A CIP-PSP funded pilot action
Grant agreement n°325188

Deliverable	**1.8.1 – Legal Requirements (first iteration)**
Work package	WP1
Due date	31-01-2014
Submission date	31-01-2014
Revision	
Status of revision	
Responsible partner	KU Leuven – B-CCENTRE
Contributors	Karine e Silva, B-CCENTRE, ICRI, KU Leuven Fanny Coudert, B-CCENTRE, ICRI, KU Leuven
Project Number	CIP-ICT PSP-2012-6 / 325188
Project Acronym	ACDC
Project Title	Advanced Cyber Defence Centre
Start Date of Project	01/02/2013

Dissemination Level	
PU: Public	X

PP: Restricted to other programme participants (including the Commission)	
RE: Restricted to a group specified by the consortium (including the Commission)	
CO: Confidential, only for members of the consortium (including the Commission)	

Version history

Rev.	Date	Author
1.1	2013-05-24	Draft EU legal analysis
1.2	2013-11-22	Draft National comparative analysis added
1.3	2014-01-24	Final Legal Analysis
1.4	2014-01-31	Editorial Corrections

Glossary

C&C	Command-and-control centre
CoE	Council of Europe
ECHR	European Convention on Human Rights
EU	European Union
ISP	Internet Service Providers
NIS	Network and Information Security
TFEU	Treaty on the Functioning of the European Union

Executive Summary

The ACDC project aims to provide an integrated strategy and full service offer for controlling cyber security problems that support criminal activities, particularly botnets. The project approach covers the full chain of an effective fight on botnets: from detection to protection of affected parties and identification of malicious users. To achieve this goal, botnet detection and prevention solutions will be provided to CERTs, Telecom operators / ISPs, owners of websites, and end users. The deployment of such tools in multiple lawyers of the information society and across different jurisdiction does pose significant legal obstacles. To this end, this document provides guidance on legal issues related to privacy encountered before the EU legal framework and the laws of selected Member States concerning the ACDC anti-botnet methods. A summary of the findings is provided below:

1. **Classification of IP addresses as personal data**. The processing conducted by the group tools raised the question on whether IP addresses should be regarded as personal data. No conclusive opinion exists at EU level on this matter since this assessment should be done on a case by case basis and depends on the circumstances of the event. Nevertheless, this study recommends partners to follow the opinion of the Article 29 Working Party which considers that IP addresses shall be treated as personal data in almost all situations.

2. Implementation of Article 7 of Directive 95/46/EC, with especial attention to paragraphs (a), (b), (c) and (f), including the interpretation of balance of interests between data controllers and data subjects. This analysis has revealed that the main legal barriers to the operation of 4 group tools, namely Network Traffic Sensors, Malware Website Analysis and the End Customer tools and Centralised Clearing Data House at EU level rely on the fulfilment of the legitimation grounds described under Article 7 of Directive 95/46/EC. The National Support Centre was considered out of the scope of the data protection framework, since it does not involve processing of personal data (ticket system enables anonymised support), nor traffic or location data by an ISP.

In order to process personal data, controllers must first justify their data processing activities on one of the legal grounds listed in article 7 of Directive 95/46/EC. Additional obligations refer to compliance with a series of principles such as: data quality principles of fairness, lawful and limited purpose, data minimization, data accuracy and storage limitation.

2.1 Implementation of Article 7(a) – End-customer tools. The End customer tools software and plugin will operate by consent, Article 7(a), Directive 95/46/EC, which will be collected from End-users prior to download. Partners must thus include all relevant information such as the purpose of sharing intelligence data with the Centralised Clearing Data House under the terms of use of the tool, and abide to all the requirements related to obtaining unambiguous user consent and respect to data subject rights, as described in this deliverable.

2.2 Implementation of Article 7(b)(c) – Network traffic sensors and Malicious or Vulnerable Website analysis tools. Article 7(b) may justify the deployment of networks sensors as well as the processing carried out by website malware analysis tools, in the circumstances described by the Article 29 Working Party in its Opinion 2/2006. In the view of the Article 29 Working Party, the setting up filtering systems by data controllers may be considered a step towards ensuring the performance and continuity of the service contracted by the customer with a reasonable level of security and confidentiality, characterizing thus a legitimate processing of the personal data involved in the operations.

In addition, Article 7(c) can also be used to legitimise the operations of these two group tools. The legal obligation enshrined under Art. 4 Directive 2002/58/EC and Article 17(1) Directive 95/46/EC for data controllers to provide security of their networks is in fact the most central element to justify the processing of personal data under ACDC for network sensors and malware website analysis. Malware mitigating solutions are essential tools in the protection of network security. To the that extent such mechanisms are used with the only purpose of safeguarding security of the network and in compliance with the data protection standards, the processing is likely to take place without further complications. One important aspect of the legal requirements is to ensure data subjects' information rights are being respected. This includes informing users in the terms of agreement of the service about the existence of sensors and the purpose of their placement.

2.3 Implementation of Article 7(f) – Centralised Clearing Data House. Article 7(f) requires a proportionality assessment, i.e. the legitimate interest of the data controller (ensuring the security of the network) must be weighed against the need to protect data subjects' fundamental rights (confidentiality of communications). In the case of ACDC, the need to fight botnets (as part of the security of the network) should be balanced against the need to protect users' confidentiality of communications. While the need to ensure the network is protected against botnet is clearly legitimate, the proportionality assessment will bear upon the adequacy and necessity of the means used to achieve this goal, thus on the design of the ACDC solution. In this case, two data processing operations should be legitimize: the sharing of personal data with the CCH and its further processing for fighting botnets. This processing will be performed by the CCH and shared with a legitimate interested party, i.c. ISPs, webmasters and hosts.

The necessity of the creation of a platform such as the CCH to efficiently fight botnets is justified by the international character of cybercrime and the significant threat posed by botnets. Large scale infections cannot be tackled by providers, webmasters, hosting services, and computer security companies individually. The need for cooperation and information sharing is thus crucial. The automated and non-human operated character of the CCH reduces chances of unauthorized or abusive intervention.

With regard to the adequacy of the means used, the CCH environment consists of data processing that have a strong and concrete potential to reduce botnets across the EU. The CCH is thus a suitable and adequate environment to the objectives pursued: the tools deployed at the clearing house are tested and efficient mechanisms capable of promoting knowledge and sharing data of infections. This will facilitate disinfection, as the news feed provided by the CCH will enable partners to alert their infected users and redirect them to the National Support Centre for cleansing. The purpose of the CCH is thus protecting end users and networks from botnets, promoting prevention, detection and disinfection. The information processed at the CCH is not intended to be used against individuals, left alone the possibility of ISPs, webmasters and web hosts to take the necessary legal measure to safeguard their networks against malicious users. To this end, ISPs and all partners are requested to, in accordance with their national law, decide upon the remedies, sanctions and means to be given to users to enable their adequate defence. It is thus a duty of data controllers to ensure that data subjects' rights are fully respected and that the necessary remedies and opportunities for their exercise are put in place.

