Enforcement Authorities

As noted in previous deliverables,<sup>12</sup> the European Union has authored a range of initiatives with the aim of encouraging collaboration and information sharing in the areas of network and information security (NIS), Critical Infrastructures and the detection and prevention of cybercrime. Three European policy statements have similarly been predominant in the question of cooperation between CERTs and law enforcement agencies (LEAs); the 2009 Digital Agenda for Europe,<sup>13</sup> the 2009 Communication on Critical Information Infrastructure Protection (CIIP),<sup>14</sup> and the 2011 CIIP Progress Report.<sup>15</sup>

In essence, these initiatives sought to build trust and security, as well as ensure the prevention, preparedness and resilience of Critical Infrastructure by promoting voluntary public-private cooperation at regional and domestic levels. Notably, within the context of the Digital Agenda, the Commission adopted a Proposal for a Directive on attacks against information systems, now Directive 2013/40/EU, that harmonizes the criminal law of Member States concomitant to the Convention on Cybercrime. Cybercrime instruments also couched LEA information sharing within the existing traditions of mutual legal assistance between states, harmonizing domestic criminal procedural law on access to intangible sources of evidence. Moreover, the CIIP also engendered specialized communications on European cooperation in criminal and judicial matters, particularly Communication on Critical Information Infrastructure Protection - "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience".<sup>16</sup>

European law and policy relevant to information sharing correspondingly followed two parallel, but separate, legal bases; ensuring freedom, security and justice (Title V TFEU) on the one hand and in view of achieving the operation of the Common Market (Article 308 TEU) on the other. Moreover, the European Parliament recently adopted Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (the NIS Directive) information sharing protocols were adopted as a matter of approximation of laws concerning health, safety, environmental protection and consumer protection (Article 114 TFEU). The NIS Directive is the first legislation to formalize information sharing structures and procedures between operators of essential services and information service providers, national competent authorities and

<sup>12</sup> D7.3 Information sharing policies in disaster situations;

<sup>13</sup> 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 (COM(2010) 245 final/2)

<sup>14</sup> COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS: on Critical Information Infrastructure Protection - "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" (COM(2009) 149 final)

<sup>15</sup> COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS: on Critical Information Infrastructure Protection - 'Achievements and next steps: towards global cyber-security' (COM(2011) 163 final)

<sup>16</sup> COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS: on Critical Information Infrastructure Protection - "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" (COM(2009) 149 final)



regional entities within the European NIS community. Moreover, the Directive also exhorts cooperation between NIS and LEA communities through criteria and procedures adopted in national law and with respect for existing channels of exchange. It is important to note that the obligations to share information on criminalized incidents will not emerge in a legal vacuum. Highly formalized procedures and channels for information sharing exist which regulate law enforcement access to cybercrime evidence.

The purpose of this section is to examine the substantive and procedural frameworks applicable to information sharing on criminal and judicial matters under these legal bases. Information sharing is studied broadly in this section and encompasses situations where bodies with or without law enforcement competence can voluntarily share information on incidents with other bodies that have law enforcement competence or can be lawfully compelled to do so. It will clarify:

- The legal bases for information sharing with and among LEAs on matters of cybercrime and the competences associated with those instruments,
- The voluntary and mandatory procedures for information sharing set out in regional arrangements, and
- The mandatory procedures for information sharing that regional instruments impose and seek to harmonize in domestic laws.

### 3.3 Implementing Information Sharing

The Digital Agenda, the CIIP Communication as well as analogous Directives, regulations, Communications and Recommendations in the field of cyber security and cybercrime attest to the political and legislative interest in ensuring effective information sharing on cyber incidents. The NIS Directive formalizes collaboration between operators and national authorities regionally. National LEAs and dedicated regional platforms Europol and the European Cybercrime Centre (EC3) have, through various regional instruments, received mandates and structures to collaborate on cross-border cybercrime. However the level of regional formalization remains much lower for the exchange between NIS and LEA communities, legally and structurally.<sup>17</sup> In the absence of a dedicated regional regulatory framework to these exchanges, a range of practical considerations have typically impacted the extent to which incident and threat intelligence is communicated to law enforcement.

There are circumstances where voluntary and spontaneous information sharing may be preferable to waiting for an authority to compel disclosure. Some incidents are systemic and have implications beyond the immediate impact to first responders, necessitating concerted efforts between law enforcement and operators. ENISA further observes that the successful investigation and prevention of pervasive cybercrime would sometimes require private CERTs not to be the first and sole responders to an incident:

*A concern has been noted that solo-actions from the private sector (including private CERTs, security companies etc.) without the backing of law enforcement may be*

---

<sup>17</sup> See ENISA (2011) A flair for sharing – encouraging information exchange between CERTs: A study into the legal and regulatory aspects of information sharing and cross-border collaboration of national/governmental CERTs in Europe (Initial Edition 1.0 November 2011); ENISA (2013) The Directive on attacks against information systems: A Good Practice Collection for CERTs on the Directive on attacks against information systems (ENISA P/28/12/TCD, Version: 1.5, 24 October, 2013); ENISA (2015) Information sharing and common taxonomies between CSIRTs and Law Enforcement (Final Version 1.0, PUBLIC DECEMBER 2015); ENISA 2015 Electronic evidence - a basic guide for First Responders Good practice material for CERT first responders

*effective in shutting down isolated incidents, but ultimately leave criminals unharmed and free to resume their activities. Such actions can furthermore harm ongoing investigations, as crucial data might be destroyed or corrupted, making it unusable as evidence in potential criminal proceedings.*<sup>18</sup>

Conversely, there are also reasons why operators and private CERTs may choose not to share information with LEAs without a judicial warrant. Whereas criminal and judicial information sharing originates from a tradition of formalized and regulated relationships between public agencies, information sharing on cyber threats in NIS and CERT communities is typically informal.<sup>19</sup> Operators and businesses may face the risk of reputational loss, which affects their competitive position on the market, if the impact of incidents are disclosed.<sup>20</sup> Additionally, stakeholders may consider legal involvement an obstacle to effective informal channels, and may have a preference for partnerships based on trust rather than legal obligation.<sup>21</sup> ENISA has found that legal uncertainty bars collaboration,<sup>22</sup> especially in cross-border scenarios as there is generally more awareness of domestic laws.<sup>23</sup> As also explained in D7.3, legal concerns are also prevalent with respects to the data protection obligations on operators, in particular when threat intelligence encompasses personal data such as IP-addresses and personal data.<sup>24</sup> In some cases, information collected and shared between CERTs may be subject to contractual obligations of secrecy, further complicating and discouraging disclosure to third parties.<sup>25</sup> The same legal concerns may be reflected among LEAs that are concerned with the court-proofness of data,

<sup>18</sup> ENISA (2013) The Directive on attacks against information systems: A Good Practice Collection for CERTs on the Directive on attacks against information systems (ENISA P/28/12/TCD, Version: 1.5, 24 October, 2013) 23

<sup>19</sup> ENISA (2011) A flair for sharing – encouraging information exchange between CERTs: A study into the legal and regulatory aspects of information sharing and cross-border collaboration of national/governmental CERTs in Europe (Initial Edition 1.0 November 2011) 6

ENISA (2012) Give and Take: Good Practice Guide for Addressing Network and Information Security - Aspects of Cybercrime Legal, Regulatory and Operational Factors Affecting CERT Co-operation with Other Stakeholders. 34

<sup>20</sup> KPMG and CYBERSTREETWISE. (2015). *SMALL BUSINESS REPUTATION & THE CYBER RISK*. Available: <https://home.kpmg.com/content/dam/kpmg/pdf/2016/02/small-business-reputation-new.pdf>. Last accessed 04/05/2017.

<sup>21</sup> ENISA (2011) A flair for sharing – encouraging information exchange between CERTs: A study into the legal and regulatory aspects of information sharing and cross-border collaboration of national/governmental CERTs in Europe (Initial Edition 1.0 November 2011) 9; ENISA (2012) Give and Take: Good Practice Guide for Addressing Network and Information Security - Aspects of Cybercrime Legal, Regulatory and Operational Factors Affecting CERT Co-operation with Other Stakeholders. 61

<sup>22</sup> ENISA (2013) The Directive on attacks against information systems: A Good Practice Collection for CERTs on the Directive on attacks against information systems (ENISA P/28/12/TCD, Version: 1.5, 24 October, 2013) 16

<sup>23</sup> ENISA (2012) Give and Take: Good Practice Guide for Addressing Network and Information Security - Aspects of Cybercrime Legal, Regulatory and Operational Factors Affecting CERT Co-operation with Other Stakeholders. 9

<sup>24</sup> ENISA (2012) Give and Take: Good Practice Guide for Addressing Network and Information Security - Aspects of Cybercrime Legal, Regulatory and Operational Factors Affecting CERT Co-operation with Other Stakeholders. 46

<sup>25</sup> ENISA (2012) Give and Take: Good Practice Guide for Addressing Network and Information Security - Aspects of Cybercrime Legal, Regulatory and Operational Factors Affecting CERT Co-operation with Other Stakeholders. 47



e.g. circumstances of data collection, integrity and authenticity of data, as well as data protection concerns.<sup>26</sup> CERTs have a natural onus to respond and keep systems running whereas criminal investigations inherently seek to freeze the crime scene and keep it in tact. Finally in states that have a very recent track record of criminalizing certain cybercrime, or where Police investigations of cybercrime are considered ineffective, private entities may be less prone to involve law enforcement unless they must.<sup>27</sup>

### 3.4 Information Sharing on Incidents

In an age of ubiquitous information and communication technologies, connected Critical Infrastructures, and pervasive cyber threats the European Union has imputed broader forms of cooperation to prevent on cybercrime. This has had the lateral effect of gradually crystallizing possibilities for operators of essential services, network operators and service providers to share information with law enforcement on matters relating to cybercrime, notably through the 2013 Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace and the NIS Directive.

The EU Cybersecurity Strategy set out the strategic priorities for Members States, including making recommendations for national level strategic initiatives.<sup>28</sup> The strategy encouraged collaborations between national authorities both with Network and Information Security (NIS) law enforcement, and defense with the private sector.<sup>29</sup> The Community further encouraged comparable collaboration between the European Union Agency for Network and Information Security (ENISA), the European Cybercrime Centre (EC3) within Europol, and the European Defence Agency (EDA), specifically in risk and trend analysis, best practice assessments and training. Moreover, the Strategy was drafted with the expectation that the NIS Directive (a proposal at that time), “would establish a cooperation framework via a network of national NIS competent authorities and address information sharing between NIS and law enforcement authorities”.<sup>30</sup>

In reality however, the NIS Directive has not made information sharing between NIS and LEA communities mandatory between the NIS and LEA communities. The Directive establishes two types of information sharing procedures on the basis of competence. Article 8 of the Directive requires the Member States to designate a national competent authority, or multiple authorities, and a single point of contact. Article 14 subsequently requires operators to notify the competent authority, or the CSIRT, of incidents having *significant impact on the continuity*

<sup>26</sup> ENISA (2012) Give and Take: Good Practice Guide for Addressing Network and Information Security - Aspects of Cybercrime Legal, Regulatory and Operational Factors Affecting CERT Co-operation with Other Stakeholders. 46

<sup>27</sup> Riksrivisionen (2015) It-relaterad brottslighet – polis och åklagare kan bli effektivare (RiR 2015:21); COUNCIL RECOMMENDATION of 25 June 2001 on contact points maintaining a 24-hour service for combating high-tech crime (2001/C 187/02), para 3

<sup>28</sup> JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (JOIN(2013) 1 final)

<sup>29</sup> JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (JOIN(2013) 1 final) Section 3.1

<sup>30</sup> JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (JOIN(2013) 1 final) 18

of services. The significance is determined through a) the users affected, b) the duration, and the c) geographical spread of the incident.<sup>31</sup> This obligation has not resulted in a mandatory information sharing arrangement between operators and LEAs. As such there are no new binding obligations for O-SOCs to report cybercrime as a result of the Directive. However, the NIS Directive changed the previously voluntary reporting norm in the regional regulation of CERT and LEA collaboration with respect to competent national authorities. NIS Directive Competent authorities shall share information from incident notifications with LEAs “when appropriate” and with discretion under national law, as clarified by Article 8(6). In view of this it must be understood that incidents reaching the *significant impact* threshold are likely to be criminalized by Directive 2013/40 on attacks against information systems. Notably, Article 9 to Directive 2013/40 imposes higher penalties on illegal system interference and illegal data interference where a significant number of information systems have been affected, cause serious damage, or are directed against Critical Infrastructure. The NIS Directive further urges competent authorities and LEAs of Member States should, when appropriate, coordinate the prevention, investigation and prosecution of cybercrime with the European Cybercrime Centre (EC3) and ENISA. ECOSSIAN is resultantly impacted by the NIS directive several ways. Firstly, O-SOCs have mandatory incident notification commitments to competent authorities which could be N-SOC level entities. Secondly, these requirements may affect or override concerns about secrecy, trust, and reputation in the information sharing landscape as O-SOCs must expect that anything shared can be passed on to other authorities. Thirdly, N-SOCs will be subject to binding domestic obligations, if they are not already, to share information indicating criminal activity with LEAs. Whereas O-SOC to N-SOC sharing is foreseeably regulated by the significance threshold in the NIS Directive, N-SOC to LEA sharing will be dependent on more complex criminal and procedural law. It is therefore important to stay seized of how the EU Member states will implement article 8(6) in national law or determine that existing channels of information sharing will be adapted to account for such reporting.

### 3.5 Information Sharing on Cybercrime

Title V of the Treaty on the Functions of the European Union (TFEU), i.e. ensuring freedom, security and justice, encompasses the approximation laws and the coordination and cooperation between police and judicial authorities in Member States. The focus of these initiatives are on crimes of a cross-border dimension and a special need to combat them on a common basis (Article 83 TFEU), such as cybercrime.<sup>32</sup> This concern about the transnationality of cybercrime is reflected and EU instruments harmonize domestic criminal law in the area of cybercrime, notably *Directive 2013/40/EU on attacks against information systems*, and the *Cybersecurity Strategy of the European Union* and the older Council of Europe (CoE) precedent *the Convention on Cybercrime* (a.k.a. Budapest Convention). These instruments place cybercrime within an established tradition of mutual assistance and cross-border cooperation in criminal and judicial procedures. For these purposes, Title V legal frameworks and CoE instruments relevant to the coordination and cooperation between police and judicial authorities in Member States encompass:

- The 1959 European Convention on Mutual Assistance in Criminal Matters (and its Additional Protocols)

<sup>31</sup> NIS Directive, Article 14(4)

<sup>32</sup> European Parliament. (2017). *Fact Sheets on the European Union: Judicial cooperation in criminal matters*. Available: [http://www.europarl.europa.eu/atyourservice/en/displayFtu.html?ftuid=FTU\\_5.12.6.html](http://www.europarl.europa.eu/atyourservice/en/displayFtu.html?ftuid=FTU_5.12.6.html). Last accessed 05/05/2017.

- The 1990 Schengen Agreement
- The 2000 Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union
- Framework Decision 2003/577/JHA — executing freezing orders abroad
- Council Framework Decision 2006/960/JHA on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union
- Council Framework Decision 2008/978/JHA of 18 December 2008 on the European evidence warrant for the purpose of obtaining objects, documents and data for use in proceedings in criminal matters
- Directive 2014/41/EU regarding the European Investigation Order in criminal matters (Repealing Framework Decision 2003/577/JHA as of May 2017)

### **3.5.1 Competence in Criminal and Judicial Cooperation**

The applicability of criminal and judicial cooperation structures typically depends on whether or not an entity has status as a competent, law enforcement, judicial, or administrative authority of a Member State under such instruments.<sup>33</sup> In the context of ECOSSIAN, N-SOC and E-SOC level entities may retain law enforcement competence. However, most operators of essential services, digital service providers, and competent authorities established in compliance with the NIS Directive will not have such competence or powers. O-SOC level and most N-SOC level entities will thus lack standing to use the information sharing procedures encompassed by the decisions and directives following the European Convention on Mutual Assistance in Criminal Matters and the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union. However it must be noted that entities lacking these competencies still have domestic legal obligations to share or provide access to data enacted to approximate the contents of regional instruments.

### **3.5.2 Bodies with Law Enforcement Competence**

To the extent that entities have law enforcement competence, they may also have the authority to share information through voluntary and formalized procedures. Firstly, authorities of CoE member states may through the course of investigations share information spontaneously with counterparts in other states, so-called “Spontaneous information sharing”. Secondly, they may also have the powers to request that a national judicial authority passes on a formal request for assistance to a judicial authority in another EU and CoE Member States as well as towards any other jurisdiction applicable under multilateral or bilateral agreements. They can likewise be required to execute such requests.

#### **3.5.2.1 Spontaneous Information Sharing**

Spontaneous information sharing is a collaboration method derived from the CoE and Article 34 TEU mandates on cross-border criminal and judicial cooperation. According to the Convention on European Mutual Assistance in Criminal Matters between the Member States of the European Union and the Convention on Cybercrime it entails voluntary forwarding of

---

<sup>33</sup> ENISA (2011) A flair for sharing – encouraging information exchange between CERTs: A study into the legal and regulatory aspects of information sharing and cross-border collaboration of national/governmental CERTs in Europe (Initial Edition 1.0 November 2011)

information with another authority through the course of a criminal investigation when that information might assist the criminal investigations of the receiving party. It typically encompasses cooperation between authorities with a law enforcement function such as a competent authority to the European Convention on Mutual Assistance in Criminal Matters and its Second Additional Protocol. Spontaneous information must be undertaken within the limits of the law.<sup>34</sup> The regional instruments grant the providing party the ability to request confidentiality or lay down binding conditions on the receiver of the information regarding the use of the information.<sup>35</sup> However, the receiving party also has the opportunity to notify the sender if the sender will not be able to comply with the conditions prior to the receipt of spontaneously shared information.<sup>36</sup>

### 3.5.2.2 Requests for Assistance

Requests for Mutual Legal Assistance (MLA) or Judicial Assistance are mechanisms whereby a Court, Judge or Prosecutor in one country requests the cooperation of a counterpart in another country. Requests for MLA or letters rogatory are addressed at specific competent authorities designated by the Member States for the receipt of requests. The ability to make requests for MLA are enshrined in domestic law and subject to arrangements between states through multilateral instruments or specific bilateral agreements. In Europe MLA applies to criminal proceedings and proceedings brought by administrative authorities that may give rise to criminal proceedings before a court or proceedings where a person may incur liability in a Member State.<sup>37</sup> MLA has been regulated multilaterally between the European states through:

- The 1959 CoE European Convention on Mutual Assistance in Criminal Matters,
- The 1978 Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters,
- The 1990 Schengen Agreement, and
- The 2000 Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union

Requests for assistance may take the form of a *letter of request* commonly known as a *letter rogatory*, typically seeking access to evidence or persons in criminal or judicial proceedings. Requests relate to procuring evidence or transmitting articles to be produced in evidence, records or documents. Regional instruments have thus formalized the sources evidence that states may seek, as well as the means of seeking them from one another, both in respect to traditional crime and in specialized instruments for cybercrime.

### 3.5.2.3 Harmonization of Evidentiary Sources

Conventional requests for assistance are focused on obtaining tangible evidentiary sources. For example, Article 3 of the European Convention on Mutual Assistance in criminal matters

---

<sup>34</sup> Article 7(1), the Convention on European Mutual Assistance in Criminal Matters; Article 26(1) Convention on Cybercrime

<sup>35</sup> Article 7(2), the Convention on European Mutual Assistance in Criminal Matters between the Member States of the European Union; Article 11(2 and 3), Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters Article 26(2) Convention on Cybercrime.

<sup>36</sup> Article 26(2), Convention on Cybercrime.

<sup>37</sup> Article 3, 2000 Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union.

concerns the “transmitting articles to be produced in evidence, records or documents” as well as securing witness and expert testimony. The Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union expedited expert and witness hearings through telephone conference.<sup>38</sup>

Within the CoE, Recommendation No. R (95)13 urged Member States to amend domestic criminal procedural law in searches and seizures as well as technical surveillance and expediting procedures for requesting evidence connected with information technology, also through MLAs.<sup>39</sup> The Convention on Cybercrime similarly imposes obligations for High Contracting Parties to afford “mutual assistance to the widest extent possible”<sup>40</sup> through the mechanisms of the Convention, provisions in other multilateral instruments, and domestic law.

Substantively, these instruments have approximated the intangible evidentiary sources relevant to the investigation of cybercrime and available through MLA. Recommendation No. R (95)13 appealed to Member States to legalize, *inter alia*, investigations of computer systems, seizure of data, collection of traffic data, as well as making automatically processed data functionally equivalent to traditional documents where applicable under criminal procedural law. The Parties to the Convention on Cybercrime must analogously ensure:

- i) the preservation of stored computer data,<sup>41</sup>
- ii) partial disclosure of traffic data,<sup>42</sup> as well as the
- iii) powers of competent authorities to conduct searches and seizures<sup>43</sup> of computer data.

A competent authority’s Production Orders pursuant to the Convention<sup>44</sup> may be directed at “persons” in the case of computer data and “service providers” in the case of traffic data. The Convention further exhorts Parties to legalize searches and seizures to ensure generalized access to computer systems and computer data of relevance to criminal investigation.<sup>45</sup>

Authorities designated to respond to MLA will frequently have judicial competence, making it unlikely that a party to ECOSSIAN would be a direct responder. To the extent that N-SOCs have law enforcement competencies, they may be called on to execute MLA. It is also possible that experts working within N-SOCs may be called upon to give expert opinion or witness testimony to significant incidents that have been criminalized.

### 3.5.2.4 Procedure for Requests & Sharing

Letters rogatory issued by judicial authorities have been the traditional international means to secure assistance from states. The European Convention on Mutual Assistance in Criminal Matters and Convention on Cybercrime rely on letters rogatory as the primary means of

---

<sup>38</sup> Article 11, 2000 Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union.

<sup>39</sup> Appendix to Recommendation No. R (95)13 Concerning Problems of Criminal Procedural Law Connected with Information Technology

<sup>40</sup> Article 23, *ibid*.

<sup>41</sup> Article 16, *ibid*.

<sup>42</sup> Article 17, *ibid*.

<sup>43</sup> Article 19, *ibid*.

<sup>44</sup> Article 18, *ibid*.

<sup>45</sup> Article 19. *Ibid*.



procuring evidence or transmitting articles to be produced in evidence, records or documents for criminal proceedings. The CoE has also exhorted members to make possible the Interconnection of files and online access through Recommendation No R(87) 15,<sup>46</sup> giving police direct access to files in MLA. The interconnection of a file may only be granted to Police if:

- i) it has been granted by a supervisory body for the purpose of inquiry into a particular offence,
- ii) it is in compliance with a clear legal provision,
- iii) in accordance with domestic law, and
- iv) satisfying Principles 3 to 6 of the Recommendation regulating the storage of data, use of data and communication of data.

Requests for assistance between European Union authorities with law enforcement competence has taken various forms pursuant to Framework Decisions. Directive 2014/41/EC repeals most of the existing laws on the transfer of evidence between Member States as of May 2017, making the European Investigative Order (EIO), the main means of cross border requests for assistance. In all, these requests may consist of:

#### **i) Freezing orders**

Freezing orders are measures taken by a judicial authority to prevent the destruction, degradation, alteration or removal of objects, documents or data which have been proceeds or instrumentalities of a criminal offence and could be produced as evidence in criminal proceedings.<sup>47</sup> European Freezing Orders are regulated by Framework Decision 2003/577/JHA.

#### **ii) European Evidence Warrants (EEW)**

The European Evidence Warrants are a judicial decisions issued by a competent authority to obtain objects, documents, and data, such as through searches and seizures, for criminal proceedings, proceedings before administrative or judicial authorities that may give rise to criminal proceedings before a court.<sup>48</sup> EEWs are regulated through Council Framework Decision 2008/978/JHA.

#### **iii) European Investigation Order (EIO)**

The European Investigation Order is a judicial decision issued or validated by a judicial authority to have any investigative measure carried out in a Member State (other than setting up joint investigative teams) to obtain evidence for criminal proceedings, proceedings before administrative or judicial authorities that may give rise to criminal proceedings before a court.<sup>49</sup> EIOs may be issued as part of national criminal procedure and rights of defense at the request of a suspect of crime or their lawyer. EIOs are regulated by Directive 2014/41/EC.

<sup>46</sup> Paragraph 5.6 Recommendation No. R (87) 15 regulating the use of personal data in the police sector

<sup>47</sup> Articles 1-3, Framework Decision 2003/577/JHA.; European Justice. (2015). *Freezing of assets and evidence*. Available: [https://e-justice.europa.eu/content\\_freezing\\_of\\_assets\\_and\\_evidence-93-en.do](https://e-justice.europa.eu/content_freezing_of_assets_and_evidence-93-en.do). Last accessed 04/05/2017.

<sup>48</sup> Articles 1, 5, and 11 Council Framework Decision 2008/978/JHA; European Justice. (2016). *Evidence*. Available: [https://e-justice.europa.eu/content\\_evidence-92-en.do](https://e-justice.europa.eu/content_evidence-92-en.do). Last accessed 04/05/2017.

<sup>49</sup> Articles 1, 3 and 4 Directive 2014/41/EU.

### 3.5.3 Bodies without Law Enforcement Competence

Most CERTs do not play a primary function in criminal investigation or criminal procedure. ENISA observes that CERTs generally lack the statutory mandate to participate in this process, as well as the competence to assess criminal and procedural law aspects to cybercrime investigation. However, they are frequently the first responders to criminal activities and first collectors of potential evidence.<sup>50</sup>

While requests for assistance are directed at Member States and their judicial, competent or administrative authorities, and not at ECOSSIAN *per se*, it is possible that requests will be directed at information produced through the course of ECOSSIAN's detection both within O-SOCs and N-SOCs. This may especially be the case when a state has been made aware of the existence of information relevant criminal and judicial proceedings through voluntary information sharing or as the result of investigations carried out in another Member State on crimes of cross-border nature. The sharing of information on incidents, such as through the mandatory notifications of the NIS Directive, can have the effect that competent authorities, or CSIRTs, and points of contact have increased discretion in determining when information is reported to law enforcement, a matter which has largely been at the discretion of first respondents. As noted previously, it has been observed that issues such as secrecy, trust, and reputation have previously dissuaded disclosure to law enforcement. ECOSSIAN must thus stay informed of reporting obligations under domestic criminal law.<sup>51</sup> Request for mutual legal assistance can affect ECOSSIAN through domestic:

- Production orders for stored computer data
- Search and seizure measures including:
  - a) a computer system, part of it, or a computer-data storage medium,
  - b) making and retaining copies of computer data,
  - c) maintaining the integrity of the relevant stored computer data,
  - d) removing or rendering data inaccessible within the computer system,

Witness and expert testimony may be relevant to O-SOC, N-SOC and E-SOC level entities within ECOSSIAN.

As previously observed, most of the CoE and EU Member State jurisdictions permit law enforcement and other investigating authorities to compel persons to hand over objects under their control or provide information required in a criminal investigation. These investigatory powers have also substantively affected by developments in European regional law on cybercrime. Directive 2013/40/EU which harmonizes definitions of cybercrime across jurisdictions invites the Member states to set up collaboration to preserve evidence of crime and identify offenders. Within the CoE, the Convention on Cybercrime likewise harmonizes domestic definitions of crime<sup>52</sup> and Recommendation R (95) 13 urges High Contracting Parties to adopt legal powers to seize and compel evidence in criminal procedural law connected to information technology.<sup>53</sup> For example, Articles 18/16 and 18/17 of Act of 1998 Governing the Intelligence and Security Services in Belgium allows the intelligence and security service to compel network operators, electronic communications service providers or "any other person having particular knowledge of a computer system" to provide information

---

<sup>50</sup> ENISA (2012) Give and Take: Good Practice Guide for Addressing Network and Information Security - Aspects of Cybercrime Legal, Regulatory and Operational Factors Affecting CERT Co-operation with Other Stakeholders. 47

<sup>51</sup> See also Recommendation No. R (89) 9 on Computer-Related Crime

<sup>52</sup> Para 23 Directive 2013/40/EU

<sup>53</sup> Recommendation R (95) 13 Concerning Problem of Criminal Procedural Law Connected with Information Technology.

or access to systems.<sup>54</sup> Comparable provisions are also found in the Dutch Act of 7 February providing rules relating to the intelligence and security services (WIV 2002) (Articles 24, 28 and 29),<sup>55</sup> and the French Code de la sécurité intérieure (Article L851-1 and Title VII).

The harmonization of criminal law in the area of cybercrime has further generated domestic law obligations to report knowledge of certain criminal activities. For example, as mentioned in previous deliverables, Article 19 of the 2011 Criminal Justice Act of Ireland there is a legal obligation to report relevant information of serious crimes to the Gardai (national police force).<sup>56</sup> The Irish Criminal Justice Act thus imposes a positive obligation to report certain crimes. Chapter 13 of the Swedish Penal Code makes the comparable proscription that failure to disclose certain serious crime, in particular *data intrusions* amounting to *sabotage* may incur criminal liability.<sup>57</sup> § 4 of Chapter 13 provides that an act amounts to sabotage by “damaging property, which is of considerable importance to national defense, public security, law enforcement or the administration or for the maintenance of public order and security in the kingdom.” The Swedish example goes farther than codifying a positive obligation to report, it criminalizes failure to disclose sabotage as an act of aiding and abetting. In result, criminal laws across European jurisdictions have created intermittent obligatory responsibilities for operators of networks and Critical Infrastructure to share information on cybercrime.