Finally, the rules of the community platform together with the numb and automated character of the CCH are designed to ensure the minimal possible impact on the fundamental rights of data subjects in being taken into account. Removing the processing of personal data would diminish the capability of the CCH to a level where the purpose is no longer attainable. However, input and output data are controlled and ranked by the community platform, which also enables sharing preferences and restricts access to data according to partners legitimate interests. For instance, ISPs receiving data feeds from the CCH can only have access to information related to their own range of IP addresses, never to data relating to users that are not related to their services. This guarantees sufficient levels of confidentiality of communications and lesser invasive means on user data.

3. National Comparative Analysis. The analysis of the national laws of Belgium, France, Germany, Italy, Portugal, Romania, Slovenia, Spain, and the Netherlands has revealed that most countries do not present a significant obstacle to the deployment of ACDC and its 5 group tools. The findings of this comparison were based in the text of the law and are thus subject to the interpretation of the national protection authorities.

3.1 Implementation of Article 7(a) of Directive 95/46/EC. No major differences were found that would impair a similar application of consent as a legitimate ground to authorise the deployment of end customer tools in the countries analysed. Therefore, the use of consent, in the terms made explicit by the Directive and in respect with specificities created by national law, shall be sufficient and adequate to legitimise the use of end customer tools across ACDC.

3.2 Implementation of Article 7(b) of Directive 95/46/EC. The laws of Belgium, France, Italy, Portugal, Romania, Spain and the Netherlands have transposed the exact terms of Article 7(b) into national legislation. Therefore, the use of this provision in the context of ACDC does not additional requirements besides the ones already enshrined under the Directive and clarified by the Article 29 Working Party. In terms of result, the German Federal Data Protection Act achieves the same goal as the text provided in the Directive. Finally, the Slovenian Personal Data Protection Act requires the processing to be not only necessary but also appropriate to the performance of the contract, what must be considered under Slovenian jurisprudence. However, this shall not amount to a significant obstacle to the deployment of the ACDC tools.

3.3 Implementation of Article 7(c) of Directive 95/46/EC. The laws of Belgium, France, Italy, Portugal, Romania, Slovenia, Spain and the Netherlands have transposed the terms of the Directive without significant differences. The analysis has revealed that the laws of Germany and Slovenia have not transposed the terms of Article 17 in conformity with the Data Protection Directive. Both Member States seem to lack implementation of a legitimate ground authorizing the processing of personal data where the processing is carried out as a necessary measure to comply with a legal obligation to which the controller is subject. The exhaustive and restrictive list[1] created by Article 7 ensures that a processing conducted in accordance with these legitimate grounds is a lawful operation, as ruled by the ECJ in the Joined Cases C‑468/10 and C‑469/10. The absence of a corresponding provision in the laws of Germany and Slovenia shall not prevent the deployment of network sensors or vulnerable and malicious website analysis tools when such processing is in accordance with Article 7(c) of Directive 95/46.

3.4 Implementation of Article 7(f) of Directive 95/46/EC. The laws of Belgium, France, Portugal, Romania and the Netherlands have transposed exact the terms of the Directive. By contrast, the analysis has revealed that the laws of Germany, Italy, Slovenia and Spain have created additional obstacles to the use of the provision, which are not necessarily in line with the terms of the Directive. A flexible implementation of Article 7(f) would undermine the value of the provision. In light of the jurisprudence of the ECJ, Article 7(f) has direct effect and precludes any national rules in contradiction with the terms of the Directive. To conclude, once the CCH fulfils the criteria of Article 7(f) as set forth by the Data Protection Directive, no obstacles should be raised by national rules so as to hamper this outcome.

[1] Joined Cases C‑468/10 and C‑469/10, para. 30.

Table of Contents

1. INTRODUCTION

The Advanced Cyber Defence Centre (ACDC) Project aims at implementing five group tools to improve detection and mitigation of botnet attacks across the European Union. The ACDC tools create an environment of data sharing and knowledge exchange among end-users, ISPs, CERTs and webmasters. The envisioned technologies and platform require the processing of several types of data such as IP and email addresses, server logs, domain names, among others, which can be subject to stringent rules applicable to personal data and require partners to comply with data protection legislation. To this end, while the applicable EU legal framework may be essentially the same, responsibilities and liabilities may vary according to the characteristics of the operations. For this reason, in addition to the EU legal analysis, we provide a more detailed examination of the data protection rules applicable to each of the group tools. As highlighted in the project proposal, the objective of the legal task is essentially to clarify the rules applicable to each of the five anti-botnet tools analysed in ACDC.

Looking at the EU legal framework, Deliverable 1.8.1 examines which grounds can legitimise the use and deployment of the five ACDC botnet mitigation tools. Furthermore and in accordance with the proposal, we looked at the national laws of Belgium, France, Germany, Italy, Portugal, Romania, Slovenia, Spain, and the Netherlands to identify potential barriers to the setting out of ACDC in the countries involved. The study of the national laws is presented under Section 5. A legal comparative questionnaire was drafted and shared with partners during M6 to M9 and the answers were compiled as inputs to the backing of this analysis, included under Annex 1 to 9. Partners have answered to legal and legal-related questions regarding data protection and anti-cybercrime legislation and practice in the country. The findings of the national comparative analysis are subject to the interpretation of the law by the national protection authorities and cover the major impediments verified upon the legal text of the instruments reported by countries in their answers to the legal questionnaire.

In order to achieve a conclusion on which legal obstacles could be present in the operation of ACDC, the following sub-questions were defined:

1. Is the European Union data protection framework applicable?
    a. Is there a processing?
    b. Is the information processed personal data?
    c. Are sensitive data processed?
    d. Is the personal data processed by service providers in the context of public available communication networks?
    e. Is the security/confidentiality of the data ensured?
2. Which controllers, processors and data subjects are involved?
    a. Who are the controllers and processors of each group tool?
    b. How will this data be processed?
    c. Who are the data subjects for each group tool?
3. Is the processing of data legitimate?
    a. What is the purpose of the processing?

    b. Is this processing lawful?
    c. Are the data collected adequate with regard to the purposes of the processing?
    d. How long will the data be stored?
    e. With whom will de data be shared?
4. How will data subjects' rights be ensured?
    a. Will data subjects be informed of the processing?
    b. Will data subjects be able to exercise his/her rights (access, rectification, cancellation)?
5. Are the data processed/sent outside the European Union?