### 3.5.3.1 Guidance for Bodies without Law Enforcement Competence

The Budapest Convention brought about the *Guidelines for the cooperation between law enforcement and internet service providers against cybercrime* (the CoE Guidelines). The Guidelines apply to public or private entity that provides to users of its service the ability to communicate by means of a computer system, and any other entity that processes or stores computer data on behalf of such communications service or users of such services. As this definition is incongruent both with the NIS Directive’s concept of “an operator of essential services” (Article 5(2) and Annex II), and the Directive 2008/114/EU<sup>58</sup> definition of “European Critical Infrastructure”, it is unlikely to have any significant regional or cross-border application. Moreover, Guideline’s scope is sufficiently broad overlap with the Directive 2008/114/EU definition of “Critical Infrastructure” and possibly with national law concepts of Critical Infrastructure relevant to domestic O-SOC and N-SOC relationships.

## 3.6 Data Protection in Criminal & Judicial Cooperation

While police, intelligence, and criminal justice authorities are historically exempted from much of European data protection law, e.g. the Data Protection Directive and Regulation (EU) 2016/679 of the General Data Protection Regulation (GDPR), specialized instruments have been developed within the CoE and EU to regulate data protection within law enforcement communities. In the Council of Europe, the Convention for the Protection of

<sup>54</sup> Belgian Standing Intelligence Agencies review Committee. (n.d.). *Legislation*. Available: <http://www.comiteri.be/index.php/en/legislation>. Last accessed 04/05/2017.

<sup>55</sup> Wet op de Inlichtingen- en Veiligheidsdiensten 2002

<sup>56</sup> Criminal Justice Act 2011, Number 22 of 2011.

<sup>57</sup> Brottsbalk (1962:700) Svensk författningssamling 1962:700

<sup>58</sup> Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection [2008] OJ L345/75.



Individuals with regard to Automatic Processing of Personal Data, regulating automatically processed personal data, is the main legislative reference point, enforced by selective “sectoral” instruments.<sup>59</sup> Data protection for the police sector was developed over time in piecemeal fashion, responding to two technological developments; i) the automated processing of personal data, and ii) the data protection in mutual assistance against cybercrime. Particular note should be taken of the data protection standards derived the Recommendation No. R (87) 15, the most comprehensive CoE data protection framework, regulating both law enforcement authorities as well as other public authorities that process personal data for police purposes.<sup>60</sup> Aspects of these data protection standards can resultantly be implemented as a measure of good practice by any N-SOC that shares personal data with LEAs for criminal proceedings. The EU on the other hand has harmonize minimum binding rules for Member State law enforcement. The Police and Criminal Authorities Directive (Directive (EU) 2016/680) adopted under the ambit of the data protection reforms, is thus the main reference source for any EU Member State on data protection in cross-border criminal cooperation.<sup>61</sup> These affect both the internal processing of personal data as well as the sharing of personal data between criminal and judicial authorities at national level. These responsibilities must be implemented by competent N-SOCs as binding obligations. Summarily, the pertinent instruments to data protection in European information sharing on criminal proceedings encompasses:

- The 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) (and its 2001 Additional Protocol with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows)
- Recommendation No. R (87) 15 regulating the use of personal data in the police sector,
- Recommendation 1181 (1992) on police co-operation and protection of personal data in the police sector,
- The 2001 Convention on Cybercrime,
- Council Framework Decision 2006/960/JHA on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union,
- Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, and
- Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data

---

<sup>59</sup> COUNCIL OF EUROPE COMMITTEE OF MINISTERS EXPLANATORY MEMORANDUM to Recommendation No. R (87) 15 of the Committee of Ministers to member states regulating the use of personal data in the police sector 1 (Adopted by the Committee of Ministers on 17 September 1987 at the 410th meeting of the Ministers' Deputies)

<sup>60</sup> Recommendation No. R (87) 15

<sup>61</sup> Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data.

<sup>61</sup> Article 1, Directive (EU) 2016/680

### 3.6.1 Automated Processing of Personal Data

The 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) was the first binding instrument within the CoE to impose obligations of data protection in the public and private sectors. The objective of Convention 108 is to secure the respect for fundamental freedoms, the right to privacy, in the automatic processing of personal data. To ensure these rights, the Convention institutes procedural safeguards on automated processing as well as a prohibition on the processing of certain special categories of sensitive data, namely racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life. Convention 108 also regulates transborder flows of data. It delegated the task of furnishing legal guidance on administrative practices for data protection to designated authorities.<sup>62</sup> All the acceding states (i.e. excluding Armenia, Azerbaijan, Bulgaria, Georgia, Greece, Malta, Montenegro, Poland, Russia and Ukraine) have national authorities in place to provide interpretation on mutual assistance. The Additional Protocol to Convention 108<sup>63</sup> incorporated stronger oversight structures for both senders and recipients of automated personal data to ensure an “adequate level of protection” for the data subject. While the Convention did not explicitly lay down requirements to implement its basic data protection principles in the context of transborder flows of personal data, the Additional Protocol enhanced data protection in this context. The Additional Protocol directly imputed the standards from Convention 108 to transboundary dissemination of automated personal data.<sup>64</sup>

#### 3.6.1.1 Definitions: Personal Data & Automatic Processing

As already mentioned, Convention 108 regulates *automated personal data*. “Automatic processing” entails “storage of data, carrying out of logical and/or arithmetical operations on those data, their alteration, erasure, retrieval or dissemination” by automated means. The application of the Convention to *dissemination* further enforces the notion that transfers of personal data are regulated activities. Personal data include “any information relating to an identified or identifiable individual”. The scope of the Convention and Additional Protocol resultantly covers any computerized handling of data about an individual who may be recognized through the contents of the data. Convention 108 imposes obligations for both private and public bodies, so-called “controllers”, which are:

*natural or legal person, public authority, agency or any other body who is competent according to the national law to decide what should be the purpose of the automated data file, which categories of personal data should be stored and which operations should be applied to them.*

#### 3.6.1.2 Obligations for Controllers

Convention 108 substantively required the High Contracting Parties to give effect to a set of basic principles in domestic law. The summative data protection standards set out by these principles can be condensed to seven conditions for dissemination:

<sup>62</sup> Chapter IV, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data

<sup>63</sup> Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows

<sup>64</sup> Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows (Ets No 181)

- Dissemination is fair and lawful (fairness and legality),
- Dissemination is limited to the legitimate purpose for which the data was initially stored (purpose limitation),
- The accuracy of the data is assured in dissemination (accuracy),
- The data is disseminated with appropriate measures for the protection of personal data against accidental or unauthorized destruction or accidental loss as well as against unauthorized access, alteration or dissemination (data security)
- Dissemination must be subject to review by independent competent authorities with powers to investigate, intervene, hear individual complaints, engage in judicial proceedings, and bring violations to the attention of judicial authorities (adequate level of protection), and
- There may be no dissemination of special categories of data, e.g. revealing, racial origin and religion, without the existence of additional safeguards in law.

Dissemination may only occur when the recipient ensures an adequate level of protection, the transfer is in the interest of the data subject, there are legitimate prevailing interest, or the competent authority has found that there are adequate contractual clauses in place. However, it must be noted that the parties to Convention 108 and its Additional Protocol may derogate from all data protection obligations except the legality and data protection conditions to secure overriding interests such as state security, public safety and the suppression of criminal offences.<sup>65</sup> This severely limits the application of Convention 108 in the detection and prevention of crime as well as mutual assistance in criminal investigations and proceedings.

### 3.6.1.3 Automated Processing of Personal Data in the Police Sector

Recommendation No. R (87) 15 is a CoE instrument standardizing principles for CoE Member States in the collection, storage, use and communication of personal data for police purposes. While other CoE instruments are binding, the Recommendation forms the most comprehensive guidance for data protection in the police sector. It was adopted in view of the increasing reliance of automatic processing of personal data and with an objective of balancing security interests with individual rights. The concept of police purposes covers all tasks undertaken by a police authority to suppress crime or maintain public order. Most of the principles contained in the Recommendation resultantly apply to authorities with law enforcement competence. However, it is critical to understand that the Recommendation also regulates any *responsible body* that automatically processes personal data for police purposes. Within the context of ECOSSIAN, the recommendation is of bearing to any N-SOC with law enforcement authority as well as any other N-SOC administering files that may be of recurrent use in police investigations. The latter type of N-SOC could typically collate to competent authorities and single points of contact under the NIS Directive. It must be noted however that the implementation of the Recommendation is uneven across CoE Member States.<sup>66</sup>

Moreover, while the Recommendation makes suggestions relevant to the “communication” of personal data, a CoE review from 1994 generated a follow-up Recommendation - Recommendation 1181 (1992) - for the purposes of intergovernmental police cooperation

<sup>65</sup> Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Ets No 108)

<sup>66</sup> CoE (2002) REPORT ON THE THIRD EVALUATION OF RECOMMENDATION N° R (87) 15 REGULATING THE USE OF PERSONAL DATA IN THE POLICE SECTOR

such as through Europol and Interpol.<sup>67</sup> Recommendation 1181 (1992) does not propose to regulate intergovernmental organizations directly. It rather invokes that Member States should ensure the application of its suggestions, and the principles contained in Recommendation No. R (87) 15 in the exchange of personal data between Member States and with third parties via Interpol. The principles of Recommendation No. R (87) 15 have further been acknowledged for the EU Member States' exchange of information and intelligence for criminal investigation by Council Framework Decision 2006/960/JHA.<sup>68</sup> The Europol Convention has also adopted the CoE principles as its own data protection standards, including those contained in Recommendation No. R (87) 15.<sup>69</sup> Although CoE Recommendations are not binding, and national implementation varies, Europol's adoption of Recommendation No. R (87) 15 presents a strong case for its implementation in all European cross-border cooperation on criminal matters. It is therefore recommended that N-SOCs within ECOSSIAN assume these principles in their communication with any N-SOC or E-SOC with law enforcement competence as a matter of good practice.

#### 3.6.1.3.1 Definitions: Personal Data & Data Processing

Recommendation No. R (87) 15 defines personal data as “any information relating to an identified or identifiable individual. An individual shall not be regarded as “identifiable” if identification requires an unreasonable amount of time, cost and manpower”. The terminology *any information* reflects the significant breadth in scope of the Recommendation. Whether or not information makes an individual identifiable must be determined through objective technical understanding of the means and methods available to police authorities to infer identity through information.<sup>70</sup>

Unlike many other data protection instruments, the Recommendation does not define “processing” but rather defines a scope encompassing “the collection, storage, use and communication of personal data for police purposes which are the subject of automatic processing”. As such, the Recommendation find its explicit application to transfer of data, or information sharing, through its bearing on the *communication of personal data*. While its application is primarily meant for automated personal data, Member States may themselves opt to apply its principles to personal data that is not subject to automated processing.

#### 3.6.1.3.2 Recommendations for Police Authorities

Recommendation No. R (87) 15 recommend overarching principles to data protection in the police sector. While these may serve as general guidelines, only a few of them can be directly applied to situations of information sharing and transmitting personal data. Principle 5 regulates the communication of personal data *from* and authority with law enforcement competence specifically. Firstly, it establishes that communication with other LEAs must only occur when there is a legitimate lawful interest. Secondly, international communication of

<sup>67</sup> CoE (2002) REPORT ON THE THIRD EVALUATION OF RECOMMENDATION N° R (87) 15 REGULATING THE USE OF PERSONAL DATA IN THE POLICE SECTOR

<sup>68</sup> Council Framework Decision 2006/960/JHA on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union

<sup>69</sup> COUNCIL ACT of 26 July 1995 drawing up the Convention based on Article K.3 of the Treaty on European Union, on the establishment of a European Police Office (Europol Convention)

<sup>70</sup> COUNCIL OF EUROPE COMMITTEE OF MINISTERS EXPLANATORY MEMORANDUM to Recommendation No. R (87) 15 of the Committee of Ministers to member states regulating the use of personal data in the police sector (Adopted by the Committee of Ministers on 17 September 1987 at the 410th meeting of the Ministers' Deputies)

personal data can be premised on either national and international legal bases or the prevention of a “serious and imminent danger”. The Recommendation in its entirety standardizes five criteria common to all communications of personal data, in particular that police authorities must ensure:

- the existence of a clear legal basis for communicating the data (legality),
- checks ensuring the quality, accuracy and reliability of data prior to communication and the possibility of rectifying mistakes after communication (accuracy and reliability),
- the ability to secure the data subject’s rights after communication, specifically rights of rectification and erasure (rectification and erasure)
- guarantees that the data will only be used for the purposes specified in the request, or that any other uses of the data will be subject to agreement (purpose limitation)
- that all measures necessary are taken for the physical and logical security of the data (data security)

### 3.6.1.3.3 Recommendations for Responsible Bodies

The concept of a *responsible body* is analogous to a “controller: under Convention 108 and covers all public bodies that have statutory authority to decide on the purpose of a file. Responsible authorities are thus be national authorities with a law enforcement competence, or a national authority without law enforcement competence but with files that are automatically processed for police purposes. In ECOSSIAN, this may encompass any N-SOC that furnishes personal data to law enforcement. Subsequently to the adoption of the NIS Directive within the EU, competent authorities such as CSIRTs are especially likely to take on the role of responsible body due to their formalized reporting on criminalized incidents towards law enforcements. Recommendation No. R (87) 15 introduces two suggestions specifically for responsible bodies that automatically process personal data for police purposes. Firstly, it gives interpretive authority to the national Supervisory authorities. A responsible body that is unsure of how the Recommendations ought to be applied in any case of relevant automated processing should thus consult their national Supervisory Authority. Secondly, the Recommendation suggests that responsible bodies have responsibility to assure the security of data, in particular for preventing unauthorized access, communication or alteration. Furthermore, it should be understood that the responsible body decides on the implementation of security measures. The role of the Supervisory Body to the Recommendation is merely advisory and cannot give binding opinions.<sup>71</sup> The privacy-by-design recommendations presented in Deliverable 7.2 to ECOSSIAN would thus go some way in adhering to the spirit, if not the letter, of Recommendation No. R (87) 15.

## 3.6.2 Data Protection & Mutual Assistance on Cybercrime

The harmonization of mutual assistance and access to intangible evidentiary sources in the Convention of Cybercrime is also complemented with data protection responsibilities. Access to trans-border data under the Convention is premised on three scenarios:

- i) Access with authorization.

---

<sup>71</sup> COUNCIL OF EUROPE COMMITTEE OF MINISTERS EXPLANATORY MEMORANDUM to Recommendation No. R (87) 15 of the Committee of Ministers to member states regulating the use of personal data in the police sector (Adopted by the Committee of Ministers on 17 September 1987 at the 410th meeting of the Ministers' Deputies)



Article 25 of the Convention sets out general principles to authorized mutual assistance for criminal and judicial cooperation against cybercrime, namely that it must be:

- Enshrined in law and through other administrative measures (legality)
  - Subject to conditions set out by law or mutual assistance treaty, including grounds for refusal of assistance (conditionality),
  - Must be provided with “appropriate levels of security and authentication (including the use of encryption, where necessary)” (data security).
- ii) Access with authorization but in the absence of a mutual legal assistance agreement.

Articles 27 and 28 of the Convention regulates situations where there mutual assistance involves a state that is not party to the convention, and in the absence of mutual assistance treaties or reciprocal agreements. Under such circumstances, MLA must

- Not be incompatible with the law (legality),
  - Kept confidential, at the appeal of the requesting party if the receiving party is capable of complying with confidentiality, or if the receiving party is incapable of complying with the request for assistance (confidentiality), and
  - Must only be used for investigations and proceedings stated in the request (purpose limitation).
- iii) Access without authorization.

Pursuant to Article 32 of the Convention, a competent authority can seek access to stored computer data without an authorization if a) the stored computer data is publically available, or b) the competent authority has obtained the voluntary consent of a person with lawful authority to disclose the data.

### **3.6.3 The Police & Criminal Authorities Directive**

As of 2016 the GDPR, specifically Directive (EU) 2016/680<sup>72</sup> (Police and Criminal Authorities Directive) repeals Council Framework Decision 2008/977/JHA, transposing its substantive standards as of May 2018. It is the foremost regional regulatory framework for the data protection in criminal and judicial authorities in Europe. The Police and Criminal Authorities Directive has a much wider scope of application than the Framework Decision, regulating not only police and judicial cooperation in criminal matters, but processing of personal data within criminal authorities comprehensively.<sup>73</sup> As an obligation under Article 8(1) of the Charter of Fundamental rights of the European Union and Article 16(1) of the Treaty on the Functioning of the European Union, the right to data protection is universal to the Member States of the European Union. The right must consequently be assured to all natural persons

<sup>72</sup> Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data.

<sup>73</sup> Statement of the Council's reasons: Position (EU) No 5/2016 of the Council at first reading with a view to the adoption of a Directive of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (2016/C 158/02)

irrespective of their nationality or residence.<sup>74</sup> The Police and Criminal Authorities Directive also applies more broadly than comparable CoE instruments, encompassing data processed by fully or partially automated means as well as by other means and forming part of a filing system or intended for a filing system. As determined by its scope, the Directive regulates authorities with criminal and judicial competence, which some N-SOC entities in ECOSSIAN may have. However, the Directive exempts Union institutions and thereby E-SOCs. Article 18 of the Police and Criminal Directive (EU) 2016/680 within the GDPR was adopted with the dual objectives of:

*(a) protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data; and*

*(b) ensure that the exchange of personal data by competent authorities within the Union, where such exchange is required by Union or Member State law, is neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.<sup>75</sup>*

This objective expands on the limited intent of the framework decisions, i.e. ensuring a “high level of protection of the fundamental rights and freedoms”. It is also more forceful approach to asserting the legitimacy of information sharing in the context of criminal investigations and proceedings than the original proposed wording of ensuring “the exchange of personal data between competent authorities within the Union.”<sup>76</sup> Prevention, investigation and detection of crime are interests of the data subject and are therefore a sufficient legal bases for processing personal information without consent.<sup>77</sup> In that way, the Directive expedites procedure if personal data processing for detection and prevention as a matter of regional law.

### 3.6.3.1 Definitions: Personal Data & Data Processing

The bearing of the Police and Criminal Authorities Directive on the specific act of processing is made explicit by adopting a comparable definition of processing as the GDPR, i.e. encompassing “disclosure by transmission, dissemination or otherwise making available” personal data. In its entirety, the Directive harmonizes national law with the following notion of processing:

*any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;*

The Directive further defines “personal data” as:

<sup>74</sup> Statement of the Council’s reasons: Position (EU) No 5/2016 of the Council at first reading with a view to the adoption of a Directive of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (2016/C 158/02)

<sup>75</sup> Article 1, Directive (EU) 2016/680

<sup>76</sup> Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL: on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data (COM(2012) 10 final 2012/0010 (COD))

<sup>77</sup> Recital 35, Directive (EU) 2016/680

*any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*

The definition contained within the Directive identifies several factors that hold relevance to the identification of a natural person, namely the “physical, physiological, genetic, mental, economic, cultural or social” attributes of their identity. The Police and Criminal Authorities Directive goes farther than previous instruments regulating data protection in the context of criminal proceedings by summing and defining three additional categories of personal data related to these attributes of identity, “genetic data”, “biometric data” and “data concerning health”. *Genetic data*, resulting of analysis and extraction of chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) from a person is considered to be especially sensitive and entail great risk of abuse. The prohibition against discrimination on the basis of such data is absolute under the Directive.<sup>78</sup> *Data concerning health* is understood to be derived from testing and examination of the body and can produce information on a person's physiological and biomedical state such as disease, medical history and disability. It has a more extensive meaning than the other two special categories and can encompass both *genetic* and *biometric data*. These additional categories of personal data are of limited application within ECOSSIAN as they encompass information which is almost exclusive to the health sector. It should nevertheless be recalled that the health sector is classified as *operators of essential services* by Annex II to the NIS Directive.<sup>79</sup> It can therefore not be excluded that competent authorities with law enforcement competencies may need to process such data in an investigation of cybercrime. It is conceivable for example, that incidents may consist of targeted intrusions to compromise medical data, or that police will have to investigate forensic artefacts within files containing such data. The specific definitions for these categories of data are enshrined in Article 3 of the Directive:

*(12) 'genetic data' means personal data, relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;*

*(13) 'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;*

*(14) 'data concerning health' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.*

### 3.6.3.2 Application to Controllers

The Police and Criminal Authorities Directive requires that “controllers” of personal data comply with certain principles of data protection. Moreover pursuant to the objective and scope of the Directive, it codifies these principles for the particular tasks undertaken by

<sup>78</sup> Recital 23

<sup>79</sup> Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, ANNEX II “TYPES OF ENTITIES FOR THE PURPOSES OF POINT (4) OF ARTICLE 4”



“competent authorities”. Consequently, both definitions must be observed to understand the application of the Directive:

(7) ‘competent authority’ means:

(a) any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; or

(b) any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

(8) ‘controller’ means the competent authority which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

In essence, the Directive regulates situations where *competent authorities*, process personal data and thus become *controllers*. The application of the Directive can be determined by whether an entity has a domestic statutory functions relating to the prevention, investigation, detection and prosecution of criminal offences, or the execution of criminal penalties or has been entrusted or delegated a responsibility to carry out such functions. A competent authority can be any body or entity that is entrusted by a members state to exercise those powers. The effect of the definition is that law enforcement authorities, judicial authorities, as well as private entities entrusted with investigative and judicial powers can have controller status.<sup>80</sup> Notably, the law enforcement and judicial functions can entail the processing of data in the domestic statutory context, e.g. domestic criminal law and procedural law, or in the discharge of duties originating from Community instruments; e.g. mutual assistance and cooperation on cross-border crime. It is also a key characteristic of a controller that they define the purpose and means for processing, or operate under a statutory mandate that defines their means and purposes for them. Additionally, It should further be highlighted that the definition imposes both separate and joint responsibilities. This means that as national law harmonizes these standards, all competent authorities that process data alone or collectively are required to uphold the principles of the Directive. This is especially relevant to the context of ECOSSIAN where information can be shared between competent authorities at N-SOC level or possibly be accessed within the system by multiple partners with law enforcement competence.

### 3.6.3.2.1 Appropriate Technical & Organizational Measures

Article 19 determines that Controller is responsible for taking “appropriate technical and organisational measures” to demonstrate its compliance with the Directive. The implementation of measures must take into account the severity and likelihood of risks to individual rights and freedoms as well as the nature, scope and context in which the processing takes place. These measures include having appropriate data protection policies in place. Following Article 23, persons acting under the authority of the controller must only

<sup>80</sup> Statement of the Council’s reasons: Position (EU) No 5/2016 of the Council at first reading with a view to the adoption of a Directive of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (2016/C 158/02)

process data on instruction from the controller. Moreover, controllers may only use processors that themselves provide “sufficient guarantees” that they can implement appropriate technical and organizational measures to comply with Directive.

### 3.6.3.2.2 Logging & Recording

It is further incumbent on the controller to see that processing operations are logged and recorded as set out in the Directive. The controller must log, at least, the i) justification, ii) date and time, iii) disclosing persons, and iv) the recipients of the data. The logging must encompass all collection, alteration, consultation, disclosure, transfers, combination, and erasure of personal data pursuant to Article 25. Logs may only be disclosed to verify the legality of processing and in criminal proceedings, self-monitoring and internal assurance of data integrity and security. Article 24 provides that records must also provide the following information, in electronic and paper form, on any processing under the responsibility of the controller:

- (a) the name and contact details of the controller and, where applicable, the joint controller and the data protection officer;*
- (b) the purposes of the processing;*
- (c) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;*
- (d) a description of the categories of data subject and of the categories of personal data; (e) where applicable, the use of profiling;*
- (f) where applicable, the categories of transfers of personal data to a third country or an international organisation;*
- (g) an indication of the legal basis for the processing operation, including transfers, for which the personal data are intended;*
- (h) where possible, the envisaged time limits for erasure of the different categories of personal data;*
- (i) where possible, a general description of the technical and organisational security measures referred to in Article 29(1) [which concerns the security of processing].<sup>81</sup>*

### 3.6.3.3 Application to Processors

The Police and Criminal Authorities Directive introduces specific requirements for entities acting as “processors” of personal data on behalf of the competent authority. In this context, it defines a *processor* as:

*a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;*

The *controllers* and *processors* share a subset of commonalities but also have key differences to distinguish them by. Both controllers and processors are subject to obligations under the Directive by virtue of processing personal data. The Directive does not make a distinction for either category on the basis of whether the entity is a public or private body.<sup>82</sup>

<sup>81</sup> Brackets added

<sup>82</sup> 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 [first reading] - Political agreement (2012/0010 (COD))

In view of Article 3, which lays down the definitions, three key points emerge when differentiating between a controller and a processor. The processor processes personal data “on behalf of” the controller. A processor does not determine the purpose and means for processing, it merely carries out the processing for a controller that does. Furthermore, the processor would not operate under a statutory mandate that sets out purposes and means of processing for the prevention, investigation, detection or prosecution crime. Resultantly, if an O-SOC, N-SOC, or E-SOC, lacking law enforcement competence, processes personal data in response to a request from law enforcement, they are processors. This means that they will also have to comply with the data protection requirements applicable to processors under the regulation.

### 3.6.3.3.1 Lawfulness & Processing Under Contract

While it is the controller’s responsibility to only engage with processors offering “sufficient guarantees”, data processors must be able to demonstrate the lawfulness of their processing. This includes effective methods for ensuring self-monitoring, data integrity, and data security.<sup>83</sup> Any person acting under the processor’s authority may only process data under instructions from the controller, unless domestic law proscribes other arrangements.<sup>84</sup> Following Article 22, the processor may only engage with other processors with written authorization from the controller. It must further inform the controller of any changes in processors so that it may object to any changes. The Directive also imposes obligations on the member states to ensure that contract or laws are in place to guide processors. It is critical that ECOSSIAN and O-SOCs and N-SOCs that are likely to respond to law enforcement request stay seized of how these contracts or laws are formulated at domestic level. These contracts or laws will be binding in their regulation of processors on the “subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.” The Directive goes far in harmonizing specific aspects of the contracts and law that will regulate controllers, requiring specifically that such instruments stipulate:

- (a) acts only on instructions from the controller;*
- (b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;*
- (c) assists the controller by any appropriate means to ensure compliance with the provisions on the data subject’s rights;*
- (d) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of data processing services, and deletes existing copies unless Union or Member State law requires storage of the personal data;*
- (e) makes available to the controller all information necessary to demonstrate compliance with this Article; (f) complies with the conditions referred to in paragraphs 2 and 3 for engaging another processor.*

---

<sup>83</sup> Recital 96, Directive (EU) 2016/680

<sup>84</sup> See Article 23, Directive (EU) 2016/680

### 3.6.3.3.2 Record Keeping

The Police and Criminal Authorities Directive further imposes an obligation for Member States to harmonize minimum standards on the record keeping. Following this harmonization, national laws will, at the least, require that the processor records the following information about its processing activities in electronic and paper form:

- (a) the name and contact details of the processor or processors, of each controller on behalf of which the processor is acting and, where applicable, the data protection officer;*
- (b) the categories of processing carried out on behalf of each controller;*
- (c) where applicable, transfers of personal data to a third country or an international organisation where explicitly instructed to do so by the controller, including the identification of that third country or international organisation;*
- (d) where possible, a general description of the technical and organisational security measures referred to in Article 29(1) [which concerns the security of processing].<sup>85</sup>*

### 3.6.3.4 General Principles of Data Protection

Chapter II of the Police and Criminal Authorities Directive reiterates six principles relating to the processing of data. The principles are common to both Regulation (EU) 2016/679 and the Police and Criminal Authorities Directive but with key differences relating to the purposes and application to the instrument. The Member States must ensure, through the harmonization of domestic law, that personal data is:

- (a) processed lawfully and fairly (legality and fairness);*

Articles 4 and 8 of the Directive elaborates on the condition of lawfulness by establishing three criteria. Firstly, legality is premised on the existence of law at domestic level. Secondly, domestic law must be enacted to allow for processing of personal data only when it is necessary for the performance tasks of competent authorities as they are defined in the Directive. Finally, the domestic law sufficiently clear enough to specify at the least, which personal data is being processed and the objectives and purposes underlying that processing.

- (b) collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes (purpose limitation);*

In situations where competent authorities transmit personal data, purpose limitation must be enforced by imposing mandatory conditions on the recipient of the data.<sup>86</sup> These conditions should not be imposed when transmitting data to Europol, Eurojust, or the European Public Prosecutor's Office.<sup>87</sup> Processing for in the public interest or the purposes of scientific and historical research is regulated by Regulation (EU) 2016/679 to the GDPR.

- (b) adequate, relevant and not excessive in relation to the purposes for which they are processed (adequacy and relevance);*

The Directive distinguishes two ways through which controllers must ensure that the processing of data is not excessive. Firstly, Article 5 imposes the requirement to enforce time limits for storage and review. While this requirement does not have direct bearing on

<sup>85</sup> Brackets added

<sup>86</sup> See Article 9(3), Directive (EU) 2016/680

<sup>87</sup> See Articles 2(3) and 9(4), Directive (EU) 2016/680

situations of data transfers, the controller has the choice to enforce them on a recipient of personal data.<sup>88</sup> Secondly, Article 10 affords additional protection to special categories of data, such as data on racial or ethnic origin, political opinions, religious or philosophical beliefs. Special categories of data may only be processed if the data has already been made public or in order to protect the vital interests of the data subject. Moreover, to the extent special categories of data are processed, such activities must be enshrined by Union or domestic law, strictly necessary and subject to appropriate safeguards.

*(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (accuracy and necessity);*

It must be understood that the accuracy and necessity criteria relates closely to the data subject's rights. When a controller transmits personal data, including to third countries and international organizations, it must be able to inform the data subject of the purpose of the processing as well as the categories of recipients that received the personal data as set out by Article 13. Moreover, Article 7 imposes specific requirement that the controller must notify the recipient "without delay" if it emerges that inaccurate personal data has been transferred or if data has been transmitted unlawfully. The data must either be erased, rectified or subject only to restricted processing and the data subject must be notified of the measure.<sup>89</sup> However, the Directive retracts the rights to information, access, rectification and erasure from regional harmonization in the course of a criminal investigation and court proceedings in criminal matters. Recitals 49 and 107 place this processing instead within the domain of rules on national criminal procedure.

*(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed;*

Pursuant to Article 5, the Member States must adopt "appropriate time limits" for the erasure or review of personal data and those limits must be enforced through procedural measures. According to Article 9(3), the controller can set conditions for recipients of personal data. In that way a controller may choose to enforce the time limits in the context of transmissions of data as well.

*(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (data security).*

The obligation to ensure data security entails data protection by design and by default. "Appropriate security" entails *technical* as well as *organizational measures*.<sup>90</sup> Technical measures can encompass solutions such as pseudonymization whereas organizational measures may cover minimization procedures and implementing the data protection principles in the design of a system.<sup>91</sup> In particular, the Directive seeks to ensure through Article 20 that "personal data are not made accessible without the individual's intervention to an indefinite number of natural persons" by default. It must be noted that it is incumbent on both controllers and processors to implement appropriate measures for data security.<sup>92</sup> The appropriateness of the measures are determined in view of the likelihood and severity of risk

<sup>88</sup> See Article 9(3), Directive (EU) 2016/680

<sup>89</sup> See also Article 16(6), Directive (EU) 2016/680

<sup>90</sup> See Article 19 and 20, Directive (EU) 2016/680

<sup>91</sup> See Articles 20 and 29, Directive (EU) 2016/680

<sup>92</sup> See Article 29, Directive (EU) 2016/680



to individual rights in freedoms in relation to the state of the art and the implementation costs of security measures.<sup>93</sup> For automated personal data, the Directive proposes that controllers and processors must take several measures to ensure security:

- (a) deny unauthorised persons access to processing equipment used for processing ('equipment access control');*
- (b) prevent the unauthorised reading, copying, modification or removal of data media ('data media control');*
- (c) prevent the unauthorised input of personal data and the unauthorised inspection, modification or deletion of stored personal data ('storage control');*
- (d) prevent the use of automated processing systems by unauthorised persons using data communication equipment ('user control');*
- (e) ensure that persons authorised to use an automated processing system have access only to the personal data covered by their access authorisation ('data access control');*
- (f) ensure that it is possible to verify and establish the bodies to which personal data have been or may be transmitted or made available using data communication equipment ('communication control');*
- (g) ensure that it is subsequently possible to verify and establish which personal data have been input into automated processing systems and when and by whom the personal data were input ('input control');*
- (h) prevent the unauthorised reading, copying, modification or deletion of personal data during transfers of personal data or during transportation of data media ('transport control');*
- (i) ensure that installed systems may, in the case of interruption, be restored ('recovery');*
- (j) ensure that the functions of the system perform, that the appearance of faults in the functions is reported ('reliability') and that stored personal data cannot be corrupted by means of a malfunctioning of the system ('integrity').*

Article 20 further determines that the controller must take into account measures for ensuring the security of the data already at a preparatory stage when it is determine the means of processing, as well as throughout the processing itself.

### 3.6.3.5 Rights of the Data Subject

The Police and Criminal Authorities Directive has also introduced several important updates to the rights of the data subject. While there is no dedicated definition for data subject under the Directive, the definition of *personal data* (Article 3) resolves that it is an identified or identifiable natural person to which the personal data relates. The rights of the data subject were initially enshrined outside the scope of processing by police and criminal authorities by the Data Protection Directive. They are comprised of a subset of auxiliary rights which assure that data subjects can stay informed of processing of personal data that concerns them and to make their views known on the completeness and accuracy of that data. Council

---

<sup>93</sup> See Article 20, Directive (EU) 2016/680; 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 [first reading] - Political agreement (2012/0010 (COD))



Framework Decision 2008/977/JHA initially reaffirmed the rights of the data subject, in the context of criminal proceedings. It codified three rights; i) the right to be informed, ii) the right of access, and iii) the rights to rectification, erasure or blocking. The Police and Criminal Authorities Directive develops the contents of most of these rights, while also introducing some modifications and additions. The Directive also transposes the GDPR's obligation to communicate personal data breaches to the data subject onto data for criminal investigations and proceedings. The Directive substantially enhances the subject's possibility to exercise these rights by introducing opportunities for independent review. Pursuant to the requirements of Article 17, data subjects will not only be able to exercise their rights directly towards the controller, but also through the Supervisory Authority, and will have the possibility of seeking judicial remedy to secure their rights. However, it must be understood that the extent to which these rights apply to criminal investigations and procedures are determined by national law.<sup>94</sup>

i) The right to be informed

The right to be informed is a right which the data subject must proactively seek by submitting a *request*.<sup>95</sup> The Directive harmonizes a duty for controllers to take "reasonable steps" to provide information to the data subject. The information must be provided in "concise, intelligible and easily accessible form, using clear and plain language". It must be observed that controllers must generally be able to provide information on, inter alia:

- the contact details to the controller and data protection officer,
- the purposes, legal basis and duration of processing,
- the right to rectification, erasure and restriction,
- the right to lodge a complaint with the Supervisory Authority,
- the categories of recipients of the personal data, and
- further information on situations where personal data was collected without the knowledge of the data subject

Request for information may only be subject to charge or refusal if the requests are excessive, repetitive or ill-founded. Furthermore it may only be subject to delay, restriction or omission if such measures are i) provided by law, ii) necessary in a democratic society, iii) are taken with due regard for fundamental rights, and iv) are taken in connection with a legitimate interest. A refusal must always be provided to the data subject without undue delay, and with information regarding the possibility to lodge a complaint with a Supervisory Authority.

ii) The right to access

This can be contrasted with Data Subject's rights in the Council Framework Decision 2008/977/JHA and the Data Protection Directive, prior to the adoption of the GDPR, where the right to access had to be guaranteed "without constraint". To that end it was concluded in Deliverable 7.1 that access would have to be assured without restriction or complication. The Police and Criminal Authorities Directive did not reaffirm the same standard of access as its predecessors. However, the Framework Decision merely sought to safeguard that the data subject could be informed of i) whether his personal data has been transmitted, ii) the recipient or categories of recipients. The Directive contributes to the substantive enhancements by harmonizing a wider scope of access to information regarding the processing available to the data subject (see above).

<sup>94</sup> See Article 18, Directive (EU) 2016/680

<sup>95</sup> Article 12, Directive (EU) 2016/680

### iii) The right to rectification, erasure and restriction

The Directive further codifies three additional rights into the domestic law of Member States; rectification, erasure, and restriction. While Council Framework Decision previously harmonized the rights of rectification, erasure and blocking, it gave the Member States full discretion in formulating the conditions and substance of these rights. The Police and Criminal Authorities Directive on the other hand enhances these right by harmonizing the circumstances under which they can be exercised. The right to blocking has also been substituted for a right to restriction.

The right to rectification encompasses two duties for the controllers. Firstly, the controller must rectify inaccurate data without undue delay. The controller must also complete any incomplete personal data, including by means of accepting supplementary statements from the data subject.

The data subject must also be able to have their personal data erased if there are principal concerns about the legality of the processing. Erasure is used in the event of processing that is incompatible with the principles relating to the processing of personal data, it is found to be unlawful, or special categories of data have been processed without appropriate safeguards or under conditions where such processing was not strictly necessary. In essence, erasure is relevant when the legality of processing has not been fulfilled or if the processing was based on consent and the data subject withdraws their consent.

If the personal data fulfills the requirements for erasure but is needed as evidence, the processing can be restricted instead of having the personal data erased. Restriction is also applicable when the accuracy of personal data cannot be established or is contested by the data subject. While the right to restriction has replaced the right to blocking, the two should not be confused. The right to blocking had a wider objective, originally intended to safeguard that personal data processed lawfully, for the limited purposes that it was collected, and accurately.<sup>96</sup>

### iv) Communication of personal data breaches

Article 31 establishes a duty for controllers to inform data subjects of personal data breaches.<sup>97</sup> A personal data breach is the unlawful, unauthorized, or accidental loss alteration, disclosure or access of personal data resulting of a security breach.<sup>98</sup> The Directive seeks to avoid communication fatigue by only requiring the controller to communicate breaches to the data subject that are associated with *high risks* to the rights and freedoms of natural persons. However, the controller has a parallel obligation to notify all personal data breaches with associated *risks* to the Supervisory authority under Article 30. This is a substantially lower threshold, encompassing more extensive reporting of breaches. It is important to note that the Supervisory Authority then has discretion to require the controller to communicate the data breach to the data subject. The information must be delivered/ communicated to the data subject without undue delay and in clear and plain language the following:

*b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;*

*(c) describe the likely consequences of the personal data breach;*

<sup>96</sup> Regulation (EC) No 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data

<sup>97</sup> See also recital 62, Directive (EU) 2016/680

<sup>98</sup> See Article 3, Directive (EU) 2016/680

*(d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.<sup>99</sup>*

The Directive lays down several exceptions for when the controller is not required to inform the data subject of a personal data breach. The controller may, for example, restrict delay or omit communication on the grounds of certain legitimate interests such as public and national security.<sup>100</sup> Moreover, the breach does not have to be communicated if a) the personal data has been rendered unintelligible to unauthorised persons (such as through encryption), b) the high risk to rights and freedoms is no longer likely to materialize, or c) the communication would involve disproportionate effort.

### **3.6.4 The Right to Privacy in Information Sharing**

Article 8 of the European Convention on Human Right (ECHR), codifies a general prohibition against interferences with privacy through respect for his private and family life, home and correspondence. The general prohibition is echoed in Article 7 of the Charter of Fundamental Rights of the European Union. Derogations are allowed under the ECHR, only in connection to certain interests and under conditions defined by the Convention. Privacy is frequently enshrined as a constitutional right.

The European Court of Human Rights (ECtHR) and Court of Justice of the European Union (CJEU) (the European Courts), enforce the Convention and Charter equivalently to the states under their jurisdiction. The case law of the European Courts may relate to information sharing resulting from ECOSSIAN threat detection in two distinct ways. Firstly, there is an established corpus of interpretation from the Courts regarding the specific conditions that must be fulfilled for any *interference (limitation)* under the Charter) with the right to privacy. Secondly, there is a growing corpus of interpretation on additional safeguards relevant to monitoring and sharing information in the context of detecting and preventing serious crime.

#### **3.6.4.1 Interferences with Privacy**

It is established case law that any interference with privacy must be prescribed by law, necessary in democratic society, and serve a certain public interest. Interferences occur by the mere existence of i) laws that mandate or require the collection of personal data,<sup>101</sup> ii) registers containing personal data,<sup>102</sup> or iii) the use of personal data.<sup>103</sup> Resultantly, any incident notification containing personal data pursuant to Article 14 of the NIS Directive or requests for MLA constitutes an interference with the right to privacy. Interferences must have a firm, clear, explicit and foreseeable legal basis and must be proportionate to the legitimate aim pursued, i.e. must “correspond to a pressing social need.” These needs correspond to the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for

<sup>99</sup> See Articles 30 and 31, Directive (EU) 2016/680

<sup>100</sup> See Articles 31(5) and 13(3), Directive (EU) 2016/680

<sup>101</sup> *Klass and others v Germany* 5029/71 [1979-80] ECHR, paragraphs 33 and 47; *Weber & Saravia v Germany* 54934/00 [2006] ECHR, paragraph 78; *C-293/12 - Digital Rights Ireland and Seitlinger and Others* [2014] CJEU, paragraph 34.

<sup>102</sup> *Leander v Sweden* 9248/8 [1987] ECHR, paragraph 48; *Rotaru v Romania* 28341/95 [2000] ECHR, paragraph 46.

<sup>103</sup> *Rotaru*, paragraph 46. See also *Kopp*, paragraph 53 and *Amann v Switzerland* 27798/95 [2000] ECHR, paragraphs 69 and 80.

the protection of the rights and freedoms of others.<sup>104</sup> As previously observed, the regional legal bases for information sharing on cybercrime are situated within Title V TFEU and the prevention of crime, or Article 308 TEU concerning the operation of the common market and thus economic wellbeing of Member States. While states may choose to echo these provisions in domestic law, they can also enact domestic regulation with a basis in national security and public safety.

#### **3.6.4.2 Interferences for Detecting & Preventing Crime**

Additional interpretations of the principles contained in the right to privacy have also been made in the context of interferences for the detection and prevention of serious crime. These interpretations mainly concern i) national authorities with a law enforcement function, as well as ii) bodies lacking law enforcement competence but with legal obligation to conduct generalized monitoring electronic communications and provide access to LEAs at request. It should be noted that these interpretations are relevant to N-SOCs with law enforcement competences relying on ECOSSIAN or ECOSSIAN-like architectures. It must further be taken into account that there is an absence of case law on NIS threat detection and collaboration between NIS and LEA communities. However, direction can be sought in this regard from case law on law enforcement access to data retained by network operators and service providers. While the interpretations of the European Courts can be of guidance in this latter regard, it must be noted that they have been generated in a technical and legal context that is substantively different from the one faced by operators and authorities encompassed by the NIS Directive, especially with respect to the scope of interference.

#### **3.6.4.3 Safeguards in Access to Data for Crime Detection & Prevention**

Safeguards relevant to the detection and prevention of crime apply to all interferences where the use of collected data is likely to give rise to criminal prosecutions through LEA access. Two especially noteworthy cases, *Digital Rights Ireland* and *Tele2 Sverige*, have laid down conditions for LEA access to that effect. In the *Digital Rights Ireland Case*, the CJEU applied several notable safeguards despite the fact that generalized monitoring pursuant to the Data Retention Directive<sup>105</sup> did not require a threat to public security nor personalized or targeted monitoring on the basis of suspicion, but rather sought to contribute to the fight against serious crime.<sup>106</sup> Advocate General Saugmandsgaard Øe later reaffirmed these safeguards in *Tele2 Sverige*, another case on LEA access to generalized data retention, holding all of them to be mandatory. In the absence of direct interpretations on LEA access to incident data, *Digital Rights Ireland* and *Tele2 Sverige* are valuable guidance where ECOSSIAN can seek direction on conditions for LEA access. Five conditions for LEA access to data can be condensed from the two case:

1. Access to data must be strictly restricted to the purpose of preventing and detecting serious crime (purpose limitation);
2. Access must be subject to prior judicial review or review by an independent administrative body capable of assuring the purpose limitation of access (authorization),

---

<sup>104</sup> Article 8, European Convention on Human Rights

<sup>105</sup> Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC

<sup>106</sup> Paras 68 -60, Directive 2006/24/EC

3. There must be effective protection of the data retained against the risk of abuse (effective guarantees),
4. There must be effective protection against any unlawful access by means of technical and organizational measures and rules which govern the protection and security of the data (data security),
5. Access must not be granted to entities outside of the European Union.

#### 3.6.4.4 Effective Guarantees against Abuse

Bodies with competence to monitor personal data as part of a law enforcement mandate must be subjected to *independent, adequate and effective* oversight.<sup>107</sup> In the *Klass Case*, the ECHR found that “whatever system of surveillance is adopted, there exist adequate and effective guarantees against abuse”.<sup>108</sup> The adequacy and effectiveness of guarantees has thus become a recurrent theme the European case law.<sup>109</sup> Substantively, this entails requirements such as:

- prior judicial oversight through judicial authorization to collect data<sup>110</sup> or procedures establishing “adequate and equivalent guarantees”,<sup>111</sup>
- ex-post and continual oversight such as through parliamentary committees or independent review bodies,<sup>112</sup> and
- ex-post judicial oversight capable of ensuring the right to legal remedy through adversarial proceedings in cases of abuse.<sup>113</sup>

The additional safeguards of oversight are also of relevance in the context of information sharing and simultaneous monitoring between national authorities for the detection and prevention of crime. In the *Weber and Saravia Case*, the Court held that the German Federal Intelligence Services’ transmissions of personal data resulting from monitoring to the Federal Government must be provisional to sufficient safeguards for the necessity of the transmission and its future use.<sup>114</sup> The *Uzun Case* further speaks to the multitude of “uncoordinated investigation measures taken by different authorities” against an individual. In that respect it finds that there must be sufficient safeguards in place “to prevent a person's total surveillance, including the principle of proportionality”.<sup>115</sup> Conclusively, the extent to which any information sharing of data resulting from monitoring complies with the right to privacy is dependent on the existence of effective guarantees.

<sup>107</sup> Sarah Eskens, Ot van Daalen, and Nico van Eijk. (2015). *Ten standards for oversight and transparency of national intelligence services*. Available: <https://www.ivir.nl/publicaties/download/1591.pdf>. Last accessed 04/05/2017.

<sup>108</sup> *Klass*, paragraph 50

<sup>109</sup> *Leander*, § 60; *L. v. Norway*, § 2; *Weber and Saravia*, § 106; *Kennedy v United Kingdom* 26839/05 [2010] ECHR, § 153;

<sup>110</sup> *Klass*, paragraph 56

<sup>111</sup> See *Klass* paragraph 55; *Weber and Saravia*, paragraphs 116 and 117

<sup>112</sup> *Leander*, paragraph 65-67; *Segerstedt-Wiberg and Others v. Sweden* 62332/00 [2006] ECHR, paragraphs 63 and 64.

<sup>113</sup> *Segerstedt-Wiberg and Others*, paragraphs 63 and 64; *Dumitru Popescu v Romania* 49234/99 [2007] ECHR, paragraph 74, 76, and 77; *Ekimdzhiiev v. Bulgaria* 22373/04 [2012] ECHR, paragraph 123.

<sup>114</sup> *Weber and Saravia*, paragraphs 121 and 122.

<sup>115</sup> *Uzun v Turkey* 10755/13 [2013] ECHR, paragraph 73.



In view of this case law, several recommendations are made for ECOSSIAN and the use of ECOSSIAN-like systems. Firstly, any O-SOC or N-SOC without law enforcement competence that receives a request to disclose personal data should assume that such a request must be supported by a warrant until the requesting authority has proven otherwise with support of domestic law. It should be known however, that many jurisdictions allow criminal authorities to compel access to certain data without a warrant as an urgent measure.<sup>116</sup> Secondly, entities lacking law enforcement competence should not voluntarily share personal data at their own accord with law enforcement. If there is suspicion that a crime has occurred, the entity may report evidence not constituting personal data to law enforcement. The law enforcement authority can then request a warrant to be issued for the personal data and any remaining evidence. Thirdly, it must also be understood whether LEA direct access is premised on certain oversight conditions. If N-SOCs or E-SOCs with law enforcement competence have direct access to the ECOSSIAN system, an oversight authority or supervisory authority may also have to have the ability to review that access to the system. Entities with law enforcement authority should resultantly consult their oversight bodies on the ex-post review requirements resulting of direct access.

### 3.6.4.5 Scope of Interference

The scope or degree of interference caused by NIS threat detection has not been assessed by the European Courts. This brings into the question, safeguards that ought to apply to data collected through those processes. It must be noted that the European Courts' approach, which assesses the conditions for derogation from a right, relies on subjective necessity and proportionality tests. These tests query, whether an interference used the least intrusive means and whether the means correspond to a "pressing social need".<sup>117</sup> This frequently leads the European Courts into complex reasoning about the characteristics of the personal data collected and how safeguards apply in relation to that interference.<sup>118</sup> With that in mind, the ECtHR Research Division concluded:

*It is worth noting that in the case of Uzun v. Germany, the Court considered that GPS surveillance of movements in public should be distinguished from other methods of visual or acoustic surveillance because they disclosed less information about the conduct, opinions and feelings of the person concerned and therefore interfered less with their private lives. The Court therefore did not consider it necessary to apply the same strict safeguards as it had developed in its case-law with regard to the surveillance of telecommunications, such as the limit on the duration of monitoring or the procedure to be followed for examining, using and storing the data obtained.*<sup>119</sup>

The interpretation of interferences have revolved around various measures of *monitoring*, some of which have comparable technical and legal traits ECOSSIAN's threat detection architecture, but none of which match its actual application and use. In practice, the European Courts use *monitoring* interchangeably with concepts such as *interception*, *surveillance*, and *strategic monitoring*. Of these concepts, only interception has been defined by EU law in Council Resolution 1995 (96/C 329/01) as a statutory-based action whereby network operators and internet service providers provide access and delivery of a subject's

<sup>116</sup> Article 29 Data Protection Working Party (536/14/EN, WP 211) Opinion 01/2014

<sup>117</sup> Korff, D. (2008). *THE STANDARD APPROACH UNDER ARTICLES 8 – 11 ECHR AND ARTICLE 2 ECHR*. Available: [http://ec.europa.eu/justice/news/events/conference\\_dp\\_2009/presentations\\_speeches/KORFF\\_Douwe\\_a.pdf](http://ec.europa.eu/justice/news/events/conference_dp_2009/presentations_speeches/KORFF_Douwe_a.pdf). Last accessed 04/11/2016. 3

<sup>118</sup> *Uzun*

<sup>119</sup> See *Leander*, paragraph 59



telecommunications and call associated data to law enforcement agencies. It is impossible to predict with exact accuracy the gravity of any interference in view of the case law or the adequacy of existing safeguards. It is therefore prudent to apply equivalent levels of protection as those prescribed by the European Courts in cases of monitoring generally.

Req. number	Description	Importance* (M/O)	Relevant for Level			Comment
			O-SOC	N-SOC	E-SOC	
GReq.	The legal status of the entity wishing to share information needs to be established in order to decipher the specific legal considerations relevant.	M	X	X	X	
GReq.	Suspected crimes should be reported as appropriate under domestic criminal law and criminal procedural law	M	X	X		
GReq	Personal data should only be shared with law enforcement pursuant to an order or warrant.	O	X			

\*M – mandatory; O – optional

\*\* Work Packages where this requirement should be implemented

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

### 3.7 ICT specific legal frameworks

#### 3.7.1 Breach notification obligations

D7.3 gave an introduction to notification obligations, focusing on the notification obligations for communication networks. In order to derive an overview on different existing notification obligations and the legal development of these in the last years, further research has been made. As explained in D7.3, obligations to notify were first introduced in the telecommunications sector where Directive 2009/140/EC amended the Framework Directive by introducing art. 13a and 13b containing amongst others the obligation, in case of a “*breach of security or loss of integrity that has had a significant impact on the operation of networks or services*”, to notify the competent national regulatory authority. The competent regulatory authority then could, if necessary, inform national regulatory authorities in other Member States and ENISA, and had the possibility to inform the public if it would be in the public interest. Furthermore, information is collected and exchanged in summary reports resulting in a single public report compiled by ENISA including analyses and recommendations and anonymised national reports available to the national authorities.

National reports are also shared voluntarily with operators who agree to provide information about their own incidents<sup>120</sup>.

As a directive, the provisions need to be implemented in the national legislation, generally the Member States included the provision in their national telecommunications legislation (e.g. Germany: §109 (5) German Telecommunications Act, the Netherlands: Art. 11a2 Telecommunicatiewet (Dutch Telecommunications Act) and Belgium: art. 114 Belgian Electronic Communications Act). The national legislation is often further specified by secondary legislation on different levels, e.g. in the Netherlands 'Besluit continuïteit openbare elektronische communicatienetwerken en –diensten'. Often of influence in this regard were the recommendations of ENISA. As an example, in Belgium in Article 114/1, §2 Electronic Communications Act it was provided that *"The undertakings providing public communications networks or publicly available electronic communications services shall immediately notify the Institute of a breach of security or loss of integrity that has had a significant impact on the operation of networks or services. Following the prior consent of the Minister, the Institute shall specify in which hypotheses the breach of security or loss of integrity has a significant impact in the sense of this paragraph."* Accordingly, the national regulatory authority BIPT (Belgisch Instituut voor Postdiensten en Telecommunicatie) provided a "Decision of the BIPT council of 1 April 2014 laying down the circumstances in which the operators have to notify BIPT of a security incident and the terms and conditions of this notification". The decision provides the practical rules regarding the notification of security incidents which do not involve personal data and is inspired by the ENISA "Technical Guidelines on Incident Reporting"<sup>121</sup>, also to ensure a coherence between the notifications of the operators to the BIPT and the summary report of the BIPT for ENISA. BIPT defines in its decision the criteria for a breach of security or loss of integrity that has had a significant impact on the operation of networks or services. It bases the criteria on the criteria defined by ENISA, but adjusted on the amount of end users in Belgium, defining six different thresholds, in case of which the incident needs to be notified to BIPT.

According to ENISA, art. 13a and the evaluation brought a certain amount of uniformity and contributed to increasing the resilience and security of the telecommunication infrastructure in Europe<sup>122</sup>.

As it was a success, the notification obligations increasingly were also used for other sectors.

Examples are Article 19 of the new eIDAS Regulation<sup>123</sup> that states almost identical provisions as for telecom providers, for qualified and non-qualified trust service providers, including a notification obligation with a time limit for notification of 24 hours after becoming aware of the incident. Another example is the PSD II Directive<sup>124</sup>, which includes incident reporting obligation for payment service providers [art. 96]. Finally, also the NIS Directive specifies notification obligations for operators of essential services and for digital service

<sup>120</sup> Dan Tofan, Konstantinos Moulinos, and Christoffer Karsberg, "ENISA Impact Evaluation on the Implementation of Article 13a Incident Reporting Scheme within EU," March 18, 2016, 5.

<sup>121</sup> Marnix Dekker, Christoffer Karsberg, Technical guidance on the incident reporting in Article 13a. Version 2.0, January 2013.

<sup>122</sup> Dan Tofan, Konstantinos Moulinos, and Christoffer Karsberg, "ENISA Impact Evaluation on the Implementation of Article 13a Incident Reporting Scheme within EU," March 18, 2016.

<sup>123</sup> Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

<sup>124</sup> Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.

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

On the other hand, there is another type of breach notifications, relating to personal data breach. While the earlier mentioned legislations set obligations with a focus on what type of service is provided, the focus of personal data breach notification is on the type of data. Therefore, the obligation applies to everybody who is controller or processor of personal data, which is a broader audience and can coincide with notification obligations pointed towards specific services, if these services also process personal data. In the earlier mentioned legislation this is often considered by obliging notification also to other relevant bodies and asking for working in close cooperation [e.g. art. 19 eIDAS Regulation, art. 15 (4) NIS Directive].

As explained in D7.3, specific obligations for the telecommunication sector were already introduced in 2009, as another part of the Telecommunications reform package was an amendment of the e-Privacy Directive (Directive 2002/58/EC) amending article 4 of the e-Privacy Directive. This article requires the provider to notify without undue delay the competent national authority in case of a personal data breach, and in certain circumstances the subscriber or individual. In order to ensure consistency in implementation the Commission is empowered to adopt technical implementing measures, which they did with Commission Regulation No 611/2013. It requires that the provider, if possible, must notify the personal data breach to the competent national authority no later than 24 hours after the detection. This can also be only an initial notification, if not all the required information is yet available, and a second notification as soon as possible, at the latest within three days after the initial notification. The Commission Regulation also defines certain circumstances in which cases a personal data breach is likely to adversely affect the personal data of a subscriber or individual : (a) the nature and content of the personal data concerned, in particular where the data concerns financial information, special categories of data, as well as location data, internet log files, web browsing histories, e-mail data, and itemized call lists; (b) the likely consequences of the personal data breach for the subscriber or individual concerned, in particular where the breach could result in identity theft or fraud, physical harm, psychological distress, humiliation or damage to reputation; and (c) the circumstances of the personal data breach, in particular where the data has been stolen or when the provider knows that the data are in the possession of an unauthorized third party.

The Data protection Directive 95/46/EC did not include a specific data breach notification obligation. However, obligations of this kind were often included in national law, or the Data Protection Authorities recommended it, by inferring obligations to notify from other provisions of the Directive. Accordingly, the new General Data Protection Regulation does include a notification obligation in case of a personal data breach in art. 33 GDPR. The controller is required to notify the personal data breach without undue delay and, where feasible, no later than 72 hours after having become aware of it (if the notification is made later, reasons for the delay must be given). In case the processor becomes aware of a personal data breach, he has to notify the controller without undue delay, which then has to notify the supervisory authority. Differently from the other notification obligations, the data protection provision does not focus on the impact of the service, triggering a notification obligation in case a certain threshold is reached. Instead, a breach generally has to be notified with the exception of a personal data breach that is unlikely to result in a risk to the rights and freedoms of natural persons. In case the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller does not only need to inform the supervisory authority but also the data subject without undue delay.