These questions were answered in light of the EU law applicable data protection framework. Furthermore, the main legal issues hampering the successful implementation of the project were narrowed down and scrutinized before the national laws of the selected countries. Additional details concerning the methodology of the national legal analysis are provided under Section 5. The conclusion highlights the key findings of the project and initial considerations concerning the legal viability of ACDC.

2. LEGAL FRAMEWORK FOR PRIVACY AND DATA PROTECTION IN THE EUROPEAN UNION

2.1 Overview

The European Union has put in place a consistent framework on the protection of privacy and data protection, spread over different instruments. These high level legal standards must be followed by and integrated under the national laws of each Member State.

2.2 Article 8 European Convention of Human Rights

The European Convention for the Protection of Human Rights and Fundamental Freedoms (hereinafter 'Convention') has been ratified by all Member States of the EU. Concluded in 1950, the Convention was one of the first actions of the then recently established Council of Europe (hereinafter, 'CoE'). Under Article 8, the Convention recognizes the fundamental right to privacy and the State duty to protect it against interference by any person or institutions, in the public or private sector:[2]

1. *Everyone has the right to respect for his private and family life, his home, and his correspondence.*
2. *There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*

The notion of private life is less tied to physical object and may protect individuals in respect of their activities in the public arena,[3] this is to say the right to private life remains applicable in public spaces. In recent years, data protection issues brought before the European Court of Human Rights (hereinafter 'ECtHR') have increasingly involved aspects of data protection in information systems. In *Copland vs. United Kingdom*, the ECtHR recognized that personal internet usage is covered under the scope of private life and considered that the *collection* and *storage* of personal information relating to telephone, e-mail and Internet usage, without the data subject knowledge, breached the guarantee of Article 8. Under the Convention, legal persons are also allowed to bring cases to the ECtHR in the case they have been victim of a violation. Although the notion of family life does not apply to legal persons, the right to privacy still covers activities of professional and business nature.[4]

Any legitimate interference in the right to privacy must fulfil a set of requirements listed in the second paragraph of Article 8 and clarified by case law. Initially, it must be noted that under the Convention only public authorities are capable of restricting the right to privacy. For the purpose of the Convention, any formality, condition, restriction or penalty, as much as collection and storage, by a public authority

[2] Ian J. Lloyd, *Information Technology Law*, Oxford University Press, 6th Edition, p. 13.

[3] Lloyd, op. cit, p. 13.

[4] P.H.P.H.M.C. van Kempen, Human Rights and Criminal Justice Applied to Legal Persons. Netherlands Comparative Law Association, Electronic Journal of Comparative Law, vol. 14. 3(December 2010). Retrieved from http://www.ejcl.org/143/art143-20.pdf. P. 17-18.

constitutes an *interference*, which is only permissible when: 1. in accordance with the law, and 2. necessary in a democratic society. Pursuant to case law, a legitimate interference must first comply with domestic law and be compatible with the rule of law (*Halford vs. United Kingdom*). The domestic law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in and conditions on which public authorities are empowered to resort to any such measures. Secondly, the measure must pursue one of the legitimate aims listed in Article 8(2) and, thirdly, be necessary in a democratic society. Here the term necessary implies that there must be no lesser means available[5] and that the interference corresponds to a pressing social need and, in particular, that it is proportionate to the legitimate aim pursued (*Uzun vs. Germany*).

2.3 Arts. 7 and 8 of the Charter of Fundamental Rights of the European Union

The right to data protection is recognised as a fundamental right in Article 8 of the Charter of Fundamental Rights of the European Union (herein 'EU Charter'), which, although related, is distinct from the respect for private and family life contained in Article 7[6] of the same instrument. Although used interchangeably and closely linked in jurisprudence, privacy and the protection of personal data are not the same. The right to data protection is the only one to cover any information relating to an identified or identifiable individual. The right to privacy, however, aims to protect private life and does not go as far as to cover all data related to a person.[7] They also differ in personal scope, as legal persons only have access to the right to privacy, according to the European Court of Justice.[8] Article 8 of the EU Charter reads as follows:

> 1. Everyone has the right to the protection of personal data concerning him or her.
>
> 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
>
> 3. Compliance with these rules shall be subject to control by an independent authority.

Through the Lisbon Treaty, the EU Charter gained binding legal status at EU level and data protection was recognised as an autonomous fundamental right part of primary EU law.[9] As a result, the right to data protection must be balanced against other values and interests before the EU legislators and the

[5] Douwe Korff, *The Standard Approach Under Articles 8 – 11 ECHR and Article 2 ECHR*, Retrieved from http://ec.europa.eu/justice/news/events/conference_dp_2009/presentations_speeches/KORFF_Douwe_a.pdf, p. 3.

[6] Data Protection in the European Union: the role of National Data Protection Authorities (Strengthening the fundamental rights architecture in the EU II), FRA – EU Agency for Fundamental Rights, Retrieved from http://fra.europa.eu/sites/default/files/fra_uploads/815-Data-protection_en.pdf, p. 14.

[7] J. Kokott and C. Sobotta, The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR. International Data Privacy Law, Oxford University Press [2013], vol. 3, issue 4, p. 4.

[8] J. Kokott and C. Sobotta, The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR. International Data Privacy Law, Oxford University Press [2013], vol. 3, issue 4, p. 4.

[9] Data Protection in the European Union: the role of National Data Protection Authorities (Strengthening the fundamental rights architecture in the EU II), FRA – EU Agency for Fundamental Rights, Retrieved from http://fra.europa.eu/sites/default/files/fra_uploads/815-Data-protection_en.pdf, p. 18.

European Court of Justice (herein 'ECJ').[10] One first observation about the EU Charter refers to its limited scope. Article 51(1) establishes that the EU Charter is only applicable to the bodies of the EU and to Member States only when implementing EU law. Thus albeit the EU Charter does not require full legal harmonisation across the Union, it must be taken into account by all Member States when implementing their national data protection laws.

Another important aspect of the EU Charter is enshrined under Article 52(3), first part, which reads as: "*In so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention*." This is understood as the main element of coherence between the EU Charter and the ECHR. It entails the need for EU institutions, here included the ECJ, and Member States, to the extent of the implementation of EU law, to observe the interpretation and the case law of the ECHR and accordingly apply them to the data protection right of Article 8 of the EU Charter.