Different from article 13a Frameworks Directive, the data protection authorities are not required to annually report the received notifications to the Commission or ENISA. Article 59 GDPR requires the data protection authorities to draw up an annual report on its activities, which shall be transmitted to different authorities and be made available to the public, the Commission and the Board. The article does not specifically mention that the DPAs should also include the received data breach notifications, however, at least at a general level it could be useful to provide an overview of this information, e.g. to ENISA.

The different Directives have or still need to be implemented at a national level. Sometimes the countries enacted specific legislation. Examples are France and Germany where the French Military Programming Law (LPM) and the German IT Security Act obliges specific operators to report cyber security incidents, implement technical and organizational security measures and undergo cyber security audits.<sup>125</sup>

The following tables provide an overview of the different notification obligations enshrined in EU legislation (Table 3: EU notification legislation) and an overview of four different countries and how notification obligations are included in the national legislation (Table 4: National notification obligations).

Legislation	Who has to notify?	What?	When?	To whom?
<b><u>Art. 13a Directive 2009/140/EC</u></b>	undertakings providing public communications networks or publicly available electronic communications services	a breach of security or loss of integrity that has had a significant impact on the operation of networks or services	<i>[not specified in the Directive]</i>	competent national regulatory authority
<b><u>Art. 19 eIDAS Regulation</u></b>	Qualified and non-qualified trust service providers	any breach of security or loss of integrity that has a significant impact on the trust service provided or on the personal data maintained therein	without undue delay but in any event within 24 hours after having become aware of it	the supervisory body and, where applicable, other relevant bodies, such as the competent national body for information security or the data protection authority,
<b><u>Art. 96 PSD II Directive</u></b>	payment service providers	major operational or security incident	without undue delay <i>[possibly specified in national legislation]</i>	competent authority in the home Member State of the payment service provider
<b><u>Art. 33/34 General Data Protection Regulation</u></b>	Controller	personal data breach that results in a risk for the right and freedom of	without undue delay and, where feasible, not later than 72 hours after having	Competent supervisory authority [in case of high risk for rights

<sup>125</sup> S. Anna, M. Konstantinos, 'Stocktaking, Analysis and Recommendations on the Protection of CII's', January 2016, p.18f.

Legislation	Who has to notify?	What?	When?	To whom?
		individuals	become aware of it	and freedoms of individuals also the data subject]
<b><u>Art. 14 NIS Directive</u></b>	Operators of essential services + digital service providers	incidents having a significant impact on the continuity of the essential service	without undue delay <i>[possibly specified in national legislation]</i>	competent authority/CSIRT appointed by Member State

Table 3: EU notification legislation

	<b><u>Germany</u></b>	<b><u>Netherlands</u></b>	<b><u>Belgium</u></b>	<b><u>Italy</u></b>
<b>Data breach</b>				
<b><u>Legislation</u></b>	<b><u>GDPR =&gt; from 25.5.2018 applicable in all MS</u></b>			
<b>Who has to notify?</b>	Controller			
<b>What?</b>	personal data breach that results in a risk for the right and freedom of individuals			
<b>How?</b>	without undue delay and, where feasible, not later than 72 hours after having become aware of it; notification must include at least: a description the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of data records concerned; the name and contact details of the data protection officer or other contact point where more information can be obtained; the likely consequences of the personal data breach; measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, to mitigate its possible adverse effects.			
<b>to whom?</b>	Competent supervisory authority [in case of high risk for rights and freedoms of individuals also to the data subject]			
<b><u>Legislation (till 25.5.2018)</u></b>	<b>Bundesdatenschutz gesetz § 42a</b>	<b>Meldplicht datalekken'</b> (change in the national data protection law (Wbp) art 34a Wbp)	<b>no general legislation</b> BUT: the Belgian DPA (Belgische Privacy Commissie) gave an <b>advice</b> that they consider an incident notification part of the general security obligations of data controllers	<b>no general legislation</b> BUT: July 2015 the Italian data Protection Authority (DPA) issued <b>provisions for public authorities; add. probably implicit duty</b> for controllers to notify based on fairness principle

	<b><u>Germany</u></b>	<b><u>Netherlands</u></b>	<b><u>Belgium</u></b>	<b><u>Italy</u></b>
<b>Who has to notify?</b>	private bodies and public bodies of the Federation in so far as they participate in competition as public-law enterprises	Controller	Controller	every public Authority
<b>What?</b>	determines that 1. special types of personal data (Section 3 (9)), 2. personal data subject to professional secrecy, 3. personal data related to criminal offences or administrative offences or the suspicion of punishable actions or administrative offences, or 4. personal data concerning bank or credit card accounts stored with that body have been unlawfully transferred or otherwise unlawfully revealed to third parties, with the threat of serious harm to the data subject's rights or legitimate interests	breach of the security of personal data against loss or any form of unlawful processing	openbare incidenten' (public incidents): not explicitly defined; events where personal data has been lost, destroyed, changed or made public in a way that the incident will be revealed by the public	all data breaches or cyber incidents that could have a significant impact on the personal data contained in their databases



	<u><b>Germany</b></u>	<u><b>Netherlands</b></u>	<u><b>Belgium</b></u>	<u><b>Italy</b></u>
<b>How?</b>	Without delay', The data subject shall be notified as soon as appropriate measures have been taken to protect the data and notification would no longer put criminal prosecution at risk. The notification for the data subjects shall describe the nature of the unlawful access and include recommendations for measures to minimize possible harm. The notification for the competent supervisory authority shall also describe possible harmful consequences of the unlawful access and measures taken by the body.	without delay', needs to include the nature of the unlawful access, the bodies where more information can be received, the recommended measures to limit the negative results of the unlawful access, the established and assumed consequences on the processing of personal data and the measures that the controller has taken or proposes to remediate the consequences	within 48 hours after becoming aware of the incident	48 hours from the knowledge of the fact (data breach); for that notification DPA has developed a standard template that prompts you to indicate, inter alia: a) the identity of the data controller and of the persons in charge of the duty of notification; b) brief description of the kind of violation; c) when and how (merely reading of the data; copy of the data; erasing of the data and so on) there has been a violation; d) number of people affected; kind of data affected (identification data; sensitive data; judicial data and so on)
<b>to whom?</b>	the responsible supervisory authority and the data subject	Autoriteit Persoonsgegevens (Dutch DPA) and the data subject if the incident will probably have negative effects on the private sphere of the data subject	Belgische Privacy Commissie (Belgian DPA)	Italian DPA
<b>CIS ICT incidents</b>				
	<b>NIS Directive</b>			
<b>Who has to notify?</b>	Operators of essential services + digital service providers			
<b>What?</b>	incidents having a significant impact on the continuity of the essential service (significant impact: e.g. number of users affected by the incident, duration, geographical spread, extent of the disruption, extent of the impact on economic and societal activities)			
<b>How?</b>	without undue delay'; notification shall include information to enable the competent authority or the CSIRT to determine any cross-border impacts of the incident			
<b>to whom?</b>	competent authority/CSIRT appointed by Member State			

	<u><b>Germany</b></u>	<u><b>Netherlands</b></u>	<u><b>Belgium</b></u>	<u><b>Italy</b></u>
<b>Current national Legislation</b>	Gesetz zur Erhöhung der Sicherheit Informationstechnischer Systeme (IT SicherheitsGesetz) Artikelgesetz: mainly changes BSI-Gesetz (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik); § 8b Abs. 4 BSI-Getz	<i>currently no legislation, but draft legislation: 'Regels over het verwerken van gegevens ter bevordering van de veiligheid en de integriteit van elektronische informatiesystemen die van vitaal belang zijn voor de Nederlandse samenleving en regels over het melden van ernstige inbreuken (Wet gegevensverwerking en meldplicht cybersecurity)'</i>	currently no legislation	Italian DPCM 17th February 2017, art. 11
<b>Who has to notify?</b>	Operators of Critical Infrastructure (private)	<i>operators of Critical Infrastructure (private and public)</i>	/	CI private operators
<b>What?</b>	serious disturbances of the availability, integrity, authenticity and confidentiality of their IT systems, components or processes, which could lead to a failure or impairment of the functioning of the Critical Infrastructure	<i>breach of security or loss of integrity of the IT system which can or does to a great extent cause interruption of the availability or reliability of a product or service</i>	/	any significant security breach
<b>How?</b>	Notification needs to include information on the incident, the technical surrounding conditions, especially the suspected or identified cause, the affected IT systems, the type of the affected system or facility and the industrial sector of the operator	<i>immediately (onverwijld); needs to include: the type and scale of the breach or loss, the suspected start of the incident, possible consequences, a forecast of the repair time, if possible also the measures taken by the CI to limit the consequences of the incident and avoid it in future, the contact information of the person responsible</i>	/	using secure transmission channels

	<u><b>Germany</b></u>	<u><b>Netherlands</b></u>	<u><b>Belgium</b></u>	<u><b>Italy</b></u>
		<i>for the notification</i>		
	Information can be given anonymously/pseudonymously if the incident did not result in a failure or disturbance of the Critical Infrastructure. Otherwise it is required that the operator is named	<i>Information of the person responsible for the notification</i>	/	shall collaborate in the management of cybercrime and shall helping to restore the functionality of systems and networks managed by them
<b>to whom?</b>	BSI	<i>Ministry of Security and Justice (more specific: the NCSC)</i>	/	NSC
<b>Telecom breach notification (country information based on ENISA Article 13a State of Play 2015)</b>				
<b>Legislation</b>	German telecommunications act (§109 (5))	Art. 11a2 Dutch Telecommunications Act + secondary legislation (Besluit Continuïteit)	art. 114 Belgian Electronic Communications Act	<i>2015: proposal</i>
<b>Who has to notify?</b>	Any person operating a public telecommunications network or providing publicly available telecommunications services	undertakings providing public communications networks and/or services	Operators	<i>Telcos</i>
<b>What?</b>	security breach, including disorders of telecommunications networks or services, having a significant impact on the operation of telecommunication networks or the provision of telecommunication services	breaches of security and integrity of networks and services, if they had 'significant impact' on operation of networks or services; no threshold, uses ENISA ("Technical Guideline on Incident Reporting")	Breach of security or loss of integrity which has a significant impact. Significant impact: Decision of BIPT, on 1st April 2014	<i>incidents having a significant impact; significant = over a defined threshold which is the same as defined in the dedicated technical guideline developed by the working group established by ENISA</i>

	<u><b>Germany</b></u>	<u><b>Netherlands</b></u>	<u><b>Belgium</b></u>	<u><b>Italy</b></u>
		as an indication. Significance is estimated by the undertaking.		
<b>How?</b>	The Agency may require a detailed report on the security breach and the remedial action taken	at once via a designated telephone line and a secure web portal (www.meldplichttel.ecomwet.nl), available 24/7. Additional information collected by e-mail and telephone		<i>a brief report within three days. Detailed report within 15 days</i>
<b>to whom?</b>	Bundesnetzagentur (Federal Network Agency)	Radiocommunications Agency Netherlands (RAN)	Belgian Institute for Postal Services and Telecommunications (BIPT)	<i>Ministry for economic development</i>
<b>eIDAS Regulation (art. 19)</b>				
<b>Who?</b>	'trust service' means an electronic service normally provided for remuneration which consists of: <ul style="list-style-type: none"> <li>· the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or</li> <li>· the creation, verification and validation of certificates for website authentication; or</li> <li>· the preservation of electronic signatures, seals or certificates related to those services</li> </ul>			
<b>What?</b>	any breach of security or loss of integrity that has a significant impact on the trust service provided or on the personal data maintained therein.  Thresholds for trust service providers to notify (i.e. what is significant) the national supervisory bodies depend on national circumstances: different countries will adopt a different approach to setting national reporting thresholds, depending on national details, including: the type of providers in the sector, the population of the country, national legislation, etc. The objective of this document is to agree upon indicators and thresholds <sup>13</sup> which can be used as a basis for the annual summary reports submitted by the supervisory bodies to ENISA and the European Commission; they can also be used as guidance to supervisory bodies when setting national thresholds.			
<b>When?</b>	Without undue delay but in any event within 24 hours after having become aware of it			
<b>To Whom?</b>	The supervisory body and, where applicable, other relevant bodies, such as the competent national body for information security or the data protection authority			

Table 4: National notification obligations

Req. number	Description	Importance* (M/O)	Relevant for Level			Comment
			O-SOC	N-SOC	E-SOC	
GReq. 3.1	National legislation on the requirements in relation to breach notification must be consulted.	M	X	X	X	i.e. the disparity between Germany and other Member States and also Ireland and the UK that have adopted codes of conduct should be assessed.
GReq.3.2	Developments in relation to proposed amendments should be consulted following the adoption of legislation.	M	X	X	X	

\*M – mandatory; O – optional

\*\* Work Packages where this requirement should be implemented

Table 5: ICT specific frameworks requirements

Also GReq 3.1 and 3.2 will stay applicable for an organisational implementation of the ECOSSIAN system. As shown in this section, the European and national legislation has changed in the last years considerably and will likely still change in the future. The increased amount of notification obligations for different sectors could be an incentive for increased information sharing. At the same time it would be beneficial if the received information from the notification obligation could be connected (e.g. currently different sectorial entities receive the notifications) and be used for increased NIS security, which is an aim of the ECOSSIAN system. However, the obligations should not deter CI operators from voluntarily sharing information.

## Chapter 4 Legal barriers to information sharing

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

### 4.1 Data protection requirements

The requirements regarding collection and sharing of personal data have been extensively explained in D7.1, D7.2, D7.3 and D7.6. Therefore, this part will only provide a general overview, focusing on the GDPR and information sharing requirements provided by the Regulation, including implications of recent case law. A full analysis of the requirements provided in D7.2 and D7.3 can be found in D7.6.

As specified in D7.3, the different national data protection legislation could provide a hurdle for information sharing. For example, the participants of ENISA interviews for a 2013 report on information exchange among CERTs indicated doubts on whether particular sets of data can be shared and with whom, mainly due to the lack from harmonization of data protection law across the EU and the different interpretations of the law by different bodies.<sup>126</sup>

The issue of different legislation will from 2018 be resolved, since after long negotiations on 24 May 2016 the European General Data Protection Regulation (GDPR) entered into force, which will start to apply from 25 May 2018. Different than the previous Data Protection Directive 95/46/EC, the GDPR as a Regulation will apply directly and does not need to be transposed in national law. Therefore, the GDPR constitutes a single set of rules for all Member States, which regulates the processing of personal data, if it is done in the context of an establishment of an actor (controller/processor) within the EU, or if personal data of people who are in the EU is processed in the context of offering goods or services or the monitoring of their behavior. The Regulation is not applicable in certain cases, therefore for example defense as an activity concerning national security would generally not fall under the Regulation and Law Enforcement does also not fall under the Regulation but is regulated in national legislation, harmonized by Directive 2016/680/EU.<sup>127</sup>

In case of information exchanges between different private and/or possibly public parties outside a defense or law enforcement context, and in case personal data will be exchanged, usually the GDPR will apply.

---

<sup>126</sup> R. Bourgue, J. Budd, H. Homola, M. Wladdenko, D. Kulawik, Detect, SHARE, Protect – Solutions for Improving Threat Data Exchange among CERTs, October 2013, p.8.

<sup>127</sup> Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA



#### d. Personal data

In order to assess whether data protection legislation is applicable, it needs to be assessed whether personal data is processed. Personal data according to the GDPR is any information relating to an 'identified or identifiable natural person'. 'Identifiable' means a person who can be directly or indirectly be identified, for example by a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. To assess whether a person is identifiable all the likely means for identifying the person that could be used either by the controller or by another person need to be taken into account.

A special position which resulted in a legal hurdle for information sharing was the status of IP addresses, which in some countries were considered personal data while in other countries not.<sup>128</sup> In 2016 the Court of Justice of the European Union (CJEU) decided a case regarding the status of dynamic IP addresses which provided a certain clarification in this question. This case is commonly referred to as the Breyer case<sup>129</sup>. The background was that the Federal Republic of Germany operates websites and in that capacity records the IP addresses of visitors to its websites. Patrick Breyer wanted the Federal Republic of Germany to cease retaining IP addresses when it is not technically necessary to keep them. The case ended up in front of the German Federal Court of Justice, the Bundesgerichtshof (BGH). On 28 October 2014 the German Federal Court (Bundesgerichtshof) decided to refer questions to the Court of Justice of the European Union (CJEU).

The first question related to whether the classification of IP addresses as personal data extends to dynamic IP addresses in situations where the website operator who processes the IP addresses does not have the identifying information necessary to link them to individual users. In such cases, the identifying information is instead held by a third party (i.e. the ISP) and is therefore beyond the reach of the website operator without direct cooperation between the parties. The second question asked whether §15 of the German Telemedia Act, which restricted collection and use of personal data by an online media service provider to the information that is necessary to facilitate and charge for the use of those services, is legitimate in light of Directive 95/46/EC and hence whether the grounds for processing contained in Article 7(f) DPD can be relied upon for the collection of IP addresses in order to ensure the functionality of a website.

Regarding the first question, the CJEU considered that the possibility to combine a dynamic IP address with the additional data held by the internet service provider could constitute a means likely reasonably to be used to identify the data subject as in the case of Germany legal channels exist to obtain the information. The Advocate General in his opinion had pointed out that a dynamic IP address would not be considered personal data if the identification of the data subject was prohibited by law or practically impossible due to the required disproportionate effort in time, cost and man-power, resulting in an insignificant risk of identification.

Regarding the second question the court decided that the German § 15 Telemedia Act was too restrictive, as it excludes the objective to ensure the general operability of the service as a possible justification.

---

<sup>128</sup> also mentioned as a point of concern for information sharing between CERTs in R. Bourgue, J. Budd, H. Homola, M. Wladenko, D. Kulawik, Detect, SHARE, Protect – Solutions for Improving Threat Data Exchange among CERTs, October 2013, p.8.

<sup>129</sup> CJEU Judgement Case C-582/14 19 October 2016 (Breyer).

This means that, considering that ISPs keep a record of the persons account to whom a dynamic IP address has been given, and there generally exist legal means to access the information, IP addresses are considered personal data.<sup>130</sup> The reasoning of the Court regarding likely reasonable means can also be applied regarding other information than dynamic IP addresses. Therefore, for example MAC addresses could be considered personal data in the same way if a register exists which links them to a natural person and this register is accessible by legal or other reasonable means.

e. Legal ground for processing

When personal data is processed, data protection legislation needs to be taken into account. Processing means any operation performed on personal data, including collection, recording, structuring, storage, consultation, disclosure by transmission or otherwise making available.

The entity that determines the purposes and means of the processing of personal data is the controller.<sup>131</sup> The controller is responsible for compliance with the data protection legislation.

Processing of personal data is only allowed if either the data subject has given consent, or there are other good grounds that make the data processing lawful, as specified in art. 6 GDPR. These can be amongst others: that the processing is necessary for compliance with a legal obligation that the controller must adhere to, that it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, or that the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party (more information in D7.6).

f. Collection of the data:

The GDPR clarifies that the processing of personal data which is necessary to ensure network and information security by public authorities, by computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), by providers of electronic communications networks and services and by providers of security technologies and services constitutes a legitimate interest of the controller (recital 49 GDPR).<sup>132</sup> However, there are some limitations to using the legitimate interest of the controller as a reason for processing: First, the general limitation of art. 6 (f) is that there must not be more important interests or fundamental rights and freedoms of the data subject which override the interest of the controller. Second, the processing of the personal data must be strictly necessary and proportionate for the purpose of ensuring network and information security. This includes that not generally information can be collected and shared to see whether it could be useful to e.g. detect an attack, but it needs to be beforehand assessed how the security should be ensured and which data exactly is necessary for this aim. Furthermore, the data subject has at any time the right to object to the processing based upon the legitimate interest of the controller. In this case the processing must be stopped, except if the controller demonstrates

<sup>130</sup> Article 29 Working Party, Opinion 4/2007 on the concept of personal data, WP 136, 20 June 2007.; WP 37: Privacy on the Internet - An integrated EU Approach to On-line Data Protection- adopted on 21.11.2000. ; CJEU Judgement Case C-582/14 19 October 2016 (Breyer).

<sup>131</sup> art. 4 (7) GDPR.

<sup>132</sup> Network and information security is considered “i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), by providers of electronic communications networks and services and by providers of security technologies and services”. Recital 49 GDPR.

compelling legitimate grounds for the processing that override the interests, rights and freedoms of the data subject, or is necessary for legal claims.<sup>133</sup> This includes that e.g. a normal employee or customer whose data is shared can object to the processing, however, an attacker cannot use data protection law to object to the processing of his personal data. Overall, it implies that an assessment must be done for different processing operations, and the result of the assessment can vary, depending on the incident.

Furthermore, it has to be considered that while the operator, who will generally be the controller<sup>134</sup> in case of the collection of NIS information of its own system, can use the legitimate interest of the controller as a legal ground, however, public entities cannot use article 6 (1) (f) GDPR if the processing is carried out in performance of their task. In such a case other legal grounds are needed, such as for example that the processing is necessary for either the compliance with a legal obligation (art. 6 1 (c) GDPR) or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (art. 6 1 (e) GDPR). For processing based on a legal obligation or performance of a task in the public interest, the Member States may maintain or introduce more specific provisions by determining specific requirements for the processing. The basis for the processing must be laid down by Union or Member State law to which the controller is subject and the law shall meet an objective of public interest and be proportionate to the legitimate aim pursued. The legal basis should determine the purpose of the processing, or the purpose must be necessary for the performance of the task. It should be assessed whether new legislation based upon the NIS Directive could provide for this.

A peculiar issue is that recital 49, as earlier mentioned, provides that the processing of personal data for network and information security constitutes a legitimate interest of the data controller, explicitly also mentioning public authorities, while these, as explained are not allowed to rely upon the legitimate interest of the data controller. It will depend on whether the processing for network and information security lies within the task of the public authority. In case it is within the task, it is not possible to rely on article 6 (1) (f) GDPR. In case the network and information security measure is not within the scope of the task of the public authority, it might be possible for the public authority to rely upon the legal interest of the controller. The type of network and information system security measure and the reason for enacting it can provide clues in this regard. While it might be debatable whether a public authority should provide a website if it is not in the scope of its task and whether retaining IP addresses is the right security measure, it is reasonable that public authorities can for example rely upon the legal interest of the controller to keep their internal computer systems secure and process different types of data in order to do this (of course making the balancing exercise of article 6 (1) (f) GDPR). Accordingly, in case of a public N-SOC, specific legislation will need to define the data processing task and capabilities of the N-SOC.

#### g. Transfer of information

In general is it important for a transfer of personal data whether the recipient is located within the European Union or in a third country/international organization. In case the recipient is located outside the European Union, stricter requirements apply and the transfer is only possible if the protection of the data is ensured<sup>135</sup>. In case the recipient is located within the

---

<sup>133</sup> art. 21 GDPR.

<sup>134</sup> The one who determines the purposes and means of the processing of personal data (Art. 4 (7) GDPR) and who is responsible to comply with the data protection obligations.

<sup>135</sup> e.g. if the Commission gave an adequacy decision for the third country or if the transfer is subject to appropriate safeguards, for example in the form of binding corporate rules, standard data protection clauses or an approved certification mechanism.

European Union, the data protection legislation applies directly to the recipient. The GDPR specifically aims at facilitating the ‘free flow of personal data’ in the EU. The question is then which status under data protection legislation the recipient has. In case the recipient only received and processes the data for the original controller (e.g. the controller instructed the recipient to make an analysis of the data, but the results are for the controller and the recipient will not use the data on its own behalf), the recipient will be considered a processor. In this case, the controller and processor should have a controller-processor contract as defined in the GDPR. In case the recipient of the data will use the data (also) on its own behalf, the recipient will be considered as a controller of the data. The controllers could then be joint controllers or separate controllers. Joint control arises “when different parties determine with regard to specific processing operations either the purpose or those essential elements of the means which characterize a controller.”<sup>136</sup> On the other hand sharing of data between two controllers without sharing purposes or means in a common set of operations is considered only as transfer of data between separate controllers.<sup>137</sup>

It should be noted that the assessment of the status is based upon a factual assessment, depending on who determines the purposes and means, contractual arrangements can only provide an indication and always need to be checked against the factual circumstances.<sup>138</sup> Therefore, it depends on how the information sharing takes place, and whether or not the information sharing can be considered one “set of operations” with a joint purpose or jointly defined means, in order to assess the status of the participants.<sup>139</sup>

Establishing who is controller is important since the controller is the one responsible for the personal data. In case the recipient is a processor, the processing will be done under the original legal ground for processing. In case the recipient is a separate controller, it needs to be ensured that the processing is still lawful and that a legal ground for processing applies.

In case the personal data have originally been collected for another purpose than network and information security, and the further processing is not based on the consent of the data subject or a specific law, it needs to be assessed whether the processing for NIS is compatible with the purpose for which the personal data originally was collected.<sup>140</sup> For that, any link between the original purpose and the new purpose, the context in which the data was originally collected and the nature of the personal data should be considered. This is especially important in case of special categories of data (data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation) and data related to criminal convictions and offences. Finally, for an assessment the possible consequences of the intended further processing for data subjects and the existence of appropriate safeguards (including encryption and pseudonymisation) need to be taken into account.

<sup>136</sup> Article 29 Working Party, Opinion 1/2010 on the concepts of “controller” and “processor”, 00264/10/EN WP 169, 16 February 2010, p.18.

<sup>137</sup> Article 29 Working Party, Opinion 1/2010 on the concepts of “controller” and “processor”, 00264/10/EN WP 169, 16 February 2010.

<sup>138</sup> Article 29 Working Party, Opinion 1/2010 on the concepts of “controller” and “processor”, 00264/10/EN WP 169, 16 February 2010.

<sup>139</sup> Article 29 Working Party, Opinion 1/2010 on the concepts of “controller” and “processor”, 00264/10/EN WP 169, 16 February 2010.

<sup>140</sup> art. 6 (4) GDPR.

#### h. Data subject rights and principles

In case of collection and sharing of personal data, certain other legal obligations are important. For example should the controller provide for the data subjects rights. The data subject has certain rights to their personal data, such as information rights, access to, rectification and erasure of the data or the data subject might want to receive the personal data, restrict the processing or object to it. The data controller has to inform the data subject on how it can exercise these rights. However, the Member States may restrict these rights by legislative measures to safeguard e.g. national security, public security or important objectives of general public interest. These legislative measures must respect the essence of the fundamental rights and freedoms and be necessary and proportionate in a democratic society. It should be assessed whether national law provides for such a restriction, under Directive 95/46/EC it was not extensively used by many Member States.<sup>141</sup>

In general, the GDPR has certain basic principles relating to the processing of personal data. It requires that the data shall be processed lawfully, fairly and in a transparent manner, which is a reason why the data subject has certain rights to information. Furthermore, the data should only be collected for specified, explicit and legitimate purposes, and needs to be adequate, relevant and limited to what is necessary in relation to that purpose. For this reason one should primarily assess what the purpose of the data is (network and information security or possible even more specified, e.g. enforcing access restrictions, mitigating DDOS attacks) and which data is necessary for this. The data should furthermore be accurate and kept up to date and only be kept as long as is necessary for the purpose. This means that it might be necessary to provide deletion timeframes for specific types of personal data and it is therefore not acceptable to keep personal data 'just in case' for an undefined timeframe.

Finally, the data needs to be protected, e.g. against unauthorised or unlawful processing and against accidental loss, destruction or damage. The controller is the one accountable for the compliance with the provisions. In case the data is shared with a processor, the controller needs to ensure the adherence to the provisions via a contract. In case the data is shared with another controller, the second controller is accountable for the shared personal data.

## 4.2 Requirements in intellectual property and unfair competition law

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

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

---

<sup>141</sup> Douwe Korff, EC Study on Implementation of Data Protection Directive, Cambridge UK, September 2002, p.142.



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

For the purposes of this Deliverable our attention will focus on the EU level legislative advances as they provide more precise insights and have grown from these international foundations.<sup>142</sup> Indeed, this is evidenced by the fact that the European Court of Justice have found Member States in breach of their obligations under EU law by failing to comply with the Berne Convention following the issuing of a reasoned opinion requiring compliance by the Commission.<sup>143</sup>

As per the liability that ECOSSIAN may incur, it must be understood that is unlikely that there would be an infringement of certain IP rights such as computer programme copyright, or those protected by patent law or trademark law.<sup>144</sup> This is based on the assumption that the information that would be shared in a disaster situation would be unlikely to constitute anything other than information to be processed by a computer programme. In this regard, liability might occur at the acquisition and information sharing stage when ECOSSIAN (1) collects data reported by the O-SOCs, and acquired from public external sources, (2) temporarily stores it, and (3) makes it available to the analysis components (Cymerius and CAESAIR). It will encompass all source materials shared in a disaster situation, including any relevant document collected and stored in the system, such as incident report from an O-SOC, security advisory, forum post, email message. Collection, storage and making available of protected content might infringe copyright or database rights as explained in more details below. Also, use and disclosure of information that qualify as “trade secrets” might be in violation of EU provisions.

In any event, please consider that exclusive rights granted to traditional copyrightable, patentable and trademarkable subject matters will apply to content, including computer programs and databases, inventions and trademarks developed as part of the ECOSSIAN Project. In particular, contents (data) of a database created by ECOSSIAN shall be protected as long as they qualify for *sui generis* database right protection (see explanation in the next section). Also, trade secrets held by ECOSSIAN shall be protected against unlawful acquisition, use and disclosure. Details of protection granted are included in the sections below.

Accordingly the key Directives<sup>145</sup> in this context are as follows:

<sup>142</sup> See: Council Resolution of 14 May 1992 on increased protection for copyright and neighbouring rights [1992] OJ C138/1; Rental lending and related rights Directive; and Treaty establishing EEA.

<sup>143</sup> Case C-13/00 *Commission v Republic of Ireland* (ECJ 19 March 2002).

<sup>144</sup> However for absolute certainty regard must be had to all relevant IP rights.

<sup>145</sup> Other EU legislation includes: Directive 2006/115/EC of the European Parliament and of the Council of 12 December 2006 on rental right and lending right and on certain rights related to



- Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (InfoSoc Directive);
- Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases (Database Directive);
- Directive 2016/943/EU of the European Parliament and the Council of 8 June on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (Trade Secret Directive).

#### 4.2.1 Copyright and Database Right

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

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

Protection	Object	Restricted acts	Relevant exceptions
<b>Ordinary copyright</b>	A ‘work’ (i.e. a person’s expression of an idea resulting in an	Directive 2001/29/EC Articles 2-4 in addition to Directive 92/100/EEC <sup>146</sup> Article 5 The acts of	- Temporary technical reproductions (Directive

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

<sup>146</sup> Council Directive 92/100/EEC of 19 November 1992 on rental right and lending right and on certain rights related to copyright in the field of intellectual property (OJ L 346, 27.11.1992, p. 61). Directive as amended by Directive 93/98/EEC.

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

Table 6: Intellectual Property

#### 4.2.1.1 Ordinary and Database Copyright

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

According to Article 2 of the Information Society Directive and Article 5(a) of the Database Directive, reproducing refers to any direct or indirect, temporary or permanent reproduction,

in whole or in part and by any means and in any form. In principle this broad notion of ‘reproducing’, also covers the often short-lived duplications necessary for a computer to perform a task. In addition, ‘reproducing’ is usually taken to cover ‘adapting’ and ‘translating’.

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

Distributing refers to any form of distribution to the public by sale or otherwise of copies of the ‘work.’ ‘Renting’ and ‘lending’ are also subject to the authorisation of the right holder. ‘Renting’ is defined as the making available for use, for a limited period of time and for direct or indirect economic or commercial advantage.<sup>147</sup> ‘Lending’ refers to the making available for use, for a limited period of time and not for direct or indirect economic or commercial advantage, through establishments which are accessible to the public.<sup>148</sup>

Finally, it is important to make one distinction regarding database copyright. From Article 3 it is the selection and arrangement of the contents of the database that constitutes the author’s own intellectual creation and that this is without prejudice to any rights subsisting in the contents themselves. This does not mean that the database copyright extends to contents but rather that the original arrangement of any information contained in the database may also have an independent protection. According to the CJEU jurisprudence—as in the case of ordinary copyright protection—the selection or arrangement of the data which the database contains must amount to an original expression of the creative freedom of its authors. As a consequence, the intellectual effort and skill of creating the data are not relevant in order to assess the eligibility of that database for protection; it is irrelevant whether the selection or arrangement of data includes the addition of important significance to that data; and the significant labour and skill required for setting up the database cannot as such justify protection.<sup>149</sup>

#### 4.2.1.2 Database *Sui Generis* Right

According to Article 1(2) of the Directive, the database *sui generis* right—which last 15 years renewable indefinitely each time the database is substantially modified—applies to any “collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means. For securing protection, however, the database creator must prove that there has been qualitatively and/or quantitatively a substantial investment in either the obtaining, verification or presentation of

<sup>147</sup> Directive 2006/115/EC of the European Parliament and of the Council of 12 December 2006 on rental right and lending right and on certain rights related to copyright in the field of intellectual property (codified version) OJ L 376, 27 December 2006 (hereinafter “Rental and Lending Directive (2006)”), Article. 2.1.

<sup>148</sup> Ibid., Article 2.1(b).

<sup>149</sup> See C-604/10 (*Football Dataco Ltd v. Yahoo! UK Ltd*), European Court of Justice 1 March 2012.

the content. In this regard, protection is not available for “created” data as such.<sup>150</sup>

Under Article 7(1) of the Directive, two categories of acts—‘extracting’ and ‘re-utilising’ (as noted in the table)—are subject to authorisation. From Article 7(2) these refer to:

*“(a) ‘extraction’ shall mean the permanent or temporary transfer of all or a substantial part of the contents of a database to another medium by any means or in any form;*

*(b) ‘re-utilization’ shall mean any form of making available to the public all or a substantial part of the contents of a database by the distribution of copies, by renting, by on-line or other forms of transmission. The first sale of a copy of a database within the Community by the rightholder or with his consent shall exhaust the right to control resale of that copy within the Community;”*

These concepts only apply in relation to acts covering the whole or substantial part (either qualitatively or quantitatively) of the content of a ‘database’. Indeed, as can be thus inferred this *sui generis* right does then not give the rightholder an exclusive power over individual elements of the database. However, from Article 7(5) the systematic and repeated extraction or re-utilisation would be deemed an infringement as soon such activities cumulatively result in a substantial part.<sup>151</sup>

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

*“The scope of application of these rights can be very broad, with the line between protection and unprotected information being particularly blurred in the case of copyrights... and sui generis database rights... as these do not require any prior registration.”<sup>152</sup>*

It is with this in mind that our attention now turns to the potentially relevant exceptions which may have an impact and legitimise such sharing. It should be noted that there are several other exceptions that are not discussed as they are not relevant in the context of information sharing in disaster situations.

#### 4.2.1.3 Exceptions

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

<sup>150</sup> See C-203/02 (*BHB v. William Hill*) European Court of Justice 9 November 2004, para 36.

<sup>151</sup> For more see: C-203/02 (*BHB v. William Hill*) European Court of Justice 9 November 2004, para 89.

<sup>152</sup> ENISA, ‘A flair for information sharing- encouraging information exchange between CERTs’ (2011) accessed on 01/03/2015 at: <http://www.enisa.europa.eu/activities/cert/support/fight-against-cybercrime/legal-information-sharing>

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

*(a) a transmission in a network between third parties by an intermediary, or*

*(b) a lawful use*

*of a work or other subject-matter to be made, and which have no independent economic significance, shall be exempted from the reproduction right provided for in Article 2.”*

The precise scope of this exception has given rise to debate.<sup>153</sup> Nevertheless, it is clear that this exception may have relevance if the sharing of information requires the creation of temporary reproductions of a work as part of the technological process needed to transmit the information.<sup>154</sup>

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

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

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

1) only those granted a licence by the right holder;

2) to anyone who lawfully acquired an embodiment of the ‘database’; or

3) also to everyone acting within the limits of a normal use of an embodiment of the ‘database’ regardless whether this embodiment was acquired lawfully.<sup>155</sup>

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

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

<sup>153</sup> See: S. Clark, “Just browsing? An analysis of the reasoning underlying the Court of Appeal’s decision on the temporary copies exemption in Newspaper Licensing Agency Ltd v Meltwater Holding BV”(E.I.P.R. 2011) 727.

<sup>154</sup> See also Directive 2001/29/EC Recital 33

<sup>155</sup> See: V. Vanovermeire, “The Concept of the Lawful User in the Database Directive” (I.I.C. 2000) 63-81.



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

(4) The final **exception** is **common** to all and relates to that of public security as provided for by Article 5(3)(e) the Information Society Directive and Articles 6(1)(c) and 9(1)(c) of the Database Directive. Member States such as Germany<sup>156</sup> and the UK<sup>157</sup> have implemented such an exception in contrast to Belgium and Ireland. However, in their review of the current implementation in Ireland the Copyright Review Committee recommended such a provision.<sup>158</sup>

#### 4.2.2 Unfair Competition and Trade Secrets

Directive 2016/943/EU protects against the unlawful acquisition, use and disclosure of trade secrets. According to Article 2 of the Directive, “trade secret” means information which (a) is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question; (b) has commercial value because it is secret; (c) has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.

Any source materials shared in a disaster situations could include trade secrets.

However, please note that trade secrets are not a form of exclusive intellectual property rights. Therefore, the Directive does not create any exclusive right to know-how or information protected as trade secrets.<sup>159</sup>

Although, unlawful acquisition of trade secrets would apparently be out of the scope of ECOSSIAN liability concerns, use or disclosure of trade secrets could occur during information sharing and making data available to the analysis components. According to Article 4 of the Directive, the use or disclosure of trade secrets is unlawful when carried out without the consent of the trade secret holder, (a) if the trade secret was acquired unlawfully, or the disclosure happens (b) in breach of a confidentiality agreement or any duty not to disclose the trade secret, or (c) in breach of a contractual or any other duty to limit the use of a trade secret. ECOSSIAN might have a duty not to disclose the trade secret, if it is included in any shared source document.

An exception to the protection of trade secrets is provided whenever the use and disclosure was carried out for the purpose of protecting a legitimate interest recognized by the EU or national law. As there is no EU case law regarding the interpretation of the Directive yet, the scope of the duties and exceptions mentioned above can hardly be predicted. In any event, ECOSSIAN should apply a stringent standard and avoid disclosure of trade secrets as part of the information sharing.

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

---

<sup>156</sup> Section 45, 2) German Copyright Law

<sup>157</sup> Sections 45-50 UK Copyright

<sup>158</sup> Modernising Copyright A Report prepared by the Copyright Review Committee for the Department of Jobs, Enterprise and Innovation [www.enterprise.gov.ie/en/Publications/CRC-Report.pdf](http://www.enterprise.gov.ie/en/Publications/CRC-Report.pdf)

<sup>159</sup> See Directive 2016/943/EU, Recital 16.



Req. number	Description	Importance* (M/O)	Relevant for Level			Comment
			O-SOC	N-SOC	E-SOC	
GReq. 5.1	The authorisation of IP right holder should be sought in relation to any protected work (most likely copyright)	M	X	X	X	
GReq. 5.2	If you are using more than an unsubstantial part of a database seek authorisation from the sui generis database owner	M	X	X	X	
GReq. 5.3	Consult national IP specialist in order to adequately assess the applicable exemptions/exceptions	M	X	X	X	
	Trade secrets acquired, collected, stored or processed as part of ECOSSIAN should not be used or disclosed	M	X	X	X	

\*M – mandatory; O – optional

\*\* Work Packages where this requirement should be implemented

Table 7: Requirements in IP

# Chapter 5    Classification    and    confidentiality

## obligations

As explained in D7.3 2.4.2.2.2, security sensitive information is a key concern for the ECOSSIAN platform. In this chapter we will have a deeper look in the EU approach regarding security rules for EU classified information, including a short analysis of several national provisions.

### 5.1 EU classification rules/strategy

As stated by Galloway *“the dispersed nature of power in the EU’s institutional structure and the sheer numbers of individuals involved in policy analysis and decision-making render it a challenging environment in which to preserve secrecy.”*<sup>160</sup> As ECOSSIAN is also envisaged in a dispersed structure, after analysing the EU approach, we will not only consider in how far the EU approach needs to be complied with in ECOSSIAN, but also reflect upon whether there are strategies that can be used within ECOSSIAN.

The EU does not have specific legislation on the classification of security information. This is due to the fact that the EU has no competency in this field, as national security is according to article 4 TEU ‘the sole responsibility of each Member State’.<sup>161</sup> Nevertheless there are reasons why the EU needs rules on security classification, as the Maastricht and Amsterdam treaties included the objective for the Union to develop a common foreign and security policy and to take action to prevent and combat crime, and security classification rules are a necessary prerequisite for the EU to co-operate in a meaningful way with third states and international organisations.<sup>162</sup> Accordingly, in order to develop a regulatory framework for security classification the EU’s institutions have taken a procedural approach largely based on internal rules.<sup>163</sup>

The front-runner in the end (after some initial but unsuccessful initiatives of the Commission) was the Council, which in 2001 adopted in a decision comprehensive security rules on protecting EU classified information, and thereby defined ‘EU classified information’ (EUCI) as a legally distinct category from ‘national classified information’.<sup>164</sup> The Commission

<sup>160</sup> David Galloway, “Classifying Secrets in the EU,” *JCMS: Journal of Common Market Studies* 52, no. 3 (May 1, 2014): 670, doi:10.1111/jcms.12122.

<sup>161</sup> Ibid.

<sup>162</sup> Ibid.

<sup>163</sup> Ibid. This approach has been criticised by some authors, e.g. Deirdre Curtin, “Overseeing Secrets in the EU: A Democratic Perspective: Overseeing Secrets in the EU,” *JCMS: Journal of Common Market Studies* 52, no. 3 (May 2014): 684–700, doi:10.1111/jcms.12123.

<sup>164</sup> Council of the European Union (2001), ‘Council Decision of 19 March 2001 adopting the Council’s security regulations’, 2001/264/EC, OJ L 101, 11 April 2001.

followed with adopting equivalent provisions in the same year.<sup>165</sup> The European Parliament adopted rules on the treatment of confidential information in 2011.<sup>166</sup>

As the system is built on legal bases used for the internal organization of EU institutions, it faces two challenges:

- 1) maintaining equivalence across institutions and bodies handling classified information
- 2) guaranteeing adequate protection of EUCI in Member States

In order to address the first challenge, internal decisions to set equivalent basic principles and minimum standards are adopted. To reinforce coherence, internal arrangements such as public joint declarations, administrative arrangements and inter-institutional agreements are used. The main actors (General Secretariat of the Council (GSC), Commission and European External Action Service (EEAS)) consult before implementing substantive changes to their respective rules on security classification. Socialization among security experts in EU institutions plays an important role, Galloway even states that *“equivalence is driven through peer pressure and practical operational considerations as a result of frequent networking across epistemic communities of relevant experts”*.<sup>167</sup>

The second challenge is addressed by the use of intergovernmental agreements.<sup>168</sup> This has several advantages, as it not only reinforces obligations on Member States to protect EUCI provided to them by EU institutions, but also ensures the protection for any classified information provided by a Member State to any EU entity which is subsequently distributed to other Member States and enables Member States to exchange national classified information in the interests of the EU where the two Member States have no bilateral security of information agreement between them and it reinforces the obligation to protect any information provided to the EU by a third state or international organization which is subsequently distributed to Member States.<sup>169</sup>

We will now turn our attention to the specific rules on EUCI. After its first decision in 2001, the Council updated its internal rules with Decisions 2001/264/EU<sup>170</sup>, 2011/292/EU<sup>171</sup> and Decision 2013/488/EU. We will analyse here Decision 2013/488/EU<sup>172</sup> including its recent amendments according to Council Decision 2014/233/EU<sup>173</sup> and the internal guidelines<sup>174</sup>.

<sup>165</sup> Commission Decision 2001/844/EC, ECSC, Euratom of 29 November 2001 amending its internal Rules of Procedure, OJ L 317, 3 December 2001.

<sup>166</sup> European Parliament (2011), ‘Decision of the Bureau of the European Parliament concerning the rules governing the treatment of confidential information by the European Parliament’, OJ C190, 20 June 2011.

<sup>167</sup> Galloway, “Classifying Secrets in the EU,” 677.

<sup>168</sup> Ibid.

<sup>169</sup> Ibid.

<sup>170</sup> Council Decision 2001/264/EC of 19 March 2001 adopting the Council’s security regulations (OJ L 101

<sup>171</sup> Council Decision 2011/292/EU of 31 March 2011 on the security rules for protecting EU classified information OJ L 141

<sup>172</sup> Council Decision 2013/488/EU of 23 September 2013 on the security rules for protecting EU classified information.

<sup>173</sup> Council Decision 2014/233/EU of 14 April 2014 amending Decision 2013/488/EU on the security rules for protecting EU classified information.

<sup>174</sup> Council of the European Union, Handling of documents internal to the Council, 1136/11 (9.6.2011) and 10384/13 (31.5.2013).

We will also consider the most recent Commission Decision (EU, Euratom) 2015/444<sup>175</sup> in this analysis<sup>176</sup>.

The Council and the Commission define EUCI as *“any information or material designated by an EU security classification, the unauthorised disclosure of which could cause varying degrees of prejudice to the interests of the European Union or of one or more of the Member States”*.<sup>177</sup>

EUCI is classified in 4 levels by the effect an unauthorised disclosure could have on the interests of the European Union or of one or more of the Member States:

- TRES SECRET UE/EU TOP SECRET: could cause exceptionally grave prejudice to the essential interests
- SECRET UE/EU SECRET: seriously harm the essential interests
- CONFIDENTIEL UE/EU CONFIDENTIAL: harm the essential interests
- RESTREINT UE/EU RESTRICTED: be disadvantageous to the interests

The competent authority shall ensure that EUCI is appropriately classified and clearly identified as EUCI.<sup>178</sup> The classification is done via markings indicating the classification level, and possibly additional markings indicating the field of activity to which it relates, the originator, distribution limitation, restricted use or releasability.<sup>179</sup> The decisions further specify security provisions, Some important rules are:

- Originator consent: the EUCI shall not be downgraded or declassified, security markings modified or removed without prior written consent of the originator.<sup>180</sup>
- the competent authorities ensure that the information retains its classification level for only as long as necessary.<sup>181</sup>
- The holder of the EUCI is responsible for protecting it.<sup>182</sup>
- An aggregate of EUCI may warrant a level of protection corresponding to a higher classification than that of its individual components.<sup>183</sup>

The Council decision also established a Council security committee as a forum where Member States' national security authorities could deliberate on all matters relating to classified information (art. 17 Council Decision 2013/488).<sup>184</sup> Likewise, the Commission decision established a Commission security authority (art. 7 (4) Commission Decision 2015/444).

<sup>175</sup> Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information, OJ L72/53, 17 March 2015.

<sup>176</sup> This decision is very similar to the Council decision including its annexes.

<sup>177</sup> art. 3 Commission decision, art. 2 Council decision.

<sup>178</sup> art. 3 Council Decision, art. 4 Commission decision (the Commission decision specifies the competent authority as each Member of the Commission or Commission department which created the EUCI).

<sup>179</sup> art. 2 (3) Council, 3 (3) Commission.

<sup>180</sup> art. 4 (2) Commission, art. 3(2) Council.

<sup>181</sup> art. 4 (1) Commission, art. 3 (1) Council.

<sup>182</sup> art. 5 (2) Commission, art. 4 (2) Council.

<sup>183</sup> art. 5 (4) Commission, art. 4 (4) Council.

<sup>184</sup> Galloway, “Classifying Secrets in the EU.”

Sharing with third states or international organisation is possible (art. 13 Council Decision 2013/488 and art. 54 Commission Decision 2015/444) and is arranged via security of information agreements.<sup>185</sup> These agreements contain provisions to ensure the appropriate protection considering the classification level and according to minimum standards equivalent to those in the decision.

Finally, the Council and the Commission decision include an appendix listing the equivalence of security classification of Member States with the EUCI classification.

### **5.1.1 National classification rules**

On a national level, Member States can consider certain information as classified. Information relating to Critical Infrastructures can potentially be security sensitive and there might be national measures relating to classification of certain types of information as secret or a similar categorisation. There is a large degree of disparity between the Member States. For example in Ireland no framework currently exists for the classification of data. However, the Official Secrets Act 1963 does stipulate the definition for an official secret. This contrasts sharply with the situation in many other countries. For example in Germany, national security secrets are defined in § 93 of the German Criminal Code (StGB), while the Safety Assessment Act (SÜG)<sup>186</sup> regulates the requirements for people who do security relevant tasks, including getting access to classified information. § 4 SÜG defines four levels of classification for information or items considered necessary to be kept secret in the public interest. Similar classification systems are evident in the UK, Italy, Belgium and France.<sup>187</sup> The key issue however relates to the fact that the precise criteria and oversight into such classifications are not always apparent.<sup>188</sup>

However, four basic principles can be identified in the laws governing the protection of classified information:<sup>189</sup>

- 1) Classified information may only be accessed by persons who have a need-to-know because of their official or contractual duties.
- 2) If the information is classified confidential UE/EU Confidential or higher, persons must also have been security cleared. Allowance is made in law in certain Member States for individuals such as government ministers or judges to be granted access by virtue of their positions without undergoing a security vetting procedure. All individuals must, however, be briefed on their responsibilities before being granted access
- 3) Appropriate physical, organisational and procedural measures are enforced to protect the confidentiality, integrity and availability of information, based on the concept of 'defence in depth' (that is, applying protective measures commensurate with the risk of disclosure)
- 4) When information originates in another entity or state, it may not be declassified, disclosed nor passed to another party without the prior consent of the originating party (so-called 'originator consent' principle).

---

<sup>185</sup> Ibid., 678.

<sup>186</sup> Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes (Sicherheitsüberprüfungsgesetz - SÜG).

<sup>187</sup> See: <http://cybersecurity.bsa.org/countries.html>

<sup>188</sup> Galloway, "Classifying Secrets in the EU," 672.

<sup>189</sup> Ibid.

The classification of a document involves a deliberate decision by an official entity producing the information, requiring that it must be marked correctly, handled in an appropriately accredited information technology system and used in an official context in accordance with the relevant legal requirements.<sup>190</sup> Of course, it is possible that documents are overclassified or underclassified.<sup>191</sup>

### **5.1.2 Technical and organizational requirements as a hurdle**

Aside from the fact that revealing classified information is punishable in many Member States, the necessary technical and organizational requirements coming along with the handling of classified information can also provide a barrier for information sharing. For example, the Council Directive 2008/114 requires that any person handling classified information (also in case of non-written information exchanged during meetings at which sensitive subjects are discussed) must have gone through an appropriate level of security vetting (Article 9, recital 18 Directive 2008/114).

The NIS Directive also includes exceptions regarding confidential information in Article 1(5) and (6). These provisions declare that confidential information based on Union or national rules (including rules on business confidentiality) shall only be exchanged with the European Commission and other relevant authorities if the exchange is necessary for the application of the Directive. Such information must be kept confidential, used to protect the interest of the operators of essential services and be limited to what is relevant and proportionate to achieve the purpose of the exchange. The Directive does not however, require the disclosure of information that Member States consider contrary to their national security interests.

### **5.1.3 ECOSSIAN**

The above mentioned two challenges also arise in the context of ECOSSIAN. The first one is to maintain equivalence across the different O-SOCs and N-SOCs handling classified information and the second one is to guarantee adequate protection of the classified information in the different SOC.

As explained, for EUCI this was handled by internal decisions setting equivalent basic principles and minimum standards, accompanied by internal arrangements such as joint declarations and inter-institutional agreements. Furthermore, intergovernmental agreements were used to guarantee the adequate protection on Member State level and socialization amongst security experts in the EU institutions was also named as an important factor.

Comparably, ECOSSIAN should also set basic principles and minimum standards, which then will be applied via agreements between the different SOC. Information should be classified, whereby the traffic light protocol is often considered as useful, possibly in combination with national or EU classification levels. Technically, the classification and access to classified information within ECOSSIAN is ensured via the Secure Gateway and ABE, as well as access authorization (which needs to be ensured organisationally). The classification should be done by the originator of the information and shall not be downgraded or declassified without consent of the originator. The holder of the information

---

<sup>190</sup> Ibid., 674.

<sup>191</sup> see e.g. the study of Renato Rocha Souza, Flávio Codeço Coelho, Rohan Shah, Matthew Connelly: Using Artificial Intelligence to Identify State Secrets. CoRR abs/1611.00356 (2016), available at <https://arxiv.org/ftp/arxiv/papers/1611/1611.00356.pdf> (last accessed 6.4.2017).



will be responsible for protecting it and in case of disagreements regarding the classification the ESGMO as mentioned in D7.9 and D7.10 could possibly act as a forum for deliberation.

At a business level, it should be noted that there might also be confidentiality obligations towards third parties, which may have a restricting impact on the sharing of information. For example, a third party may make its voluntary cooperation subject to a confidentiality agreement in the form of a non-disclosure agreement. These non-disclosure agreements need to be taken into account on the CI operator side (there especially by the human operator in order not to disclose information covered by the non-disclosure agreement) and also on the SOC sides.

The GReq outlined in D7.3 stay applicable for an ECOSSIAN implementation.

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

\*M – mandatory; O – optional

\*\* Work Packages where this requirement should be implemented

Table 8: Confidentiality obligations

## Chapter 6 Italian Analysis

### 6.1 Introduction to the Italian legal framework

As pointed out in “D7.3 version 1”, information sharing in disaster situation is a crucial issue for damage prevention and to avoid, or at least to curb, its further dissemination. ECOSSIAN aims to design detection tools that facilitate preventive functions such as threat monitoring, early warning and alerting for Critical Infrastructures. While the main focus of “D7.3 version 1” and the main part of D7.7 is the EU legal framework for information sharing, this chapter will instead focus on the national legislation of Italy.

The analysis will be divided as follows: section 6.2 will first review the Italian Critical Infrastructure framework, comparing Directive 2008/114/EC and its Italian implementation providing further information on (a) the actors of the Italian emergency system; (b) the CI information sharing platform and PPP models; and (c) the Italian Civil Protection regulation and Italian CIP mechanism for disaster management. Section 6.3 will focus on criminal law and the ICT specific legal framework. Section 6.4 will focus on legal barriers to information sharing, whether they are arising from legislation or arising from an agreement of the parties. Section 6.5 will focus on the impact on the ECOSSIAN System.

### 6.2 Disaster Management

As stated in the introduction, this section focuses on the disaster management framework in relation to Critical Infrastructures. The analysis is divided into five sub-sections. Sub-section 6.2.1 focuses on the Critical Infrastructure framework, summarizing the basic concepts, extrapolated from D7.2 and D7.3; sub-section 6.2.2 focuses on the Italian information sharing platforms in relation to Critical Infrastructure protection; subsection 6.2.3 focuses on the Italian Civil Protection mechanism; subsection 6.2.4 concerns public-private partnerships; and finally, subsection 6.2.5 is about Italian national approaches to disaster management.

For the Disaster Management we have to distinguish between several actors, and several scenarios which will be further described below.

#### 6.2.1 Critical Infrastructure Framework

Critical infrastructure framework can be described as a wheel with several spokes, in which the central pin is Directive 2008/1147/EC and its national implementation, and the spokes are the rules regarding specific sectors, still in the field of Critical Infrastructure.

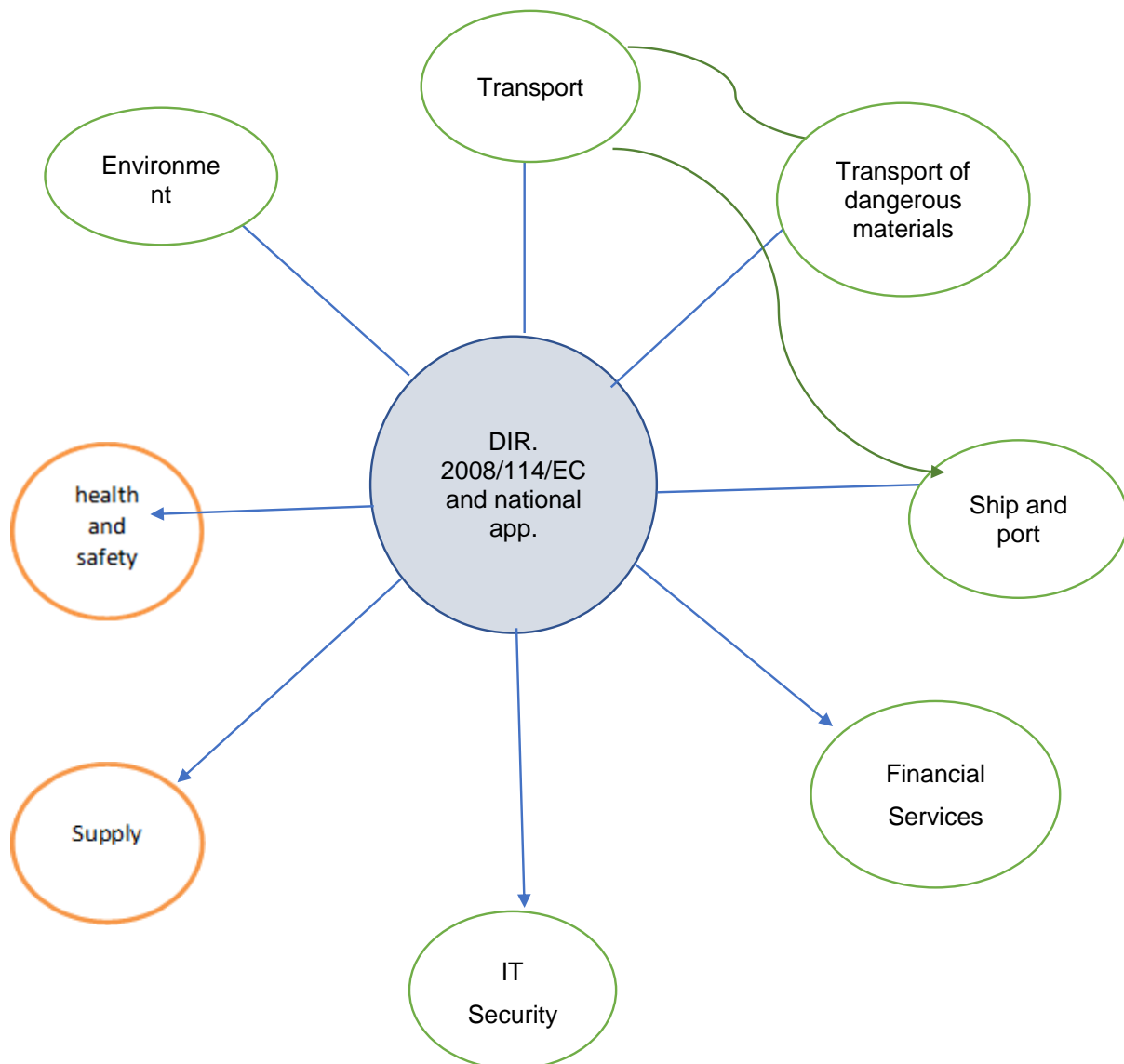


Figure 1: Directive 2008/114/EC and some of its specific applications

For each specific sector again different legislation applies which is found in specific EU directives, in their national implementation, and in international standards which are often applied on voluntary basis.