Under Article 52(1), interferences with the right to data protection must be provided by law and attempt to the principle of proportionality, and only to the extent they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others. Any limitation or restriction to the right to data protection that does not fulfil these requirements will be illegitimate and thus void.

2.4 Applicable EU data protection framework

The EU framework on data protection is composed by two main instruments: Directive 95/46/EC on the protection of personal data, and Directive 2002/58/EC on the protection of privacy in the electronic communications sector. However, since EU Directives are legally binding only in terms of results,[11] Member States were given discretion to implement Directive 95/46/EC and Directive 2002/58/EC, albeit this flexibility was narrowed down by the aim of harmonisation brought by these instruments.[12]

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 (hereinafter 'Data Protection Directive') is the major instrument of EU Data Protection Law. This Directive has two main purposes: (1) to allow for the free flow of data within Europe, preventing Member States from blocking inter-EU data flows on data protection grounds, and (2) to achieve a minimum level of data protection throughout all Member States. Addressing the nature of the Data Protection Directive in *Rechnungshof*, the ECJ indicated that in so far as the provisions of the Directive govern the processing of personal data liable to infringe fundamental freedoms, in particular the right to privacy, the Data Protection Directive must necessarily be interpreted in the light of fundamental rights.[13]

[10] Data Protection in the European Union: the role of National Data Protection Authorities (Strengthening the fundamental rights architecture in the EU II), FRA – EU Agency for Fundamental Rights, http://fra.europa.eu/sites/default/files/fra_uploads/815-Data-protection_en.pdf, p. 18.

[11] Lee A. Bygrave, *Data Protection Law – Approaching its rationale, logic and limits*, Kluwer Law International [2002], p. 34.

[12] Lee A. Bygrave, op. cit., p.34.

[13] C-138/01 Rechnungshof [2003] ECR I-6041, paras. 68-69.

Directive 2002/56/EC (herein 'e-Privacy Directive') particularises and complements Directive 95/46/EC for the purpose of promoting harmonisation of privacy and confidentiality, with respect to the processing of personal data in the electronic communication sector, and to ensure the free movement of such data and of electronic communication equipment and services in the EU.

2.4.1 Scope of Directive 95/46/EC

The application of Directive 95/46/EC is defined under Article 3(1) and covers the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system. Article 3(2) has also specified the areas in which the Directive is not deemed applicable:

1. Data processing carried out as part of activities falling beyond EU law (processing operations concerning public security, defence, national security, and activities in the area of Criminal Law).
2. Data processing carried out by a natural person in the course of a purely personal or household activity.

Two concepts are central to the application of the Directive, namely 'personal data' and 'processing'. Personal data is defined under Article 2(a) of the Directive and refers to any information relating to an identified or identifiable individual (data subject). Corroborating this definition, the Article 29 Working Party[14] affirms 'data relates to an individual if it refers to the identity, characteristics or behaviour of an individual or if such information is used to determine or influence the way in which that person is treated or evaluated'. The concept of personal data is to be interpreted broadly and covers not only information about someone's personal life, but to all data about a person, be it private or publicly available.[15]

The second key concept to the scope of the Data Protection Directive is the one of processing. This is also defined broadly and covers any operation or set of operations which is performed upon personal data, whether or not by automatic means (Article 2(b) Directive 95/46/EC). It includes but is not limited to collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction of personal data. Although the Directive does not go as far as to define what should be considered automatic means, the term normally refers to data processing by computers and software, such as computerized databases and IT-networks.[16]

2.4.2 Scope of Directive 2002/58/EC

The e-Privacy Directive only applies to personal data processed in publicly-available electronic communications services in public communication networks (Article 3). Overall, the e-Privacy Directive

[14] Article 29 of Directive 95/46/EC established a working party on the protection of individuals with regard to the processing of personal data, which became to be known as the Article 29 Working Party. This independent advisory board is comprised of representatives of the Member States Data Protection Authorities and issues interpretative documents without legal binding effects. See Christopher Kuner, op. cit., pp. 9-10.

[15] Christopher Kuner, op. cit., p. 92.

[16] Waltraut Kotschy in Alfred Bullesbach, Yves Poullet, Corien Prins, *Concise European IT Law*, Kluwer Law International [2006], p. 37.

imposes additional obligations on providers of public available communications with the goal of preserving and protecting the privacy of users. Because the nature of the e-Privacy Directive is complementary in relation to the Data Protection Directive, the latter continues to apply to matters not specifically covered by the first.[17] Differently from the Data Protection Directive, the e-Privacy Directive does not define legal actors for the processing but mainly refers to providers of electronic communications services and users. This preference reveals the choice for a functional rather than a legal approach.[18] In the terms of Article 2(a) of e-Privacy Directive, user means any natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to this service.

The applicability of the e-Privacy Directive requires personal data, traffic data or location data to be processed by an electronic communications service in the context of publicly available communication networks. The definition of electronic communications services and public communications networks, however, is to be found in the Framework Directive 2002/21/EC, and relate to the very concept of electronic communication network.[19] Pursuant to Article 2(c) of the Framework Directive, 'electronic communications service' is a service provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting (e.g. ISPs, mobile and telephone operators, etc.). Article 2(d) defines 'public communications network' means an electronic communications network used wholly or mainly for the provision of electronic communications services available to the public which support the transfer of information between network termination points. In effect, the e-Privacy Directive only applies to electronic communications which are non-content services.[20] Finally, the concept of 'electronic communication networks' is also given by the Framework Directive under Article 2(a), meaning transmission systems and, where applicable, switching or routing equipment and other resources, including network elements which are not active, which permit the conveyance of signals by wire, radio, optical or other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed. In summary, it means that in the context of ACDC the e-Privacy directive is only applicable to the processing of data (personal data, traffic data and location data) by ISPs in the context of public networks.

Not all ACDC tools are intended to process data in public communication networks. In fact, the Centralised Clearing Data House is an internal platform exclusively designed to share data about infections with trusted partners. The same is valid for the National Support Centres, which do not involve processing of personal data in connection with public networks. Albeit both group tools are fed

[17] Christopher Kuner, op. cit., p. 24.

[18] Christopher Kuner, op. cit., p. 137.

[19] Pursuant to Article 2 of the e-Privacy Directive, save as otherwise provided, the definitions in Directive 95/46/EC and in Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) (1) shall apply.

[20] Christopher Kuner, op. cit., p. 136.

with information collected in public available networks, the processing carried out in their environments does not amount to a processing conducted in connection with public communication networks.