So, the basic Critical Infrastructure framework was pointed out before:

- in D7.2 «Legal Requirements» the focus was on the legal requirement relevant for ECOSSIAN, with specific attention to privacy and data protection requirements, derived mainly from Directive 95/46/EC and the GDPR<sup>192</sup>); it further also sets out and describes the essential features of the concept of “Privacy by design”<sup>193</sup>.
- in «D7.3 version 1» the focus is on Directive 2008/114/EU and in particular on the disaster management framework and on the legal framework for information sharing. About that, we have to remember that presently there is no requirement to share

<sup>192</sup> General Data Protection regulation: Proposal for a Regulation of the European Parliament and of the Council on the people protection with regard to the processing of personal data and on the free movement of such data.

<sup>193</sup> This deliverable derived from D 7.1 “Analysis of the applicable legal framework”.

information on threats or attacks (except for specific notification obligations), despite the above mentioned rules it is clear that some degree of cooperation and information sharing between the operators is necessary<sup>194</sup>.

### 6.2.1.1 ITALY

With regard to the Italian legislation, we analyse below the national implementation of Directive 2008/114/EU which is Legislative Decree April 11th, 2001 No. 61<sup>195</sup>.


DIRECTIVE 2008/114/EU	TOPIC	Legislative Decree 2011/61
Art. 1 subject matter: The Directive establishes a procedure for the identification and designation of ECIs and a common approach to the assessment of the need to improve their protection in order to protect people.	Matter	Art. 1 object: First paragraph repeats art. 1 of the Directive, restricting the scope to the transport and energy areas. Paragraph 3 states that the procedure for the identification pertaining ECIs located in Italy would have an interest in designating as ECI. Other paragraphs concern the identification of the responsible ministries.
Art. 2: Definitions (a) 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, people economic or social well-being, 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; (b) European critical infrastructure [...]; (c) 'risk analysis' means consideration of relevant threat scenarios, in order to assess the vulnerability and the potential impact of disruption or destruction of	Definitions	Art. 2, Definitions: in addition to the definitions of the Directive, the Italian legislation also defines: - sector: areas of similar activities (mentioned in art 3. Dir. EC and in Annex III); - intersector: related to two or more sectors or related to subsector; - external negative effects: negative effects on service delivery; - internal negative effects: damage or destruction of infrastructure; - sectorial evaluation criterion: percentage of service users, compared to the national population.

<sup>194</sup> This is pointed out, inter alia, by Directive 2008/114/EC through the obligation:

- to create a Security Liaison Officer (art. 6);
- for Member State, to report generic data to the Commission every two years on a summary basis on the types of risks, threats and vulnerabilities encountered per ECI sector (art 7.2);
- for the Commission, to support, through the relevant Member State authority, the owners/operators of designated ECIs by providing access to available best practices and methodologies as well as support training and the exchange of information on new technical developments related to critical infrastructure protection (art. 8). See D 7.3 page 30 and D 7.9.

<sup>195</sup> A "legislative decree" is a regulation issued by the Government empowered by the Parliament.

DIRECTIVE 2008/114/EU	TOPIC	Legislative Decree 2011/61
critical infrastructure; (d) see above; (e) 'protection' [...]; (f) owners/operators of ECIs [...];		
Art. 2 (d): sensitive critical infrastructure protection related information means facts about a critical infrastructure, which, if disclosed, could be used to plan and act with a view to causing disruption or destruction of critical infrastructure installations;	Sensitive Information	<p>Art. 2 (n) and art. 3: the definition in art. 2 (n) follows the provision of Directive. Art. 3 "Sensitive Information protection" refers to the Italian Regulation Act on "State secrets" (L. 2007/124). This act states the following secrecy classifications:</p> <p><i>Top secret, secret, confidential and restricted.</i></p> <p>According to abovementioned art. 3, if you give a greater qualification of <i>restricted</i>, only authorized personnel can process information, except for the necessary information to protect and to safeguard users. So information sharing is expressly provided, even as a precautionary measure.</p> <p>With regard to communications to the EU Commission and to the Member States, Legislative Decree 2001/61 refers to EC Regulation no. 1049/2001 of the EU Parliament and of the Council of 30<sup>th</sup> May 2001 regarding public access to European Parliament, Council and Commission documents</p>
<p>Art. 3: Pursuant to the procedure provided in Annex III, each Member States shall identify potential ECIs which both satisfy the cross-cutting and sectoral criteria and meet the definitions set out in Article 2(a) and (b).</p> <p>The cross-cutting criteria referred to in paragraph 1 shall comprise the following:</p> <p>(a) casualties criterion (assessed in terms of the potential number of fatalities or injuries); (b) economic effects criterion (assessed in terms of the significance of economic loss and/or degradation of products or services, including potential</p>	Identification of ECIs	<p>An interdepartmental group (called NISP) supports the competent body with technical skills (hereinafter "competent body"), appointed by the Government Chief, which has to:</p> <ul style="list-style-type: none"> <li>- identify ECIs;</li> <li>- liaise with the EC Commission and with the Member States.</li> </ul> <p>With regard to civilian defense, <b>NISP has to acquire the prior opinion of Italian Civil Protection</b> (see <i>infra</i>)</p> <p>(art. 4 and art. 5)</p> <p>The cross-cutting criteria referred to in art. 3 Dir. 2008/114/EC are reported in art. 6 of Italian regulation.</p>

DIRECTIVE 2008/114/EU	TOPIC	Legislative Decree 2011/61
environmental effects); (c) public effects criterion (assessed in terms of the impact on public confidence, physical suffering and disruption of daily life; including the loss of essential services). See also ANNEX III.		
<p>Art. 4 (1) Each Member States shall inform the other Member States which may be significantly affected by a potential ECI about its identity and the reasons for designating it as a potential ECI. (2) Each Member States on whose territory a potential ECI is located shall engage in bilateral and/or multilateral discussions with the other Member States which may be significantly affected by the potential ECI. The Commission may participate in these discussions but shall not have access to detailed information which would allow for the unequivocal identification of a particular infrastructure.</p> <p>(3) The acceptance of the Member State on whose territory the infrastructure to be designated as an ECI is located, shall be required.</p> <p>(6) The process of identifying and designating ECIs pursuant to Article 3 and this Article shall be completed by 12<sup>th</sup> January 2011 and reviewed on a regular basis.</p>	Designation of ECIs	<p>Art .7 (1) pursuant to art. 4 EC dir. the Italian regulation identifies the responsible organization for the communications of art. 4 (1) dir EC. That organization receives the representatives of the other Members States, according to the prevision of bilateral/multilateral discussion of art. 4 (2) and it shall inform the Commission about its will to start bilateral/multilateral discussion with other Member States.</p> <p>The bilateral/multilateral discussion aims to (i) identify the cross-cutting criteria limits fixed in art. 3 EC dir; (ii) verify whether the effect of the damage to the infrastructure exceeding that limits. If so, that infrastructure is described as ECI. The EU Commission may participate in the bilateral/multilateral discussion, but it has no access to the information that would enable to identify the infrastructure.</p> <p>Art. 8: according to art. 7 (3) of EU dir., the acceptance of the Member State on whose territory the infrastructure to be designated as an ECI is located, shall be required. The Ministerial Council President grants their permission on a proposal of NISP. Art. 8 (5): (5)The definition of infrastructure as ECI is given a suitable degree of secrecy, pursuant to art. 42 of Law No. 124, dated 3th August 2007 and relative implementation rule.</p> <p>Pursuant to art. 9, ECIs identification and designation process should be reviewed every 5 years.</p> <div style="border: 1px solid green; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p>In Italy, “<i>reviewed on a regular basis</i>” means every 5 years</p> </div> 
Art. 4(4) The Member State on whose territory a designated ECI is located	Reporting	Art. 10 identifies the relevant organization for the communication to the Commission.



DIRECTIVE 2008/114/EU	TOPIC	Legislative Decree 2011/61
shall inform the Commission annually about the number of designated ECIs per sector and the number of Member States based on each designated ECI. Only those Member States that may be significantly affected by an ECI shall know its identity.		
Art. 6: The Security Liaison Officer shall function as the contact point for security related issues between the owner/operator of the ECI and the relevant Member State authority.	Security Liaison Officer	Art. 12: The name of the Security Liaison shall be communicated to the Prefect within 30 days of the designation of ECI.
Art. 10: Each Member States shall appoint an European Critical Infrastructure Protection contact point ('ECIP contact point').	ECIP contact point	Art. 13: The Italian national ECIP is NISP; moreover in accordance with the former art. 11 for each ECI a contact point is identified within the relevant Ministry (Ministry of Transport with regard to transportation, Ministry for Economic Development with regard to the energy sector and so on); this is the trade union between the Ministry and the "Competent Body".
Art. 5 (1) The Operator Security Plan ('OSP') procedure shall identify the critical infrastructure assets of the ECI and which security solutions exist or are being implemented for their protection. The minimum content to be addressed by an ECI OSP procedure is set out in Annex II. (3) Each Member States shall ensure that the OSP or equivalent is in place and is reviewed regularly within one year following designation of the critical infrastructure as an ECI. This period may be extended in exceptional circumstances, by agreement with the Member State authority and with a notification to the Commission.	Operator Security Plan (OSP)	<p>Art. 12: (4) the official ECIP contact point and the owner/operator work together with the "Competent Body" to draw up the OSP;</p> <p>(7) the PSO must be completed within one year following the infrastructure designation as ECI and reviewed every five years.</p> <div style="border: 1px solid green; border-radius: 15px; padding: 10px; margin-top: 10px;"> <p>In Italy, "<i>reviewed regularly</i>" means every 5 years</p> </div>

Table 9: Comparison Directive 2008/114/EC with Legislative Decree April 11th, 2001 No. 61

### 6.2.1.2 MILESTONES in ITALY

- Inter-ministerial decree September 21st, 1999: it established a working team composed by representatives of Ministry of Justice, Ministry of Communications, Ministry of Internal Affairs, in order to work as a support in the sector of network and communications security. In 2003 a representative of the Ministry of Economic Development was added to this team and the whole group was converted into a Permanent Observatory for the network and communications security. The Observatory had a great role in the national implementation of Directive 2002/58/EC<sup>196</sup>;
- October 2001: the Technical inter-ministerial commission of defense was established; together with the Italian Civil Protection it has to assess and to prevent emergency situations and take action to reduce its consequences;
- March 2003: the Ministry of Innovation and Technology established a working group on CIIP, where representatives of business and representatives of public sector (Ministry and Academia) worked together in the analysis of the Italian ICIs situation (see also § 2.4);
- D.L. July 27th 2005, No. 144 and July 31th 2005, n. 155 (the so called Legge Pisanu (Pisanu Law)), on urgent measures to fight international terrorism. Art. 7 bis, entitled, Cybersecurity, states that the Ministry of Internal Affairs shall provide information security services for the critical information infrastructure, relevant for the national interest, working in connection with the manager of that ICIs. That is a first step to the later approach of Directive 2008/114/EC. The Postal Police has its jurisdiction for the purposes referred above, and for the prevention and repression of terrorist activities conducted by electronic systems. From this prevision CNAIPIC (National Center for the Protection of the ICIs and the fight of cybercrime) was born which works with, inter alia, Microsoft, Cisco System, McAfee in a PPP perspective;
- L. August 3rd, 2007 No. 124, amended by L. August 7th 2012, No. 133, established the DIS (Department for Information Security) and the COPASIR (Parliamentary Committee for the Security of the Republic)<sup>197</sup>.
  - DIS: it works with the Prime Minister's Office. The Prime Minister's Office gives DIS the directives and the instructions to strengthen information activities for the protection of Critical Infrastructure, with particular regard to cybersecurity and national security. Inter alia DIS ensures unified action to AISE<sup>198</sup> (Agency for the external information and security) and AISI<sup>199</sup> (Agency for the internal information and security);
  - COPASIR: It is a political body that aims to ensure a continuous and holistic security system, in compliance with the law. It shall give a non-binding opinion in every law or regulation proposal about entities involved in security affairs;

<sup>196</sup> *Critical Infrastructure Protection: Threats, Attacks and Countermeasures*, final report of the TENACE project, funded under the *Relevant National Interest Research Projects 2010* (PRIN 2010) by the Italian Ministry of the University and Research (MIUR), page 10.

<sup>197</sup> It consists in 10 Parliament Members chosen in such a way as to guarantee equal representation of the majority and the opposition. The Committee is chaired by an opposition member.

<sup>198</sup> It shall investigate and process all the information in order to defend the independence, integrity and security of the Italian Republic from threats come from abroad.

<sup>199</sup> It has the task to research and process all the information needed to defend the national security of the Italian Republic and democratic institutions from any threat, subversive activities, any form of criminal or terrorist aggression that don't come from abroad.

- Directive 2008/114/EC and Italian implementation by Legislative Decree April 11th, 2001, No. 61 (see above);

DPCM<sup>200</sup> January 24<sup>th</sup>, 2013 (the so-called *Decreto Monti (Monti Decree)*): Repealed and replaced by DPCM Febr. 2017 (see below).

Even though the Monti decree was replaced, it is still important as it provided a first modern configuration of the Italian cybersecurity system. This configuration is partially still existing and it framed the cybersecurity management on 3 levels:

- (i) political level (CISR, *Inter-ministerial committee for the safety of the Republic*), for the development of strategic plans;
- (ii) technical and political level: permanent operational and administrative support given by NIS<sup>201</sup> (*Nucleus for computer security*), lead by the Military Adviser of the Prime Minister;
- (iii) technical level: entrusted by NIST, an Inter-ministerial working group on Cybernetics Crisis. It is operationally supported by the CERT. Here a PPP cooperation has been established as private operators providing public communications networks or electronic communications services to the public and operators who manage ICIs and ECIs, whose operation is influenced by operations of computer, shall:
  - (a) notify the NSC of any significant breach of security or integrity of its information systems, using secure transmission channels;
  - (b) adopt best practices;
  - (c) provide information to the media organizations for safety and allow them the access to databases for the purposes of cybersecurity relevance, when required by law No. 124/2007 (law on State secret, see section 6.3.1 ;
  - (d) collaborate in the cyber crisis management by helping to restore the system functionality and they managed networks.

According to DPCM 24<sup>th</sup> Jan. 2013, which defines the cybersecurity institutional architecture, each year the Prime Minister sets the National strategic framework for cybersecurity on the proposal of the Interministerial Committee for Security of the Republic (CISR) and the related National plan for cybersecurity. So we can say Italy has already done what is required by the NIS Directive, art. 1 lett. A).

In such a context, the CERT-PA (i.e. Public Administration) was established, in order to act as coordinator and facilitator for incident response or for threats to the PA domain and, in general, to provide services for:

- promotion of culture in cyber security;
- analysis in order to develop methodologies to improve cybersecurity;
- collection of useful data for cybersecurity;
- reaction to the threats and the resolution of incidents.

Moreover, the “National CERT” (IT CERT)<sup>202</sup> was established at the Ministry of Economic Development. As mentioned in the official profile<sup>203</sup> of the CERT, according to the PPP

<sup>200</sup> Decree of the President of the Council of Ministers.

<sup>201</sup> Not to be confused with NIS Directive.

<sup>202</sup> Official name: “CERT Nazionale Italia”; short name: IT-CERT; see <https://www.cernazionale.it/cert@mise.gov.it>.

<sup>203</sup> <https://www.cernazionale.it>.

model, IT CERT “supports citizens and companies through awareness and prevention measures and by coordinating the response to large-scale cyber-attacks”.

IT CERT, in fact, consists of Italian citizens and companies; it receives, from its constituency, alerts related to incidents or threats. It evaluates their possible impact at national level, informs all the involved actors and coordinates them in order to find the most suitable solutions, however, the Internet Service Providers (ISP) and the network, system and computer administrators are responsible for the direct support in solving computer issues.

The main goals of the IT CERT are:

- to provide prompt information regarding potential cyber-threats that could damage companies and citizens;
- to improve cybersecurity awareness and culture;
- to cooperate with national and international institutions and other actors, from both the public and private sectors, which are involved in cyber security, by promoting cooperation between them;
- to facilitate the response to large-scale security incidents;
- to support the cyber crisis management process, pursuant to the DPCM 24th Jan. 2013 (see above).

IT CERT is not an authoritative body. It performs its functions through cooperation agreements and protocols. IT CERT assesses the triage label of the reported incidents. Events are analysed, considering and verifying the reliability of the source and under consideration of any other available information. Then they are categorized according to their seriousness.

IT CERT provides services to two groups of users:

- an open group which includes companies and citizens, providing them with information to prevent and to solve cyber incidents and to increase awareness on information security issues;
- a restricted group which includes the main private operators of the Critical Information Infrastructure. The objectives of IT CERT are pursued by using the "infosharing" platform. The platform allows users to share information related to threats or incidents, in order to develop a common approach.

In case of transnational incidents, IT CERT acts as the national Contact Point, so “it receives and shares useful information for mitigating and solving incidents and/or coordinates the response among national and international actors. It undertakes the task to keep its constituency updated on potential vulnerabilities, possibly before they can be exploited”<sup>204</sup>.

Anyone can send information about security incidents, threats or related information to IT CERT by sending an e-mail, possibly encrypted, to [cert@mise.gov.it](mailto:cert@mise.gov.it).

In this case, it is necessary to provide as much information as possible, such as:

- type of incident (or threat);
- involved systems (even potentially involved ones);
- date/time and, if possible, place of the reported event;
- sources of information;
- possible large-scale impacts;

---

<sup>204</sup> see <https://www.certnazionale.it/>, RFC 2350 PROFILE.

- level of confidentiality of information (mainly whether it is in the public domain or not).

The Regulatory Framework for IT CERT is:

- Code of Electronic Communications (Legislative Decree 1st August, 2003 No. 259), as amended by the Implementation of Directive 2009/140/EC (Legislative Decree 28th May, 2012 No. 70, art. 16 *bis*);
- DPCM 24<sup>th</sup> Jan. 2013. It assigns IT CERT the task to support the “NISP Table” (Interministerial Team for Situation and Planning, see above), which acts as the “Interministerial Table for Cyber Crisis”;
- DPCM 5th Dec. 2013 No. 158 which entrusted the High Institute for Communication and Information Technologies<sup>205</sup> with the management of the activities of IT CERT (art. 14).

As a conclusion we can say Italy has already done what is stated by NIS Directive, art. 1 lett. c).

Legislative Decree October 30<sup>th</sup>, 2015, No. 174 (art. 7 *bis*), converted, with modifications, by law 198/2015, has assigned consulting, proposal and deliberation functions to CISR, in case of crisis situations involving national security issues;

DPCM February 17<sup>th</sup> 2017: it is the first attempt to reorganize the national cyber security infrastructure after the NIS Directive. It introduces a new institutional setup to simplify and streamline the chain of command; so nowadays the national cyber security system in Italy is divided in two levels:

A) political level: The Bureau of the Council of Ministers and Interministerial committee for public security (CISR). The role of CISR is stronger than before, because now it approves guidelines to favor the effective collaboration among public actors and private operators, it promotes information sharing and the elaboration and adoption of best practices and measures to increase cyber security;

B) Technical-operational level: DIS, Nucleus for cybersecurity (NSC) and CERT<sup>206</sup>. DIS has an increasingly central and preponderant role. DPCM in fact provides that DIS is the core of prevention, contrast and response actions in cybercrime, so it is the operational center for cybersecurity, oriented both to direct action and to the coordination activity (e.g. with the private industry). In addition, the DIS General Director is the secretary of the CISR.

In the following, further novelties introduced by the DPCM: Moreover, the most novelties introduced by the DPCM are the following:

NIS (*Nucleus for computer security* the acronym in Italian is NIS) is replaced by NSC (*Nucleus for cybersecurity*). NIS was part of the Office of the Military Advisor of the President of the Council (see above), NSC instead is part of DIS and it relies on CERT and CERT-PA (see *supra*). NSC includes the Military Advisor of the Prime Minister and representatives from DIS, AISE, AISI, from the Ministry of Foreign Affairs, the Ministry of Internal Affairs, the Ministry of Defense, the Ministry of Justice, the Ministry of Economic Development, the

<sup>205</sup> The Head of IT CERT is the Director General of the “High Institute for Communication and Information Technologies” within of the Ministry of Economic Development, where CERT Nazionale is established.

<sup>206</sup> National CERT (*Computer Emergency Response Team*; also called IT CERT, see also above in text), established at Ministry of Economic Development, in a PPP prospective, it supports citizens and companies through awareness-raising, prevention and coordination of the response to cyber events on a large scale; in the text see also CERT-PA.



Ministry of Economy and Finance of Department of Civil Protection and the AgID<sup>207</sup>. In relation to the topics of the meetings representatives from other administrations (universities or research institutes, as well as private operators interested in the subject of cyber security) may also be invited to attend. The working group shall meet at least once a month and it reports to the DIS General Director, who reports to the President and CISR (art. 8). Particularly, NSC (art. 9):

- keeps active, 24 hours a day, 7 days a week, the unit for alerting and responding to cybercrime situations;
- promotes information sharing, including with private operators, in order to spread alerts related to cybernetic events and crisis management;
- receives communications about violations or attempts to violate security and about significant loss of the proper functioning of the networks (this information comes in particular from CNAIP);
- promotes and coordinates interministerial exercises and national participation in international exercises related to the simulation of cybernetic events,
- is a national point of contact with the UN, NATO, EU and other international organizations;
- receives, even from abroad, alerts about cybernetic events and delivers alarms to administrations and private operators;
- evaluates whether the event is of an intensity or nature that can not be confronted by the administration itself and if the event is such as to require the adoption of coordinated decisions at interministerial level, it provides coordination;
- promptly informs the Prime Minister of the current situation, through the General Director of DIS;
- drafts reports on the state of implementation of coordination measures in order to manage any crisis;
- Moreover NSC, managing the crisis (art. 10);
- must ensure that the reaction and stabilization activities by the various entities are coordinated, also using CERT and CERT-PA for technical aspects;
- collects all the data about the crisis.

Moreover, in a PPP perspective, due to art.11, private operators providing public communications networks or publicly accessible electronic communications services, as well as key service providers, digital service providers and CI operators:

- have to report to the NCS any significant security breach, using secure transmission channels;
- have to adopt best practices and measures to ensure cyber security;
- have to collaborate to the management of cybercrime;
- have to help to restore the functionality of systems and networks managed by them;
- The DPCM set that the Ministry for Economic Development promotes the establishment of a center establishes a national assessment and certification center for verifying the security conditions and the absence of vulnerabilities on products, equipment and systems intended to be used for the operation of critical networks, services and infrastructures (art. 11, par. 2).

---

<sup>207</sup> AgID stay for “Italian Digital Agency”, it has the task of ensuring the achievement of the goals of the Italian digital agenda in compliance with the European Digital Agenda. For this reason, AgID is assigned, among other things, to the following skills and functions: a) the coordination of central, regional and local governments with regard to cyber issues; b) the issuance of interpretative opinions; c) the issue of addresses, technical rules, guidelines and design methodologies in computer technology; d) the homogeneity of public information systems, see <http://www.agid.gov.it/agid/competenze-funzioni>.



- The DPCM attributes to CISR the power to issue directives to increase the country's computer security level;
- Due to art. 12, about information sharing and dissemination of classified information, all the operators (public and private) shall observe Law No. 124/2007 (art. 4, paragraph 3, letter l)

The DPCM came into force on 13<sup>th</sup> April 2017.

As a conclusion we can say Italy has already done what is stated in the whole art. 1 of NIS Directive.

Many of the above highlights have overlapping skills due in part to the will not to focus the cybersecurity control in few hands, partly, undeniably, due to a poor coordination among the various regulations.

For a comparison, the public actors of the emergency system before DPCM 17<sup>th</sup> February 2017 were:

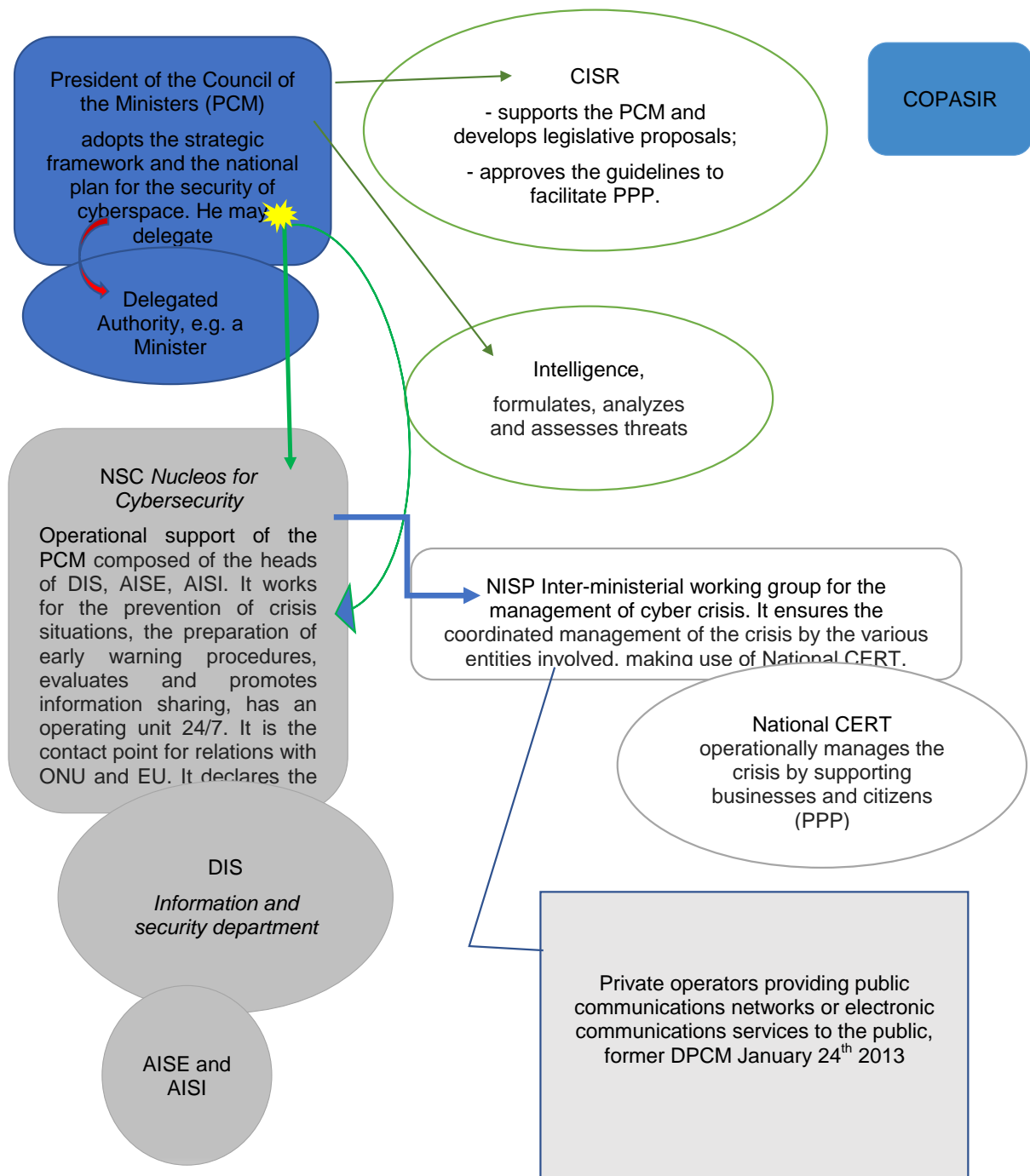


Figure 2: Public actors of the emergency system before DPCM 17<sup>th</sup> February 2017

The public actors of the emergency system after DPCM 17<sup>th</sup> February 2017 are:

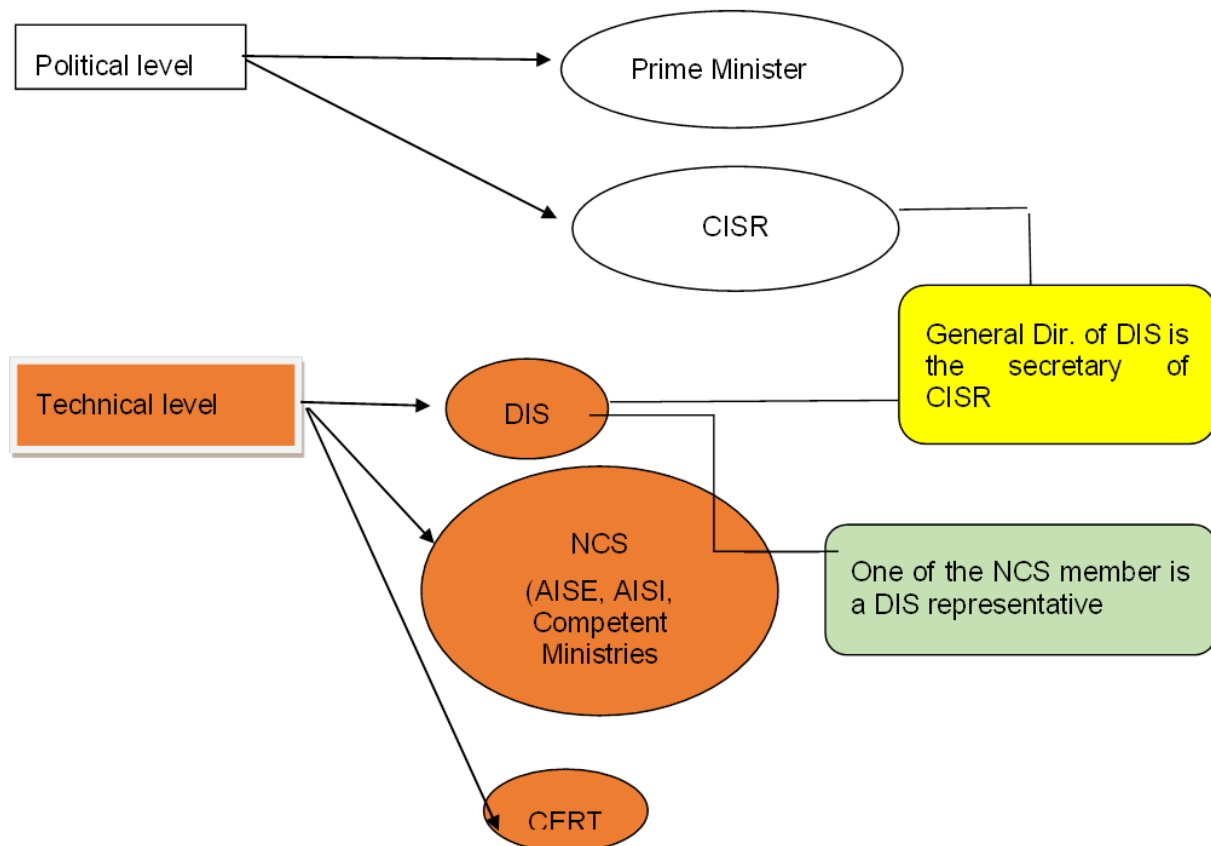


Figure 3: Public actors of the emergency system after DPCM 17<sup>th</sup> February 2017

As becomes clear from the overview, the system has been rationalized and the chain of command shortened.

### 6.2.2 Italian CI Information Sharing Platforms

As referred in the “Proposal for a Directive of the Council on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection”<sup>208</sup>, the European Council of June 2004 asked the Commission to prepare an overall strategy to protect Critical Infrastructure. On 20th October 2004, the Commission adopted a Communication on Critical Infrastructure Protection in the fight against terrorism which put forward suggestions on what would enhance European prevention, preparedness and response to terrorist attacks involving Critical Infrastructures (CI).

The Council conclusions on “Prevention, Preparedness and Response to Terrorist Attacks” and the “EU Solidarity Programme on the Consequences of Terrorist Threats and Attacks”, adopted by Council in December 2004, endorsed the Commission intention to propose an European Programme for Critical Infrastructure Protection (EPCIP) and, in the knowledge that the developing of Critical Infrastructure Protection activities require a degree of confidentiality, it was deemed appropriate to ensure a coherent and secure information exchange. *“Information sharing regarding Critical Infrastructure should take place in an environment of trust and security. The sharing of information requires a relationship of trust*

<sup>208</sup> COM(2006) 787 final, Brussels, 12.12.2006, in [http://www.europarl.europa.eu/meetdocs/2004\\_2009/documents/com/com\\_com\(2006\)0787\\_/com\\_com\(2006\)0787\\_en.pdf](http://www.europarl.europa.eu/meetdocs/2004_2009/documents/com/com_com(2006)0787_/com_com(2006)0787_en.pdf)

*such that companies and organisations know that their sensitive data will be sufficiently protected. To encourage information sharing, it should be clear for the industry that the benefits of providing Critical Infrastructure related information outweigh the costs for the industry and society in general. Critical Infrastructure Protection information exchange should therefore be encouraged*.<sup>209</sup>

The above Council conclusions resulted in the set-up by the Commission of a Critical Infrastructure Warning Information Network (CIWIN). After that, as outlined in D 7.1 and D 7.3 version 1, more than one prototype of information sharing platforms was born, so nowadays a variety of information sharing platforms co-exist involving different purposes<sup>210</sup>, however, these provide a mere voluntary participation

An interesting initiative was undertaken in an Italian PPP context, where business operators, academia and intelligence created a new technology center called “*malware laboratory*” in November 2015, in order to share experiences and information and to develop capacity in the field of malware reverse engineering<sup>211</sup> (see also 6.2.4 ).

Finally, we have to mention the Crisis Management Network (*Rete di gestione della crisi* – RGCC). It is a project for a national net of information sharing between all the public actors of the cybersecurity, mentioned in 6.2.1 (see under section “DPCM January 24<sup>th</sup>, 2013).

### 6.2.3 Italian Civil Protection

At EU level, Civil Protection is hinged in the European Commission's Humanitarian Aid and Civil Protection department (ECHO)<sup>212</sup>, it was set up to support a coordinated and quicker response to disasters both inside and outside Europe using resources from the countries participating in the *European Union Civil Protection Mechanism* and is divided into units:

- *Emergency Response*: This unit is responsible for response and international cooperation, including the *Emergency Response Coordination Centre* (ERCC)<sup>213</sup>. It is responsible also for managing (a) the ERCC' operations, (b) the *Common Emergency Communication and Information System* (CECIS); (c) missions of experts, (d) it takes care of the transport provision and (e) of monitoring and sharing of early warning.
- *Policy prevention*: this unit is responsible for the development of a Community framework of prevention. It care preparation activities including training courses, simulation exercises, promotion of exchange of experts, development of new training programs ext.

At Italian level the Civil Protection Department (CPD) is hinged in the Presidency of the Council of Ministers Office. It was founded in 1982 in order to provide the country with an organisation able to mobilize and coordinate all national resources useful to ensure

<sup>209</sup> COM(2006) 787 final, Brussels, whereas 14.

<sup>210</sup> It refers to the following platforms: (a) CIWIN, see text above; (b) TNCEIP, specifically focus on the energy sector; (c) EP3R *European Public-Private Partnership for Resilience*, established in March 2006 by the European Commission in order to increase information sharing between private and public actors at a European level, see also D 7.3 page 5.

<sup>211</sup> See *Report on information security* 2015, introduced by the Italian Parliament Government according to art. 38, L. 2007/124, in <http://www.sicurezzanazionale.gov.it/sisr.nsf/archivio-notizie/un-framework-nazionale-per-la-cyber-security.html>

<sup>212</sup> ECHO was born after the introduction of the “solidarity clause”, art. 222 TFEU, see D 7.3 and D 7.9.

<sup>213</sup> See art. 7 Decision No. 1313/2013/EU of the European Parliament and of the Council on a Union Civil Protection Mechanism, in <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013D1313&from=EN> accessed on 3 Feb 2016.

assistance to the population in case of a major emergency<sup>214</sup>. Law Febr. 24<sup>th</sup> 1992, n. 225 has identified the CPD as the National Service of Civil Protection, with tasks to guide, promote and coordinate the entire emergency system. The CPD deals with all the activities for the risk prediction and prevention, the rescue and care of people affected by disasters, first response to emergency and overcome the emergency.

Through permanent working groups with representatives of the Central and Local Authorities, the CPD has an ongoing relationship with all the national components and the operating structure for the emergency response. Particularly, CPD has also the duty to coordinate the activities of first response to natural disasters, catastrophes or other events that, due to their intensity and extent, must be dealt with immediate intervention and with extraordinary powers and means. With the declaration of a state of national emergency by the Council of Ministers, it is up to the Head of the CPD to issue ordinances that will regulate the carrying out of the first interventions.

Among its powers, the CPD supports the civil protection voluntary work - as specifically provided by Presidential Decree n. 194/2001 - the promotion of initiatives for the dissemination of knowledge of civil protection and information to the public.

In summary, the CDP is competent to intervene for the prevention and for the management of all emergencies in the field of seismic risk, volcanic risk, tsunami risk, fire and environment risk, nuclear risk and health risk.

Recently the Law Decree May 15<sup>th</sup> 2012, no. 59 and Law July 12<sup>th</sup>, 2012 no. 100 have amended Law no. 225/1992, in order to strengthen the interventions in emergency management.

The reform in 2012 reaffirms the role of direction and coordination of the CPD and it redefines:

- The classification of disasters, the Civil Protection activities, the declaration of a state of emergency and the ordinance power;
- The first emergency phase, with emphasis on the "time factor", specifying that the "extraordinary powers" to deal with disasters should be used only as limited and predetermined: the duration of the state of emergency cannot exceed 90 days, with the possibility of extension to further 60 days. This "expire time" has been further amended by the Law 119/2013: the state of emergency may not exceed 180 days and can be extended up to additional 180 days.
- The state of emergency: it may be declared as "imminent" and not just "at the occurrence" of the adverse event and provides from the beginning to the identification of the competent "ordinary authority" that carries on the activities, after the expiration of a state of emergency.

Moreover, according to the 2012 reform the civil protection ordinances necessary to overcome the emergency are usually issued by the CPD Head and not by the Council of Ministers President.

---

<sup>214</sup> The rescue delay and coordination lack that characterized the management of a big earthquake in South Italy (Irpinia) in 1980 had, in fact, highlighted the need to establish a structure that took care permanently of the civil protection; see <http://www.protezionecivile.gov.it/jcms/it/dipartimento.wp.jsessionid=9533F77F7D47CA9CE0D143566736C031.worker1>.

#### 6.2.4 Public-Private Partnerships (PPP)

As outlined in D 7.3 version 1, many CIs are in private ownership; that's a key concern in the protection of Critical Infrastructures and hence the need for a strong and integrated public-private partnership.

In this context, the Italian experience is interesting since in March 2003 the Ministry of Innovation and Technology established a working group on CIIP where business representatives<sup>215</sup> and public sector representatives (Ministry and Academia) worked together in the analysis of the Italian ICIs situation.<sup>216</sup>

Moreover, Legislative Decree 1st August 2003, no. 259 - as amended by Legislative Decree 28th May 2012, no. 70 (implementation of Directives 2009/140/EC) - laying down the electronic communications code, in Art. 16a paragraph 4 provides for the IT CERT identification at the Ministry of Economic Development; IT CERT works in connection with Public Administration CERT (CERT-PA) and Defence-CERT; it is based on a PPP model and it supports individuals and businesses with tasks of prevention and response coordination in case of cyber events on a large scale.

Recently, in the last years (2014-2015), some other relevant working groups have been set up in form of a PPP. The DIS (Department for Information Security), based at the Prime Minister's Office, had led a Working Group on Cyber and Information Technology (WGC) and a Working Group connecting business and authorities (WGI).<sup>217</sup>

The tasks undertaken by WGC are:

- raising awareness on the issue of information security;
- collaboration with the Academy, that led to the presentation, on Febr. 4th 2016, of the "Italian Cybersecurity report".<sup>218</sup> It is a framework on Italian national cyber-security situation, edit by Academia, with the support of DIS and with the participation of private companies, some of which qualified as ICIs. The Report aims, inter alia, to give companies a benchmark for assessing their situation in front of cyber risks, suggesting appropriate standards which join on a purely voluntary basis.

The tasks undertaken by WGI are:

- Focus on the evolution of threats in the field of cyber terrorism and espionage;
- Focus on the main vulnerabilities of the Industrial Control System;
- "Technical dialogues": create opportunities for dialogue between engineers of strategic enterprises and the authorities, so that intelligence increases its information assets and businesses learn the most important threat trends, to increase their defences in a targeted manner;
- "Uses case": in the above context some seminars were held between intelligence, Security manager and ICT manager, in which they discussed "Uses case", in order to

<sup>215</sup> Inter alia: representatives of business communication technology (Telecom, and Wind); representatives of the Italian Banking Association (ABI, Associazione Bancaria Italiana).

<sup>216</sup> *Critical Infrastructure Protection: Threats, Attacks and Countermeasures* (Tenace project), page 11.

<sup>217</sup> National security document, page 7, attached to the *Report on information security* 2015.

<sup>218</sup> It is a framework on Italian national cyber-security, edited by R. Baldoni, L. Montanari, La Sapienza University (Rome) and the Cyber security National Lab (an Inter-University Consortium – CINI), with the support of DIS.



allow the rapid detection of the threat and to prevent, or at least to slow down, its propagation.

From the above exchange, in the second half of 2015, a portal has been implemented in order to ease information sharing. This portal will use quantitative analysis and correlation tools in order to exploit the information assets.

Moreover, that working group creates opportunities for bilateral B2B meetings to deal with specific issues.

Additionally, there were also some meetings between the two working groups due to cross-cutting issues. The first meeting was in March 2015, with the representative of NATO, on the occasion of the presentation of the NATO *Enhanced policy on Cyber Defence*; the second one in December 2015 for the discussion of two issues: (a) the contents of the proposal of the NIS directive; (b) the so called *contractual Public-Private Partnership*, in the context of the *Digital Single Market Strategy* (DSM)<sup>219</sup>.

A further initiative to facilitate the partnership between business operators, academia and intelligence was the “ICT 4INTEL 2020” in November 2015, in which a new technological center was presented, where the 3 above mentioned institutions will cooperate in a so called “*malware laboratory*”, in order to develop capacity in the field of malware reverse engineering<sup>220</sup>.

As a conclusion we can state that the information sharing is pursued in a PPP perspective in Italy mainly through working groups.

In this regard it is worth remembering what was already said in section 6.2.1 DPCM ; January 24th, 2013 (the so called *Decreto Monti* (*Monti Decree*, now replaced by DPCM 17th February 2017) embedded ECIs and ICIs’ Private operators in the architecture for the national cybernetic security, establishing that those who providing public communications networks or electronic communications services to the public shall: (a) notify the NIS of any significant breach of security or integrity of its information systems, using secure transmission channels; (b) *adopt best practices*; (c) provide information to the media organizations for safety and allow them access to databases for the purposes of cybersecurity respective relevance, when required by law no. 124/2007 (law on State secret, see chapter 3.1); (d) collaborate in the cyber crisis management by helping to restore the functionality of the systems and they managed networks.

Moreover, we have to recall here, that DPCM 17th February 2017 has improved PPP; in fact, that, due to art. 11, CI private operators shall communicate to the NSC any significant security breach, using secure transmission channels; shall collaborate in the management of cybercrime and shall helping to restore the functionality of systems and networks managed by them.

---

<sup>219</sup> “On 6<sup>th</sup> May 2015, the European Commission adopted the DSM, which establishes a Public-Private Partnership (PPP) on cybersecurity in the area of technologies and solutions for online network security during 2016. The PPP will be a contractual arrangement between the Commission and an industrial grouping, both of which are committed to supporting, in the EU Horizon 2020 programme, research and innovation activities of strategic importance to the Union competitiveness in the cybersecurity field”. See <https://ec.europa.eu/digital-single-market/en/news/public-consultation-public-private-partnership-cybersecurity-and-possible-accompanying-measures>.

<sup>220</sup> See *Report on information security* 2015.

### 6.2.5 Disaster Management and Italian CIP Mechanisms

Recalling here what we said in section 6.2.3 about the role, functions and operating models of the CPD, we have now to further add and clarify the concrete operating model of prevention and intervention in emergency situations.

In 6.2.3 we mentioned Law July 12<sup>th</sup>, 2012 no. 100, that reformed CPD. According to that regulation, the Mayor of a Municipality is the CPD local representative. Within 90 days from the enactment of above mentioned law, every Municipality must have prepared an “emergency plan”, according to the directives of the CPD. That plan consists in the development of operational procedures to deal with any disasters, including (i) the coordination of the relief operations and assistance to the population and (ii) the control/reduction of the negative effects of the disaster.

Moreover, specific procedures are provided by the Ministry of Culture, Art and Tourism for the safety and protection of the cultural and artistic heritage, through the action of local crisis units, led by a national crisis unit with the coordination of CPD.<sup>221</sup>

With specific reference to Italian CIP mechanism, recalling what we said in 6.2.1 we have to remember the following partition of skills and accountability, according to legislative decree 61/2011, mentioned above:

- NISP: is a planning group for the ICI identification. It is composed by representatives inter alia of the Ministry of Internal Affairs, the Ministry of External Affairs, the Ministry of Defense, the Ministry of Infrastructure and Transport, the Ministry of Economic Development, DIS, AISE, AISI, CPD and firefighters. The group meets at least once every 2 months (art. 5, DPCM May 5th 2010, titled: National Organization for crisis management, art. 4, legislative decree 61/2011). For the matters linked to civil defense, the NISP acquires the prior opinion of the Ministry of the Internal Affairs and for the matters linked to civil protection, the NISP acquires the CPD prior opinion.
- “Competent Body” (CB): is appointed by Prime Ministerial Decree and works as a scientific and technical support to NISP. Taking into account the guidelines developed by the European Commission, the CB determines the extent of sectorial criteria according to which the infrastructure can be considered potentially critical (art. 4 and art. 5, legislative decree 61/2011). The CB, moreover, keeps the NISP informed and:
  - (a) communicates the identification of an potential ECI to the representatives designated by other Member States which may be significantly affected, in national territory as well as the reasons that could lead to their designation as ECI;
  - (b) receives, from the other Member State, the communication of identified potential ECI in foreign territories, of which Italy could be affected;
  - (c) starts bilateral or multilateral discussions with representatives of Ministry of Internal Affairs, Ministry of External Affairs, Ministry of Defence, CPD and the representatives of other Member States in order to verify if an infrastructure is really “critical”;
  - (d) receives any communications from the European Commission.

Subsequently, on a proposal from the CB, the NISP gives or denies its consent on the classification of an Italian infrastructure<sup>222</sup> as “critical”. Then that infrastructure is designated as CI by the Council of Ministers President.

<sup>221</sup> See Directive December 12<sup>th</sup> 2013 emended by Directive April 23<sup>th</sup> 2015, in <http://www.beniculturali.it/mibac/export/MiBAC/sito-MiBAC/MenuPrincipale/Normativa/Direttive/index.html>.

<sup>222</sup> It means “an infrastructure located in Italian territory”.

CB informs the European Commission about the number of ICs located on the Italian territory and, with regard to ICs not located on the Italian territory, after the bilateral/multilateral meetings with the Member States concerned, CB prepares the agreement to be signed in order to designate that infrastructure as ICE (art. 8 and art. 10 legislative decree 61/2011).

## 6.3 Legal Framework for Information Sharing

### 6.3.1 *Criminal law - Implications for data sharing in disaster situations*

Information sharing in disaster situations may have two kind of side effects in the light of criminal law.

#### (A) Public perspective

From this point of view, information sharing in disaster situation may configure a case of agreement with the foreign State against Italian State interests and this is sanctioned by the Italian Penal Code (art. 243 ff). Information sharing may also configure a violation of State secrets, sanctioned by Law Aug. 3th, 2007, no. 124, art. 39 ff.

Such situations can occur both, with regard to private ECIs and public ECIs, being sufficient that a breach of confidentiality is made by one of the operators.

#### (B) Private perspective

In a private perspective, i.e. even if the confidentiality breach did not go against the interests of the Italian State, information sharing could constitute the following criminal offense:

- (a) The unauthorized access to a computer system is a criminal offense (art. 615 ter Italian Penal Code), the offense is committed if anyone enters illegally in a computer system protected by security measures. That provision was introduced in 1993 (L. Dec. 23th 1993, no. 547, art 4), implementing the Recommendation of the EU Council (89)9, Sep. 13th 1989;
- (b) Illegal possession and sharing access codes to computer or telecommunications systems. However, the crime is committed only if the spread of the access codes is done in order to obtain a profit for themselves or others or to cause damage to others (art. 615 quater Italian Penal Code);
- (c) Disclosure of secret documents or a professional secrecy. However, the crime is committed only if the disclosure is accomplished without cause (art. 621 and 622 Italian Penal Code);
- (d) Disclosure of scientific or industrial secrets: Anyone who comes to know, by reason of their status or office, or of his profession or art, news to remain secret, above discoveries and scientific inventions or industrial applications, and reveals or uses them in its own or another's benefit, shall be punished by imprisonment up to two years (art. 623 Italian Penal Code).

So, in an ECOSSIAN perspective, it's clear that information sharing could well lead to criminal offence, where such diffusion is not justified by an overriding public interest. However, as the ECOSSIAN normally is not unauthorized accessing the system, nor sharing information without agreement of the operator, this should not be applicable to it.

### 6.3.2 *ICT Specific Legal Frameworks*

The purpose of this section is to analyse the Italian ICT specific legal frameworks in the light of the European framework seen in D 7.3 – Version 1.

It is known that “To accompany the opening up of the telecommunications market to competition, the European Union (EU) has adopted a regulatory framework with regard to electronic communications in line with technological progress and market requirements”<sup>223</sup>. For this aim the European Union adopted in 2002 the so called ‘Telecoms Package’, amended in 2009. This package includes<sup>224</sup> two important Directives in ECOSIAN prospective:

- Directive 2002/21/EC “on a common regulatory framework for electronic communications networks and services”, the so called ‘framework directive’
- Directive 2002/58/EC “Directive on privacy and electronic communications”

The Directive 2002/21/EC “framework directive” seeks primarily to stimulate investment and foster freedom of choice for consumers (innovative services and lower rates). As outlined in D 7.3 – Version 1, the operations of ECOSIAN remain outside the scope of Directive since ECOSIAN is neither a public communications network nor a service provider. However, it is interesting to note that the Directive lays down the tasks of the national regulatory authorities (NRAs), as well as the principles underpinning their operations; inter alia, NRAs have to promote the interests of European citizens by helping to ensure a high level of protection of personal data and privacy by ensuring the security of communications networks. It is significant how these two requirements are increasingly mentioned in EU sources governing the electronic communications field, as well as in Directive 2002/58/EC “*Directive on privacy and electronic communications*”. In Italy, according to art. 32 *bis*, Legislative Decree no. 196 of 30<sup>th</sup> June 2003: (1) “*In case of a personal data breach, the provider of publicly available electronic communications services shall notify the said breach to the Warrantor without undue delay.* (2) *When the personal data breach is likely to be detrimental to the personal data or privacy of the contracting party or another individual, the provider shall also notify the contracting party or the individual of the said breach without delay (unless for anonymous data).* (5) *The notification to the contracting party or individual shall at least include a description of the nature of the personal data breach and the contact points where additional information can be obtained, and shall list the measures recommended to mitigate the possible detrimental effects of the personal data breach. Additionally the notification to the Warrantor shall describe the consequences of the personal data breach and the measures proposed or taken by the provider to remedy the breach.* (7) *Providers shall keep an updated inventory of personal data breaches including the circumstances of the breach, its consequences, and the measures adopted to remedy the breach, in such a way as to enable the Warrantor to verify compliance with the provisions laid down herein. The inventory shall only include the information that is necessary for this purpose.*

<sup>223</sup> <http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=URISERV:I24216a&from=IT>.

<sup>224</sup> Indeed, Telecoms Package includes one framework directive’, Directive 2002/21/EC “on a common regulatory framework for electronic communications networks and services (see above) and four ‘specific’ Directives which regulate specific aspects of electronic communications, as well as two Regulations: Directive [2002/20/EC](#) or ‘[Authorisation Directive](#)’; Directive [2002/19/EC](#) or ‘[Access Directive](#)’; Directive [2002/22/EC](#) or ‘[Universal Service Directive](#)’; Directive [2002/58/EC](#) or ‘[Directive on privacy and electronic communications](#)’ (see above); Regulation (EC) No. [1211/2009](#) establishing a [Body of European Regulators for Electronic Communications \(BEREC\)](#); Regulation (EU) No. [531/2012](#) on [roaming on public mobile communications networks](#), see <http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=URISERV:I24216a&from=IT>.

## 6.4 Legal Barriers to Information Sharing

### 6.4.1 Data Protection Requirements

In D 7.3 – Version 1<sup>225</sup>, we saw that Directive 95/46/EC requires a legitimate ground for processing personal data and this “legitimate ground” can be found in art. 7, where it is stated that Member States shall provide that personal data may be processed only if (*inter alia*): c) processing is necessary for compliance with a legal obligation the controller is subject to; e) processing is necessary for the performance of a task carried out in the public interest (i.e. the disaster management); f) processing is necessary for the purposes of the legitimate interests pursued by the controller.

In Italy, Directive 95/46/EC was implemented by Legislative Decree no. 196 of 30th June 2003; with regard to information sharing in disaster situation, art. 24 reproduces article 7 (at least in part), so personal data may be processed even if data subject doesn’t give his/her express consent *inter alia* in the following cases: a) it is necessary to comply with an obligation imposed by a law, regulations or Community legislation; e) it is necessary to safeguard life or bodily integrity of a third party; g) it is necessary to pursue a legitimate interest of either the data controller or a third party.

Moreover, according to art. 18 (2), Public bodies shall only be permitted to process personal data in order to discharge their institutional tasks. (4) Subject to the provisions of Part II as applying to health care professionals and public health care organizations, public bodies shall not be required to obtain the data subject’s consent. So public bodies, exercising their duties, may process personal data without the data subject’s consent.

Moreover, according to art. 8 and 53 of the Legislative Decree no. 196 of 30th June 2003, data subject can’t exercise the fundamental rights on processing (e.g. updating, rectification, erasure) if the personal data are processed, *inter alia*, by Public Security Department or by the police, or by other public bodies or public security entities for the purpose of protecting public order and security, and in general for the purposes related to the exercise of police tasks to prevent crime.

Accordingly, thanks to the above mentioned provisions, the Italian system is sufficiently flexible to enable information sharing in disaster situation.

### 6.4.2 Requirements in Intellectual Property Law

In D 7.3 – Version 1<sup>226</sup> we saw why Intellectual Property Law (IPL) may be interesting from an ECOSSIAN perspective: to respond to a disaster situation information sharing incorporating intellectual property (IP) may be required. We saw also that IPL stems from a combination of international treaties, EU legislation and national provisions.

Also the Italian provisions were adopted or have changed over time in total harmony with the European standards.

With regard to IP we have to distinguish between:

- a) corporate information and technical-industrial experiences, i.e. confidential information for anti-competitive purpose;
- b) patent and software;
- c) database.

---

<sup>225</sup> See D 7.3, page 30 ff.

<sup>226</sup> See D 7.3, page 35 ff.



Intellectual Property Code<sup>227</sup> in art. 98, 99 states that corporate information and technical-industrial experiences are protected if they have the 3 following features:

1. They are information objectively “secret”, that is not known and not easily accessible to anyone;
2. They have commercial value because they are secret;
3. They have been subject to reasonable steps, under the circumstances, to keep it secret.

As evident, it is almost perfectly overlapping with the conditions as foreseen in the proposal for a Directive on the trade secret protection we saw in D 7.3 – Version 1<sup>228</sup>.

Moreover, with reference to the subcontracting cases, i.e. work for third parties where the customer provides the technical specifications necessary to perform the job, Law June 18th, 1998, no. 92 states that *“the customer retains ownership of industrial projects and technical specifications communicated to the supplier. The supplier is required to maintain the confidentiality of such information”* (art. 7).

With regard to software protection, Italian regulation, Legislative Decree Dec. 29th, 1992, no. 518, was based upon Directive 1991/250/EC, replaced by the Directive 2009/24/EC; the above mentioned Legislative Decree has amended the law on copyright (April 22th, 1941, no. 633) and it extended the protection provided by the Berne Convention<sup>229</sup> for literary and artistic works to the software.

Accordingly, in order to protect software by using the so called “copyright approach”, it is necessary that the requirement of creativity is fulfilled, i.e. it must be the expression of a personal and original idea turned into “something new” (song, book and precisely software).

In order to ensure a high level of protection for software the Italian legislature opted for the so called “copyright approach” instead for patent. In fact the patent requires the most restrictive requirement of “industrial applicability”. Moreover the software author is entitled to the moral rights and exploitation rights, which last throughout the author's life and up to 70 years after his death (art. 25 L. April 22th, 1941, no. 633); while patent protection has an expiration time of 20 years (L. decree 2005/30, art. 60).

Also databases are protected by the copyright law, April 22th, 1941, no. 633, as amended by implementing Directive 96/9/EC (Database Directive). According to the EU provision, in the Italian regulation we can distinguish: (i) database that may be considered an “intellectual creation” (art. 1): the ‘originality’, i.e. the creative character is to be revied in the criterion the information has been ordered with. The provided protections are similar to those applied to the software (art. 64 bis); (ii) sui generis Database right: the database maker has the right to prohibit to extract or reuse all or a substantial part thereof. The right lasts 15 years after January 1st of the year following the date of the database completion (art. 102 bis).