That is not the case for the remaining group tools. Network traffic sensors, malware website analyses, and end customer tools involve the exchange of personal data from an individual with the outside world conveyed by public communication networks. In fact, the very goal of such tools is to provide real time detection, reporting, and immunisation mechanisms for malicious traffic/websites found online. Nevertheless, the processing activities carried out by these three anti-botnet tools only fall within the e-Privacy directive when conducted by ISPs. Because the End customer tools do not involve the participation of ISPs, but rather plugins to be downloaded by users from the National Support centre website, they are out of the scope of this directive. Finally, this also means whenever malware analysis tools and network sensors are operated agents other than ISPs, the e-Privacy directive is not applicable.

Concerning jurisdictional scope, the e-Privacy Directive is applicable whenever the processing is carried out in connection with a service provided via public communications network located in the EU. It means not only that any use of physical networks located in the Community is covered by the Directive, but also that any data subject using such networks benefit from its protection.[21] In other words, the e-Privacy Directive is applicable whenever the processing involves personal data of a user located in the EU or is provided by a public communications network based in the EU. Defining which Member State law is applicable to the processing, however, is a second step. To this end, the e-Privacy Directive introduces the 'country of destination' rule,[22] which disregards the location of the service provider. Under the e-Privacy Directive and the country of destination rule, the applicable law is the one of the country where the data subject is based. The overall idea behind the rule is to enable data subjects to, whenever needed, bring a case to its own national court.

2.4.3 Anonymisation or de-identification, pseudonyms and re-identification

The concept of personal data brings questions about the notion of anonymised or de-identified data, how this can be achieved and what does it mean to the data processing. The principle of storage limitation embodied in Article 6(1) (e), as it will be explained further, introduced the idea of data anonymisation at EU level. In summary, the process of anonymisation aims to produce the effect of making impossible to re-relate data to a specific person.[23] The possibility of anonymising data at ACDC can be considered by partners and shall be agreed upon in collectively, as it may affect the achievement of certain purposes at a later stage. Therefore, partners may want to discuss the possibilities and context for anonymisation and pseudonymisation at an early phase of the ACDC project.

According to Recital 46 of Directive 95/46/EC, data which are integrally anonymised don't need to comply with the principles of data protection. This is because anonymisation removes the component that calls for legal protection: the possibility of identifying a person through the use of data. Therefore,

[21] Christopher Kuner, op. cit., p. 138.
[22] Christopher Kuner, op. cit., p. 139.
[23] Philippe Meier, op. cit., p. 204.

anonymised data eliminates the chances of linking a "name and face" to that set of data. On the one hand, data anonymisation can be understood as a safeguard for improving data protection for individuals,[24] as it ensures respect to the proportionality principle and to the balance of interests between data controllers and data subjects. On the other hand, as pointed by Ohm, progressive removal of personal elements can reduce the possible data utility to controllers.[25] The extent of and need for anonymisation, therefore, shall be internalised by partners. They are in the best position to understand the purpose and legal obstacles to the processing of the relevant personal, as much as any losses that may rise with anonymisation of such data.

Determining whether anonymisation was fully accomplished requires a case-by-case examination.[26] Albeit Recital 26 refers to anonymised data as a processing where the data subject is no longer identifiable, total impossibility of re-identification can be extremely difficult to achieve. Moreover, even if identification through a single data source is no longer possible (direct identification), it can be that by the combination of two or more data sources (indirect identification) anonymised data will become once again personal data.[27] For this reason, a realistic approach should understand anonymised data as data that does not itself identify any individual and that is unlikely to allow any individual to be identified through its combination with other data.[28] This line of thought (de facto anonymisation)[29] is recognised by the Article 29 Working Party and by national legislators in the UK and in Germany.[30]

The degree of anonymisation will depend on the complementary information held or capable of acquisition by the data controller or by the entity/person that will use the data in the end. If re-identification is possible by the combination of this information or by comparison with other data originating from different sources, it is no longer possible to speak of de facto anonymisation.[31] The storage duration/data retention can also play an important role: the faster the elimination of de facto anonymised data, the smaller the risks of re-identification.[32] When assessing the degree of anonymisation, one can consider the theory of relativity of re-identification, which says that only the knowledge, means and possibilities, as well as the data controller own (potential) interest, shall be taken into account to determine the likelihood of re-identification.[33] As noted by the Information Commissioner Office of the UK, "*the DPA does not require anonymisation to be completely risk free – you must be able to mitigate the risk of identification until it is remote. If the risk of identification is reasonably likely the information should be regarded as personal data - these tests have been*

[24] UK Information Commissioner's Office, *Anonymisation: managing data protection risk code of practice*. Retrieved from http://www.ico.org.uk/for_organisations/data_protection/topic_guides/~/media/documents/library/Data_Protection/Practical_application/anonymisation_code.ashx, p.12.

[25] Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization* (August 13, 2009). UCLA Law Review, Vol. 57, pp. 1701-1777, 2010, pp. 1705-1706.

[26] Article 29 Working Party Opinion 4/2007 on the concept of personal data adopted on 20 June 2007, p.21.

[27] UK Information Commissioner's Office, op. cit., p.16.

[28] Article 29 Working Party Opinion 4/2007, p.21.

[29] Philippe Meier, op. cit., p. 204.

[30] This is the approach followed by the UK (see ICO, Anonymisation: managing data protection risk code of practice) and in Germany (German Federal Data Protection Act) – however local Germany data protection laws may follow the absolute theory and thus require the impossibility of re-identification to consider data as anonymised. See Christopher Kuner, op. cit., p. 66.

[31] Philippe Meier, op. cit., p.204.

[32] Philippe Meier, op. cit, p. 205.

[33] Philippe Meier, op. cit., p. 206.

confirmed in binding case law from the High Court. Clearly, 100% anonymisation is the most desirable position, and in some cases this is possible, but it is not the test the DPA requires."[34]

Due to the difficulties of achieving anonymisation and in light of the disadvantages brought by such procedure, pseudonymisation has grown as an alternative to reduce data protection issues while preserving the value of the data. Pseudonymisation aims to replace the identifiable characteristic of a person for a code (pseudonym), in such a way that the data can no longer be related to a specific individual, unless by the ones that are capable of or authorised to conduct the reversing process (e.g. by crossing data between the individuals and their pseudonym, via two-way encryption algorithms, etc.).[35] In the case of pseudonymisation, the data subject identity is disguised in a re-traceable way.[36] This results in a greater risk to individuals when compared to anonymisation, as pseudonymisation does not change the nature of the concealed data, which remains personal.[37] While no data protection standards apply to fully anonymised data, pseudonymous data are still subject to data protection law, as there is a concrete risk of re-traceability[38] that can lead to access to the concealed data. Nevertheless, this remains an important tool to help mitigate data protection risks, as pseudonyms are only indirectly identifiable[39] and the reversing process can only be conducted by means of a key.[40] Ideally, the key should be conserved apart by a trusted third party.[41]