	REQUIREMENT	OBJECT	EXPIRATION TIME	REGULATION
<b>SOFTWARE</b>	Creativity	- author moral right - copyright	70 years after author's death	L. 1941/633, art. 25
<b>DATABASE</b>	Creativity	Copyright	70 years after	L. 1941/633, art. 64 bis

<sup>227</sup> Legislative Decree Febr. 10<sup>th</sup>, 2005, no. 30.

<sup>228</sup> See D 7.3, page 42.

<sup>229</sup> The Berne Convention was adopted in Italy with Law June 6<sup>th</sup>, 1978, no. 399.



	REQUIREMENT	OBJECT	EXPIRATION TIME	REGULATION
<b>COPYRIGHT</b>			author's death	
<b><i>Sui generis</i> DATABASE</b>	substantial investment	Sui generis right	15 years after January 1 <sup>st</sup>	L. 1941/633, art. 102 bis
<b>PATENT</b>	industrial applicability	- author moral right; - copyright	20 years	L. decree 2005/30, art. 45 and 60

Table 10: Overview Italian IP legislation

From an ECOSSIAN perspective we must point out that any copyrights or sui generis rights are not fully applicable to public safety according to EU regulation (Directive 2001/29/EC, art. 5; Directive 96/9/EC, art. 6 and 9) and according to the Italian Law:

	REGULATION
<b>SOFTWARE</b>	L. 1941/633, art. 67
<b>DATABASE COPYRIGHT</b>	L. 1941/633, art. 64 sexies b)
<b><i>Sui generis</i> DATABASE</b>	L. 1941/633, art. 71 quinquies
<b>PATENT</b>	L. decree 2005/30

Table 11: Limitation of IP rights in Italian legislation

### 6.4.3 Confidentiality obligations

As we know, the information dissemination can be limited using specific contractual clauses, named “Confidentiality” or “Non-Disclosure” clauses (or “Non Disclosure Agreement”, NDA); indeed we know that, in practice, these clauses are generally contained in all B2B agreements, but they may concern also employment contracts: between employers and the workforce to prevent the worker from spreading confidential information in the course of his employment and for anti-competitive purpose, after the employment period.

Italian Civil Code (art. 2015) states that the worker cannot divulge information concerning the organization and production methods. In a wide sense this means that the worker should be loyal to the employer, so the employee must not make unfair competition to the employer, using the knowledge gained during his employment.

Those provisions can also be arranged in the “search contracts”, with regard to (i) the information that the employer must provide the researcher so that they can fulfil their assignment; (ii) the to the results of the research activity<sup>230</sup>. A breach of obligation may give the other party the right to terminate the agreement and recover damages.

So, in addition to what we saw in 6.4.1 and 6.4.2, NDAs are mere agreements between the parties, which may be extended to third parties entering the agreement a commitment to sign the confidentiality clause to anyone who contracts with the original parts.

<sup>230</sup> According to art. 65 Legislative Decree Febr. 10<sup>th</sup>, 2005, no. 30, when the employment relationship is between the researcher and an university or a public research center, the researcher is the exclusive owner of the rights deriving from the patentable invention they are the author of.

All these clauses, it is worth repeating it, are mere agreements, therefore they cannot derogate the mandatory law rules; this means that (i) *ECI owner/operator and indeed everybody “should abide by any contractual obligations in order not to share confidential information as contained for example in Non-Disclosure Agreements”<sup>231</sup>*; (ii) the parties agreement may well be exceeded by a provision of law requiring information sharing.

## 6.5 Impact on ECOSSIAN

This section aims to value the impact of the Italian system on ECOSSIAN.

Indeed, as we saw, in most cases Italian law is not so different from EU provisions, rather in many cases it is the exact implementation of EU Directives. So nowadays we may say that the Italian system has no special characteristics such as involving special criticality in an ECOSSIAN perspective.

### 6.5.1 About the Italian Demo

The Italian demo is based, essentially, on the functionality of a malware. The assumption is that the employees of a financial CI receive a fake e-mail, promoting holidays. One employee downloaded the malware, then credentials to access the intranet are stolen and design vulnerabilities are detected. Exploiting such vulnerabilities with a suitable designed malware allows the fraudster to publish a malicious document into the corporate portal, whose massive download takes new internal users to be infected and the network structure to be identified.

However, the malware is detected by the ECOSSIAN sensors, so the O-SOC can detect the threat, rate it as relevant and share it with N-SOC, asking for more information. N-SOC can warn E-SOC and other CI if it rates the event as relevant for all EU financial CIs.

In that use-case the financial CI does not have to share any information about customers, so they have no problems regarding data protection, but O-SOC could detect an IP address from which malware might be coming from and it might be useful to communicate the IP address to the N-SOC in order to allow information sharing among CIs to prevent the spread of malware. We know that even the IP address may be considered as personal data within the meaning of Directive 95/46/EC, art. 2 (a)<sup>232</sup>. The same can be said with regard to the GDPR. We also know that GDPR (and the Directive) do not apply to the processing of personal data “by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security” (art. 2, par. 2d).

The purpose of the O-SOC, sharing the information about the IP address, is exactly the one indicated above, but are O-SOC/N-SOC “competent authorities”?

---

<sup>231</sup> See D 7.3, page 43.

<sup>232</sup> Court of Justice, in “Breyer decision”, C-582/14, 19th October 2016, in <http://curia.europa.eu/juris/document>, said that, according to “Article 2(a) of Directive 95/46/EC [...] on the protection of individuals with regard to the processing of personal data and on the free movement of such data must be interpreted as meaning that a dynamic IP address registered by an online media services provider when a person accesses a website that the provider makes accessible to the public constitutes personal data within the meaning of that provision, in relation to that provider, where the latter has the legal means which enable it to identify the data subject with additional data which the internet service provider has about that person”.

We can find the meaning of the expression “competent authorities” in Directive 2016/680/EU of April 27th 2016<sup>233</sup>, on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, art. 3, n. 7, lett. b) “For the purposes of this Directive, competent authority’ means: any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security”. So each Member State could attribute that qualification to the O-SOC and to the N-SOC; in that case, obviously, it must comply with Directive 2016/680/EU, including the obligation to notify the data breach (art. 30, see also art. 40 about information sharing).

In case O-SOC and N-SOC are not considered competent authorities, we also have to consider that processing by O-SOC and N-SOC can be qualified as i) “necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller”, due to art. 6 lett. e) GDPR; or ii) as “necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child”, due to art. 6 lett. f) GDPR.

---

<sup>233</sup> The directive is in force since 5th May 2016, but the Member States have two years to implement it. Italy has not implemented it yet.

## Chapter 7 Impact on ECOSSIAN/Evaluation

In D7.3 requirements were specified. Not all requirements can be addressed within the scope of work in the ECOSSIAN project and might need to be addressed on an organisational level when the ECOSSIAN System would be implemented.

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

Applied Req.	Description	Evaluation
AReq. 1.1	All communications should be encrypted	Considering the evaluation of REQ 4.4.7 in D7.6 and D5.6, this requirement can be considered as mostly fulfilled, since all communication using the secure gateway is encrypted. Communication inside the respective SOC's is excluded from the test, but in a final implementation of ECOSSIAN also this communication should be encrypted if classified data is exchanged.
AReq. 1.2	Personal data are only transmitted as frequently as necessary for the system to operate and any such transfer should be encrypted and anonymised	Considering the analysis of REQ 4.4.1 in D7.6 the function of a human operator is introduced which controls manually which data should be sent. Properly executed, this will ensure data minimisation. Support can be provided with a previous DPIA, to assess what kind of data may be involved within this entity, and which data possibly may be sent out, as well as guidelines for the human operator. Finally an automatic anonymization function provides automatic hashing of IP addresses and operator information, therefore minimising the risk.
AReq. 1.3	Systems should be designed to ensure that even where personal data are transmitted, any data elements which are not necessary to fulfil the purpose of the transmission are filtered out or removed.	Considering the analysis of REQ 4.4.8 in D7.6 and D5.6, this requirement can be considered as in principle fulfilled, since at the SGW, data transmitted between layers, can be filtered manually by an operator. An automatic anonymization feature is implemented for emails and IP addresses, pseudonymising this data.
AReq. 1.4	Systems should be designed so as to allow access to the transferred personal data only to the extent necessary for the role being	Considering the analysis of REQ 4.4.9 in D7.6 since the inclusion of ABE allows for limited access based upon set

Applied Req.	Description	Evaluation
	performed.	requirements, this requirement can in principle be considered fulfilled. However, the establishment and verification of requirements for receiving access is essentially an organisational one, which needs to be considered in an organisational setup of ECOSSIAN. At the moment ECOSSIAN in principle provides for access on an entity level, however, for certain information it will be necessary to ensure only access on personal level (person with required security clearance) and in this case privacy features should be considered. This can only be ensured on an organisational level and is currently out of the scope of ECOSSIAN.
AReq. 1.5	If possible, systems should be designed in separate compartments; this strategy calls for distributed processing instead of centralised solutions; in particular the ENISA suggests to store data in separate database, and these databases should not be linked.	There is no one database for the whole of ECOSSIAN, instead databases at the different SOC levels are envisaged. However, even at the different SOC levels it would be useful to allow for separate databases, depending e.g. on whether personal data is included, different deletion timeframes, confidentiality levels etc. This is at the current point not included in the project, however, it would be useful to consider it in a future implementation.

Table 12: Applied Requirements Table I

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

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

Applied Req.	Description	Evaluation
AReq. 2.1	All entities utilising the ECOSSIAN system should licence the use of any IP works being shared within the purposes of Critical Infrastructure protection.	This is a requirement for a potential implementation of the ECOSSIAN system and can therefore not be assessed.
AReq. 2.2	All information shared through ECOSSIAN should automatically be treated as confidential.	This requirement should be reevaluated as possibly different classification levels could be included, whereby the potential application of Freedom of Information legislation and whether this provides a hurdle for information sharing should be evaluated. However, the level of classification is also an organisational question and should be ensured via

Applied Req.	Description	Evaluation
		agreements.
AReq. 2.3	All unnecessary information that is transferred should be deleted and should not be used for non-critical infrastructure protection purposes.	Considering the introduction of the human operator, the possibility exists to delete all unnecessary information before transfer, and also at every SOC level. Ensuring that information will not be used for other purposes will only be possible on an organisational level, possibly with contractual obligations.
AReq. 2.4	Systems should be designed so as to only allow access to select persons to reduce the confidentiality concerns.	See evaluation of D7.6 REQ 4.4.9 and AReq 1.4.

Table 13: Applied Requirements Table II



## Chapter 8 Guidelines

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

Guid. No.	Description	Comment	
Guid. 1	Identify and coordinate with the relevant national critical infrastructure protection authority.		Relevant for an organisational ECOSSIAN implementation
Guid. 2	Consult specific national laws for reporting requirements and consider the overlap between disaster management and critical infrastructure protection frameworks and agencies.	Due to the level of disparity, this consultation is necessary in order to decipher the relevant obligations.	Relevant for an organisational ECOSSIAN implementation
Guid. 3	Refer to the specific privacy and data protection implementation guidelines described in D7.2 'Legal requirements'.	This would ensure a legally compliant ECOSSIAN solution.	Addressed during the project, however, certain requirements will need to be addressed in an organisational ECOSSIAN implementation, see D7.6.
Guid. 4	Conduct a privacy and data protection impact assessment.	This ensures that the fundamental rights to data protection and privacy of the data subjects concerned are sufficiently taken into account.	This has been addressed in D7.6, and is recommended to be done per CI provider and also for the full ECOSSIAN system when implementing the ECOSSIAN system.
Guid. 5	Conduct impact assessments regarding IP rights.	This allows the identification of any IP rights holders.	Relevant for an organisational ECOSSIAN implementation
Guid. 6	Designate specific person(s) with the authority to reveal trade secrets in the event of a disaster.	This avoids confusion amongst employees, and a defined operational structure creates a clear division of responsibilities.	Relevant for an organisational ECOSSIAN implementation
Guid. 7	Integrate non-disclosure agreements for all employees above a certain level with access to sensitive information and provide guidance to clarify responsibilities.		Relevant for an organisational ECOSSIAN implementation

Table 14: Guidelines

## 8.1 Human operator guidelines

In cooperation with the DOGANA project, a first draft outline of human operator guidelines to support the human operator in the task have been drafted. However, these guidelines are still in a general way phrased and need to be further adjusted per CI provider. The DPIA can be useful in this regard, in order to identify personal data processed in the CI operators system and to provide the human operator with specific guidelines on which data may be shared and which shouldn't. Possible lines for future research would be automatic personal data recognition tools, which could support the human operator in the task of recognizing and possibly deleting personal data included in the files. The ongoing project DOGANA will further develop the guidelines for their system based on the feedback of trial partners in DOGANA.

For ECOSSIAN the initial points for guidelines are outlined below:

For the CI provider it is important to consider that, especially depending on the employed surveillance systems, national rules need to be adhered to and possibly approval from certain bodies, e.g. the work council, will be required.

When the CI provider becomes part of the ECOSSIAN system, an agreement will need be entered into, which ensures certain requirements relating to e.g. the lawfulness of the shared data, confidentiality requirements etc. are adhered to.

For the Human Operator the guidelines are outlined below as a code of conduct / ethics / manual for the task of the Human Operator. However, these guidelines should always be adapted to the specific CI environment.

Below a number of initial pointers is listed.

Pointers for Human Operators:

- Information gathering stage:
  - Data gathering itself (is here already a first machine-based selection of relevant data?):
    - Goal only NIS data (personal data allowed if necessary, but not encouraged)
    - Only non-sensitive personal data (be careful e.g. especially in Finance/Health environments)
    - In case personal data is included, pseudonymization where possible
  - Data analysis [before transfer to the N-SOC]> mainly manual, thus: verify the gathered information for their relevance, lawfulness and legitimacy:
    - Selection of the relevant data based on the scope and goal of the assessment
      - ➔ delete all personal data that is not relevant for threat detection/mitigation
    - Not exceeding the legal limitations,
      - ➔ ensure that no business secrets/confidential information will be shared
    - Focus on whether the data can be used to detect/mitigate threats by others (e.g. Information about an employee who falls for phishing mails not relevant outside the company)
  - Data processing/transfer:
    - Interpretation of the results, add additional information
    - Select confidentiality level and required attributes of receiving entities
    - Possibly tag personal data, indicate deletion timeframe

## Chapter 9 Conclusion

To conclude, this deliverable has outlined the requirements and policies associated with information sharing in disaster situations in the context of ECOSSIAN. It has built upon the work completed in D7.1 “Analysis of the applicable legal framework”, D7.2 “Legal requirements” and D7.3 “Information sharing policies in disaster situations – Version 1” and has provided insights into the application of the general requirements provided for by the legislation, updating D7.3 and extending it with an overview of new legislation and its impact on ECOSSIAN, insight in the information sharing with law enforcement, confidentiality obligations and a complete analysis of the Italian legislation. Furthermore, it has also provided insights in the form of requirements and guidelines.

## Chapter 10 List of Abbreviations

Abbreviation	Description
AISE	Italian Agency for the external information and security
AISI	Italian Agency for the internal information and security
BIPT	Belgian Institute for Postal services and Telecommunication
BSI	Bundesamt für Sicherheit in der Informationstechnik
CECIS	Italian Common Emergency Communication and Information System
CERT	Computer Emergency Response Team
CI	Critical Infrastructure
CII	Critical Information Infrastructure
CIIP	Critical Information Infrastructure Protection
CIP	Critical Infrastructure Protection
CIWIN	Critical Infrastructure Warning Information Network
CPD	Italian Civil Protection Department
CoE	Council of Europe
DAE	Digital Agenda For Europe
DPA	Data Protection Act
EEAS	European External Action Service
ECHR	European Convention of Human Rights
ECI	European Critical Infrastructure
ENISA	European Network and Information Security Agency
EPCIP	European Programme for Critical Infrastructure Protection
ERCC	Emergency Response Coordination Centre
EU	European Union
GSC	General Secretariat of the Council
GDPR	General Data Protection Regulation
LEA	Law Enforcement Agencies
MLA	Mutual Legal Assistance
MSs	Member States
NIS	Network Information Security
NIS	Italian Nucleus for computer security (only used in Chapter 6)
NISP	Italian national Organisation for crisis management
NSC	Italian Nucleus for cybersecurity

Abbreviation	Description
PPP	Public Private Partnership
TEU	Treaty on European Union
TFEU	Treaty on the Functions of the European Union
WGC	Working Group on Cyber and Information Technology
WGI	Working Group connecting Business and Authorities

## Chapter 11 Bibliography

### 11.1 Primary sources

#### 11.1.1 Legislation

Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs, OJ L 122.

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

COUNCIL ACT of 26 July 1995 drawing up the Convention based on Article K.3 of the Treaty on European Union, on the establishment of a European Police Office (Europol Convention), OJ C316/38.

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

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

Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (InfoSoc Directive).

Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive) OJ L 108.

Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications networks and services (Authorisation Directive) OJ L 108.

Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive) OJ L 108.

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 on privacy and electronic communications) OJ L 201.

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

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

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly



available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105/54.

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

Regulation (EC) No. 1211/2009 establishing a Body of European Regulators for Electronic Communications (BEREC).

Regulation (EU) No. 531/2012 on roaming on public mobile communications networks.

Directive 2013/40/EU of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, OJ L 218/8.

Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, OJ L 257/73.

Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, OJ L 337/35.

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119/89.

Directive 2016/943/EU of the European Parliament and the Council of 8 June on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (Trade Secret Directive), OJ L 157/1.

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

#### national

##### *Germany:*

German telecommunications act: Telekommunikationsgesetz, Gesetz vom 22.06.2004 (BGBl. I S. 1190) zuletzt geändert durch Gesetz vom 23.12.2016 (BGBl. I S. 3346) m.W.v. 31.12.2016.

Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes (Sicherheitsüberprüfungsgesetz - SÜG).

Gesetz zur Erhöhung der Sicherheit Informationstechnischer Systeme (IT SicherheitsGesetz)

Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIg)

Bundesdatenschutzgesetz (BDSG)

##### *Netherlands:*

Dutch Telecommunications Act: Wet van 19 oktober 1998, houdende regels inzake de telecommunicatie (Telecommunicatiewet)

Besluit van 19 oktober 2012, houdende nadere regels met betrekking tot technische en organisatorische eisen ter beperking van risico's voor de veiligheid en de integriteit, de

meldplicht van inbreuken op de veiligheid en verliezen van integriteit, de verstrekking van informatie voor de beoordeling van de veiligheid en de integriteit en de aanwijzing van inbreuken op de veiligheid en verliezen van integriteit van openbare elektronische communicatienetwerken en -diensten (Besluit continuïteit openbare elektronische communicatienetwerken en -diensten)

*Draft 'Regels over het verwerken van gegevens ter bevordering van de veiligheid en de integriteit van elektronische informatiesystemen die van vitaal belang zijn voor de Nederlandse samenleving en regels over het melden van ernstige inbreuken (Wet gegevensverwerking en meldplicht cybersecurity)'*

Wet van 6 juli 2000, houdende regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens)

*Belgium:*

Belgian Electronic Communications Act: 13 JUNI 2005.- Wet betreffende de elektronische communicatie

*Italy:*

No. 124/2007, on State secret  
No. 100/2012 on Civil Protection Department  
No. 92/1998, on subforniture  
No. 633/1941, on intellectual property  
Italian Penal Code

Legislative Decree No. 174/2015  
Legislative Decree No. 70/2012  
Legislative Decree No. 61/2011  
Legislative Decree No. 30/2005  
Legislative Decree No. 196/2003  
Legislative Decree No. 259/2003  
Legislative Decree No. 518/1992

DPCM  
DPCM 5<sup>th</sup> May 2010,  
DPCM 24<sup>th</sup> January, 2013  
DPCM 5<sup>th</sup> December 2013  
DPCM 17<sup>th</sup> February 2017

### **11.1.2 Case law**

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

Case C-203/02 (*BHB v. William Hill*) CJEU 9 November 2004.

Case C-604/10 (*Football Dataco Ltd v. Yahoo! UK Ltd*), CJEU 1 March 2012.

Case C-293/12 - *Digital Rights Ireland and Seitlinger and Others* [2014] CJEU

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

*Klass and others v Germany* 5029/71 [1979-80] ECHR

*Leander v Sweden* 9248/8 [1987] ECHR

*Rotaru v Romania* 28341/95 [2000] ECHR

*Segerstedt-Wiberg and Others v. Sweden* 62332/00 [2006] ECHR

*Weber & Saravia v Germany* 54934/00 [2006] ECHR

*Dumitru Popescu v Romania* 49234/99 [2007] ECHR

*Kennedy v United Kingdom* 26839/05 [2010] ECHR

*Ekimdzhev v. Bulgaria* 22373/04 [2012] ECHR

*Uzun v Turkey* 10755/13 [2013] ECHR

## 11.2 Secondary Sources

Article 29 Working Party, Opinion 4/2007 on the concept of personal data, WP 136, 20 June 2007.

Article 29 Working Party, Working Document: Privacy on the Internet - An integrated EU Approach to On-line Data Protection, WP37, adopted on 21.11.2000.

Article 29 Data Protection Working Party Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector, WP 211, 27 February 2014.

Article 29 Working Party, Opinion 1/2010 on the concepts of "controller" and "processor", WP 169, 16 February 2010.

Belgian Standing Intelligence Agencies review Committee. (n.d.). *Legislation*. Available: <http://www.comiteri.be/index.php/en/legislation>. Last accessed 04/05/2017.

Brottsbalk (1962:700) Svensk författningssamling 1962:700

BIPT, Decision of the BIPT council of 1 April 2014 laying down the circumstances in which the operators have to notify BIPT of a security incident and the terms and conditions of this notification.

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

Commission Decision 2001/844/EC, ECSC, Euratom of 29 November 2001 amending its internal Rules of Procedure, OJ L 317, 3 December 2001.

Council Recommendation, Recommendation of the EU Council (89)9, Sep. 13<sup>th</sup> 1989.

Council Decision 2001/264/EC of 19 March 2001 adopting the Council's security regulations OJ L 101, 11 April 2001.

Council Framework Decision 2006/960/JHA on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union

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

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

Council Decision 2014/233/EU of 14 April 2014 amending Decision 2013/488/EU on the security rules for protecting EU classified information.

Council of the European Union, Handling of documents internal to the Council, 1136/11 (9.6.2011) and 10384/13 (31.5.2013).

Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information, OJ L72/53, 17 March 2015.

European Commission, Decision, 6<sup>th</sup> May 2015 on DSM, See <https://ec.europa.eu/digital-single-market/en/news/public-consultation-public-private-partnership-cybersecurity-and-possible-accompanying-measures>.

Position (EU) No 5/2016 of the Council at first reading with a view to the adoption of a Directive of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (2016/C 158/02)

Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL: on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data (COM(2012) 10 final 2012/0010 (COD))

COUNCIL RECOMMENDATION of 25 June 2001 on contact points maintaining a 24-hour service for combating high-tech crime (2001/C 187/02)

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 (COM(2010) 245 final/2)

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS: on Critical Information Infrastructure Protection - "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" (COM(2009) 149 final)

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS: on Critical Information Infrastructure Protection - 'Achievements and next steps: towards global cyber-security' (COM(2011) 163 final)

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

Council of Europe, Recommendation No. R (89) 9 on Computer-Related Crime.

Council of Europe, Recommendation R (95) 13 Concerning Problem of Criminal Procedural Law Connected with Information Technology.

COUNCIL OF EUROPE COMMITTEE OF MINISTERS EXPLANATORY MEMORANDUM to Recommendation No. R (87) 15 of the Committee of Ministers to member states regulating

the use of personal data in the police sector 1 (Adopted by the Committee of Ministers on 17 September 1987 at the 410th meeting of the Ministers' Deputies) .

Council of Europe, Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows (Ets No 181)

Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Ets No 108)

Council of Europe (2002) REPORT ON THE THIRD EVALUATION OF RECOMMENDATION N° R (87) 15 REGULATING THE USE OF PERSONAL DATA IN THE POLICE SECTOR

Curtin, D. "Overseeing Secrets in the EU: A Democratic Perspective: Overseeing Secrets in the EU," *JCMS: Journal of Common Market Studies* 52, no. 3 (May 2014): 684–700, doi:10.1111/jcms.12123.

Korff, D. (2002) EC Study on Implementation of Data Protection Directive, Cambridge UK, September 2002

Korff, D. (2008). *THE STANDARD APPROACH UNDER ARTICLES 8 – 11 ECHR AND ARTICLE 2* ECHR. Available: [http://ec.europa.eu/justice/news/events/conference\\_dp\\_2009/presentations\\_speeches/KORFF\\_Douwe\\_a.pdf](http://ec.europa.eu/justice/news/events/conference_dp_2009/presentations_speeches/KORFF_Douwe_a.pdf). Last accessed 04/11/2016.

ENISA (2011) A flair for sharing – encouraging information exchange between CERTs: A study into the legal and regulatory aspects of information sharing and cross-border collaboration of national/governmental CERTs in Europe (Initial Edition 1.0 November 2011)

ENISA (2012) Give and Take: Good Practice Guide for Addressing Network and Information Security - Aspects of Cybercrime Legal, Regulatory and Operational Factors Affecting CERT Co-operation with Other Stakeholders.

ENISA (2013) Marnix Dekker, Christoffer Karsberg, Technical guidance on the incident reporting in Article 13a. Version 2.0, January 2013.

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

ENISA (2013) The Directive on attacks against information systems: A Good Practice Collection for CERTs on the Directive on attacks against information systems (ENISA P/28/12/TCD, Version: 1.5, 24 October, 2013)

ENISA (2015) Information sharing and common taxonomies between CSIRTs and Law Enforcement (Final Version 1.0, PUBLIC DECEMBER 2015);

ENISA (2015) Electronic evidence - a basic guide for First Responders Good practice material for CERT first responders.

ENISA (2016), S. Anna, M. Konstantinos, 'Stocktaking, Analysis and Recommendations on the Protection of CILs', January 2016.

ENISA (2016) Dan Tofan, Konstantinos Moulinos, and Christoffer Karsberg, "ENISA Impact Evaluation on the Implementation of Article 13a Incident Reporting Scheme within EU," March 18, 2016

Eskens, Sarah, Ot van Daalen, and Nico van Eijk. (2015). *Ten standards for oversight and transparency of national intelligence services*. Available: <https://www.ivir.nl/publicaties/download/1591.pdf>. Last accessed 04/05/2017.

European Parliament (2011), 'Decision of the Bureau of the European Parliament concerning the rules governing the treatment of confidential information by the European Parliament', OJ C190, 20 June 2011.



European Parliament. (2017). *Fact Sheets on the European Union: Judicial cooperation in criminal matters*. Available: [http://www.europarl.europa.eu/atyourservice/en/displayFtu.html?ftuld=FTU\\_5.12.6.html](http://www.europarl.europa.eu/atyourservice/en/displayFtu.html?ftuld=FTU_5.12.6.html). Last accessed 05/05/2017

Decision No. 1313/2013/EU of the European Parliament and of the Council on a Union Civil Protection Mechanism, in <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013D1313&from=EN> accessed on 3 Feb 2016.

European Justice. (2015). *Freezing of assets and evidence*. Available: [https://e-justice.europa.eu/content\\_freezing\\_of\\_assets\\_and\\_evidence-93-en.do](https://e-justice.europa.eu/content_freezing_of_assets_and_evidence-93-en.do). Last accessed 04/05/2017.

European Justice. (2016). *Evidence*. Available: [https://e-justice.europa.eu/content\\_evidence-92-en.do](https://e-justice.europa.eu/content_evidence-92-en.do). Last accessed 04/05/2017.

Florian Skopik et al., “Collaborative Cyber Threat Intelligence – Creating, Sharing and Processing Security-relevant Information on National Level”.[forthcoming]

Galloway, D. “Classifying Secrets in the EU,” *JCMS: Journal of Common Market Studies* 52, no. 3 (May 1, 2014): 670, doi:10.1111/jcms.12122.

JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (JOIN(2013) 1 final)

Renato Rocha Souza, Flávio Codeço Coelho, Rohan Shah, Matthew Connelly: Using Artificial Intelligence to Identify State Secrets. CoRR abs/1611.00356 (2016), available at <https://arxiv.org/ftp/arxiv/papers/1611/1611.00356.pdf> (last accessed 6.4.2017).

Riksrevisionen (2015) It-relaterad brottslighet – polis och åklagare kan bli effektivare (RiR 2015:21);

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

### 11.3 Other

Italian *Report on information security* 2015

Italian Cybersecurity report, edited by R. Baldoni, L. Montanari, La Sapienza University (Rome) and the Cyber security National Lab (an Inter-University Consortium – CINI), with the support of DIS.

*Critical Infrastructure Protection: Threats, Attacks and Countermeasures*, final report of the TENACE project, funded under the *Relevant National Interest Research Projects* 2010 (PRIN 2010) by the Italian Ministry of the University and Research (MIUR), page 10

Berne Convention for literary and artistic works to the software

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

KPMG and CYBERSTREETWISE. (2015). *SMALL BUSINESS REPUTATION & THE CYBER RISK*. Available: <https://home.kpmg.com/content/dam/kpmg/pdf/2016/02/small-business-reputation-new.pdf>. Last accessed 04/05/2017.