According to the Article 29 Working Party, the efficiency of this processing depends on different factors that can influence the likelihood of the reversing process occurring. These are at which stage the data is used, how secure it is against reverse tracing, the size of the population in which the individual is hidden, the ability to link individual transactions or records to the same person, an external hack, etc.[42] It continues by stating that "*pseudonyms should be random and unpredictable. The number of pseudonyms possible should be so large that the same pseudonym is never randomly selected twice. If a high level of security is required, the set of potential pseudonyms must be at least equal to the range of values of secure cryptographic hash functions*.[43] In effect, much of the value of pseudonyms lies in the size of the data set,[44] but as noted by Anderson and quoted by Korff, "*the problem with pseudonyms is that if they're used for more than one purpose, the anonymity they give rapidly erodes, and this is the case regardless of the form of the pseudonym."*[45] In the ACDC scenario, partners may have the option to anonymise data or to use pseudonyms to reduce data protection conflicts. All and

[34] UK Information Commissioner's Office, op. cit., p.6.

[35] Philippe Meier, op. cit., p.206.

[36] Article 29 Working Party, Statement of the Working Party on the current discussions regarding the data protection reform package, p.1.

[37] Article 29 Working Party, Statement of the Working Party on the current discussions regarding the data protection reform package, p.1.

[38] Christopher Kuner, op. cit., p. 66. Opposite to this, see Philippe Meier, op. cit., p. 207.

[39] Article 29 Working Party, Opinion 4/2007, p. 18.

[40] Douwe Korff*, Comparative Study On Different Approaches To New Privacy Challenges, In Particular In The Light Of Technological Developments*, Final Report [2010], p. 48.

[41] Philippe Meier, op. cit., p.206.

[42] Article 29 Working Party, Opinion 4/2007, p. 18 and Philippe Meier, op. cit, p. 207 and Douwe Korff, Final Report [2010], op. cit., p. 48.

[43] Article 29 Working Party, Opinion 4/2007, p. 18.

[44] Douwe Korff, Final Report [2010], op. cit., p. 48.

[45] Christopher Kuner, op. cit., p. 50.

all, partners must bear in mind the circumstances described above, as well as the classification of anonymised and pseudonymised data as interpreted by the Courts and recognised by legislation.

Finally, when choosing for anonymisation or pseudonymisation, partners shall not forget the threat imposed by re-identification. In the words of Paul Ohm, "*reidentification occurs by the combination of datasets that were meant to be kept apart, and in doing so, gains power through accretion: Every successful reidentification, even one that reveals seemingly nonsensitive data like movie ratings, abets future reidentification."* [46] With the recent developments in ICTs and the widespread availability of population datasets, identification of persons becomes increasingly easier to achieve, even when essential personal information has been removed or disguised. For Ohm, "*this is not to say that all anonymization techniques fail to protect privacy—some techniques are very difficult to reverse—but researchers have learned more than enough already for us to reject anonymisation as a privacy-providing panacea*."[47] One of the examples given by the author to illustrate the problems related to anonymisation is the abundance of outside information: *"once an adversary (person trying to reidentify the data) finds a unique data fingerprint, he can link that data to outside information, sometimes called auxiliary information. Many anonymisation techniques would be perfect, if only the adversary knew nothing else about people in the world. In reality, of course, the world is awash in data about people, with new databases created every day. Adversaries combine anonymized data with outside information to pry out obscured identities."*[48]

If anonymisation and pseudonymisation are not the final answers to the issue of data protection, what can be done by data controllers to reduce the requirements they need to comply with and still be able to process relevant data? According to Korff, "*the basic approach should be to reduce the collecting and even initial storing of personal data to the absolute minimum (cf. the German - but also European - principle of "data minimisation" and the Australian "anonymity principle"): once data have been collected and are stored, they are almost impossible to eradicate or (to take Ohm's point) truly, permanently anonymise."*[49]

As it is clear from our examination, full anonymisation is very hard to achieve, while pseudonymisation does not release data controllers from ensuring compliance with data protection legislation. Therefore, partners must bear in mind the risks and standards for anonymisation and pseudonymisation and take into account the interpretation used by DPAs in their national jurisdiction.

2.4.4 Technology related data as personal data: IP addresses and domain names

In line of principle, several operations envisioned by the ACDC project will inevitably fall in the ambit of Directive 95/46/EC, as they imply processing of data that can relate to identified or identifiable persons in the offline world. ACDC partners will often have no access to the real identity of users, but nevertheless will be able to single out an individual user within a universe of users. Truth is the efficiency of the entire project would be significantly reduced if such differentiation would be unfeasible. However, the likelihood of identification would be minimal, as long as partner-operators do

[46] Paul Ohm, op. cit., p. 1705.
[47] Paul Ohm, op. cit., p. 1716.
[48] Paul Ohm, op. cit., p. 1724.
[49] Douwe Korff, Final Report [2010], p. 48.

not possess particularly privileged information that could be linked to the data generated by the mitigation tools so as to increase the potential identifiability of subjects.

Whereas identification through names is the most common occurrence in practice, identification can take place in its absence. In the words of the Article 29 Working Party[50]: "*computerised files registering personal data usually assign a unique identifier to the persons registered, in order to avoid confusion between two persons in the file. Also on the Web, web traffic surveillance tools make it easy to identify the behaviour of a machine and, behind the machine, that of its user. Thus, the individual's personality is pieced together in order to attribute certain decisions to him or her*."

In fact, differentiating users according to their online behaviour is at the very core of multiple technologies available in ACDC. The architecture of ACDC has been structured in such a way that the purpose of group tools may involve personal data processing in the terms of Article 2(a) and (b). If partner-operators are in possession of information that would lead to a close link between the data generated and the identity of the user employed to single out individuals, the Data Protection Directive becomes applicable. Nevertheless, national laws may have narrower concepts of identifiability and personal data. They may require the presence, possession or knowledge by operators of elements such real names, address, and other regular personal data for data protection legislation to become applicable.

For instance, the indication of which users were assigned a particular **IP address** at particular times consists of personal data under Article 2(a) of the Directive,[51] even without disclosure of close personal details, as explained above. The Study of case law on the circumstances in which IP addresses are considered personal data (SMART 2010/12)[52] points that a broad interpretation of recital 26 of the Directive could lead to the conclusion that there is always an 'other person' (namely the ISP) who is reasonably likely to be capable of using the IP address to identify a subscriber or a natural person linked to the subscriber, a strict reading of the Directive would imply that the IP address should be considered as personal data. However, the same study affirms that by considering that an IP address strictly speaking identifies a specific network device, rather than the individual using that device, and is generally issued only temporarily, a very narrow reading of recital 26 might lead to the inverse conclusion[53].

In fact, the Article 29 Working Party is of the opinion that, in most cases, cookies and IP addresses are to be considered personal data. It affirms that "w*hen a cookie contains a unique user ID, this ID is clearly personal data. The use of persistent cookies or similar devices with a unique user ID allows tracking of users of a certain computer even when dynamic IP addresses are used. The behavioural data that is generated through the use of these devices allows focusing even more on the personal*

[50] Article 29 Working Party Opinion 1/2008 on data protection issues related to search engines, adopted on 4 April, 2008, p. 14.

[51] Article 29 Working Party Opinion 1/2008, p. 8.

[52] Study of case law on the circumstances in which IP addresses are considered personal data SMART 2010/12 D3. Final report. P. 7.

[53] Study of case law on the circumstances in which IP addresses are considered personal data SMART 2010/12 D3. Final report. P. 7.

characteristics of the individual concerned".[54] With the aid of those data, actions performed using the IP address concerned are linked to the subscriber.[55] The question whether IP addresses can be considered personal data may strongly depend on the circumstances in which they are used. Most DPAs are of the opinion that they should be regarded as personal data in most cases[56], and if any doubt exists before the influence of these circumstances, the cautious approach is utmost expected[57]. Some of the circumstances that can influence the classification of IP address as personal data include[58]:

- The infrastructure available to the data controller (such as the aforementioned logs in combination with customer data);

- The availability of other related data which can be combined with IP addresses to improve identifiability (such as the search history behind a specific address);

- The purpose or intent behind the processing of IP addresses (such as the aforementioned example of logging with the specific intent of enabling the identification of the end user);

- The context of the processing of IP addresses (such as an ISP which also operates its own content portal, on which IP addresses are only processed to suggest an appropriate initial language choice).

Nevertheless, the Article 29 Working Party is of the opinion that unless a controller is in a position to distinguish with absolute certainty that the data correspond to users that cannot be identified, it will have to treat all IP information as personal data, to be on the safe side. This also opens the possibility for controllers to prove that the use of IP addresses may not imply the application of the Data Protection Directive. In spite of this, the SMART 2010/12 study found that countries like France, Germany, Italy, and Slovenia have strongly highlighted that the possibility of identifying a person on the basis of an IP address can never be completely excluded if the assistance of third parties (e.g. ISPs with log files) can be ensured, and therefore that all IP addresses should be protected as personal data by default[59].

EU Data Protection Supervisor (EDPS) Peter Hustinx affirms that a person does not have to be identifiable by name for data protection law to apply to details of their computer usage. In fact, all user activity, server logs and records of IP addresses could be classified as personal data. Details such as name, birth data, address, etc., do not need to be known from the data controller, as along as the processing of the IP address can be used to make him/her identifiable. This means to use this data in such a way as track the behaviour of a user and thus single him/her out.[60] In his opinion on the EU

[54] Article 29 Working Party Opinion 1/2008, p. 9.
[55] A.G. Kokott, C-275/06, Promusicae [2006] ECR I-00271, paragraph 61.
[56] Christopher Kuner, op. cit., p. 94.
[57] Study of case law on the circumstances in which IP addresses are considered personal data SMART 2010/12 D3. Final report. P. 24.
[58] Study of case law on the circumstances in which IP addresses are considered personal data SMART 2010/12 D3. Final report. P. 10.
[59] Study of case law on the circumstances in which IP addresses are considered personal data SMART 2010/12 D3. Final report. P. 24.
[60] ZDNet interview with Peter Hustinx, available at: http://news.zdnet.co.uk/security/0,1000000189,39540137,00.htm.

Anti-Counterfeiting Trade Agreement (ACTA)[61], the EDPS reaffirmed his understanding of IP address as personal data: "*If a user engages in a given activity, for example, uploads material onto the Internet, the user may be identified by third parties through the IP address he/she used. For example, the user holding IP address 122.41.123.45 uploaded allegedly copyright infringing material onto a P2P service at 3 p.m. on 1 January 2010. The ISP will then be able to connect such IP address to the name of the subscriber to whom it assigned this address and thus ascertain his/her identity*. *If one considers the definition of personal data provided in Article 2 of Directive 95/46/EC, 'any information relating to an identified or identifiable natural person (data subject); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number', it is only possible to conclude that IP addresses and the information about the activities linked to such addresses constitutes personal data (…). Indeed, an IP address serves as an identification number which allows finding out the name of the subscriber to whom such IP address has been assigned. Furthermore, the information collected about the subscriber who holds such IP address ('he/she uploaded certain material onto the Web site ZS at 3 p.m. on 1 January 2010') relates to, i.e. is clearly about the activities of an identifiable individual (the holder of the IP address), and thus must also be considered personal data.*"

All the opinions above rely on the availability of additional data that, together with the IP address, would result in the identification of a "name and face". This is to say that the mere nature of IP address does not classify the string of numbers as personal data, but depends on the person of the controller and on the information that is likely to be accessible to him/her. Therefore, the analysis of IP address as personal data is an investigation of context. The European Data authorities have not issued a conclusive opinion on this matter and have limited themselves to general and abstract statements. By avoiding this confrontation, the Article 29 Working Party resolved to adopt a safe harbour approach that requires IP addresses to be treated as personal data unless proven otherwise.

In 2007, a case brought before the Paris Appeal Court asked the Court to recognise that the processing of IP addresses required authorization from the DPA, as it was a case of processing of personal data. The Court rejected the argument to find that a series of numbers such as contained in an IP address by no means constitute an indirectly nominative data of a data subject as it only relates to a machine and not to the individual who is using the computer. It also recognised when assessing the likelihood of use of other means by data controllers, there should be no consideration to illegitimate ways of accessing this data, as the law enforcement authority should be the only one authorised to obtain the user identity from the ISP. In 2008, the District Court of Munich argued that in that case dynamic IP addresses were not personal data, because Internet portals or website operators could not link "names and faces" to IP addresses by employing "normally available tools". The Court restricted the test of likelihood of means to be used by the controller to legal methods of identification, excluding thus from the analysis hypothetical situations where a third party (e.g. Internet Access Provider) could give the website operator/portal access to additional information about the user

[61] Opinion of the European Data Protection Supervisor on the current negotiations by the European Union of an Anti-Counterfeiting Trade Agreement (ACTA), 2010/C 147/01, available at: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2010/10-02-22_ACTA_EN.pdf

connected to the IP address. However, neither the Paris Appeal Court nor the District Court of Munich went as far as to define which normally available tools would make dynamic IP addresses fall within the personal data category.

Opposing to the findings of Paris and Munich, the Regional Court of Berlin, upholding the ruling of the District Court of Berlin, considered that all means of identification, regardless of whether controller by a third party or by the data controller, must be taken into account when evaluating the identifiability of the user. In its assessment, the Regional Court did not disregard the influence of illegal means. The likelihood test thus would be carried out in light of the costs associated with the exchange of information that could lead to the identification of the address-holder. The costs of communication would thus be the key element to defining on the identifiability of a user. This was also the interpretation of the Stockholm Laensraett in a trial case in 2005, where the likelihood test considered that the effort to contact a third party in order to get illegal access to data was small and would result in the identification of the address-holder.

What all the above decisions fail to do is to present a concrete test to determine in which cases IP addresses are to be considered as personal data. But combining elements of these findings can result in important aspects of this consideration[62]. This can be achieved by a close examination of Article 2(a) in combination of Recital 26 of the Data Protection Directive. To evaluate the personal data character of an IP address, one shall consider a two-tier test, composed by a legality step (identification and exclusion of illegal means of identification from the assessment process) and a likely reasonable step (evaluation of effort and costs associated with the use of all the various means of identification that could be used to unmask the address-holder)[63].

Therefore, in ACDC each partner processing IP address is advised to conduct an internal evaluation to understand the likelihood of their processed data to be matched to privileged information and fall within the category of personal data. It is clear that processing of IP addresses is likely to be considered as personal data when the controller is an ISP, as this actor holds additional information at hand that can be used to put a name and face in the address-holder. This likelihood is certainly lower when the processor is a webmaster or website owner, as he/her does not necessarily possess qualified information that could end up unmasking the user. Other factors that may influence the likelihood of having IP addresses classified as personal data relate to the technical capabilities of the processor, what type of data is involved, whether other data are available in the matching, as well as the effort and the costs associated with the measures that such controller would need to take to obtain this additional information.[64] Clearly, this is a matter that can only be determined in a case-by-case basis and needs to be interpreted in light of national legislation and case law.

Nevertheless, it is clear that anonymising data such as IP addresses and domain names or treating them as personal data by default will minimise this uncertainty. While anonymisation may impose the drawbacks highlighted above, treating IP addresses as personal data may reduce the range of

[62] Lundeval-Unger, P. & Tranvik, T. IP Addresses – just a number? P. 14.
[63] Lundeval-Unger, P. & Tranvik, T. IP Addresses – just a number? P. 14.
[64] Christopher Kuner, op. cit. p. 91.

legitimate operations and subject processing to specific regulation. However, both measures will provide partners with greater legal certainty. In light of the opinions issued by the EDPA and the Article 29 Working Party, these are the safest approaches and therefore recommended in this legal analysis.

With respect to **domain names**, questions may rise on whether spaces which carry iterations of particular personal data (e.g. personal name, address, etc.) would classify as personal data in the terms of the Data Protection Directive. It is difficult to imagine how a domain name, even if including elements of personal data, would per se lead to identification of an individual.[65] However, if a domain is combined with the content of its related website and together reveal substantial information to enable identifiability by someone, the Data Protection Directive shall apply. With regards to domain names and their related websites, particular uses of a personal domain name in combination with web content about the person in question may classify as personal data and require attention to the standards created by Directive 95/46.[66] Finally, the same interpretation given to understand whether IP addresses shall be regarded as personal data applies here: whenever a controller in the possession of a domain name is also likely to obtain privileged information that can lead to identifying the user behind the data, chances are the domain name will fall within the personal data category.

Finally, questions regarding sensitive data are not relevant to ACDC. Sensitive data refers to personal data revealing the racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health of sex life (Article 8 of Directive 95/46/EC). Because the misuse of these data could have more severe consequences on the individual's fundamental rights, such as the right to privacy and non-discrimination, than misuse of other, 'normal' personal data,[67] especial protection rules shall be observed. However, since no such type of data will be processed by partners, additional stringent rules are not applicable to ACDC.

2.4.5 Processing, storage and retention of traffic and location data

The term 'traffic data' comprises any data processed in connection with the transmission of signals over a communication network[68] and is defined under Article 2(b) of e-Privacy Directive as "any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof". "*It includes the data relating to the point of origin of a communication, its destination, and the duration of the communication (…) This will encompass both data relating to use of a telephone and any data which might be processed by an ISP concerned with Internet usage,*" says Lloyd.[69] Pursuant to Article (5) of e-Privacy Directive, **traffic data is to be regarded the same confidentiality standards given to personal data**, and cannot be listened to or tapped, nor stored or intercepted by persons other than users without their consent. The only

[65] Jacqueline D. Lipton, *Internet Domain Names, Trademarks and Free Speech*, Edward Elgar Pub [2010], pp. 55-56.

[66] Jacqueline D. Lipton, op. cit., pp. 55-56.

[67] Article 29 Working Party, Advice paper on special categories of data ("sensitive data"), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/others/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf, p. 4.

[68] Ian J. Lloyd, op. cit., p. 169.

[69] Ian J. Lloyd, op. cit., p. 169.

exceptions to this rule are the technical storage necessary to convey the communication and the grounds provided by Article 15(1). IP addresses are typical examples of traffic data.

While the basic prohibitions to data processing are extended to traffic data, the range of permissible use is wider for the later.[70] Article 6(1) requires traffic data to be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication. The exceptions that allow service providers to process such data (1. for the purpose of billing and interconnection payments; 2. for marketing electronic communications services; 3. for value added services) are not relevant in the context of ACDC. Finally, Article 6(5) requires the processing of traffic data to be restricted to authorised personnel handling billing or traffic management, customer enquiries, fraud detection, marketing electronic communications services or providing a value added service, and to the end and duration necessary for the purposes of such activities.

In the terms of Article 2(c) of e-Privacy Directive, location data means any data processed in an electronic communications network or by an electronic communications service, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service. With regards to the processing of location data, Lloyd notes that "*given that the processing of data will take place in real time and be associated with the movements and location of the user, the processing might be considered rather more sensitive than in the cases where traffic data is used for marketing purposes*".[71]

The processing of this type of data is limited and can **only take place after anonymisation or with user consent for delivering a value added service** (Article 9(1)). Prior to giving consent, users must be informed of the type of location data which will be processed and whether it will be transferred to a third party. Users shall be able to withdraw consent at any time, without prejudice of using simple and free means to temporarily refuse the processing of such data for each connection to the network or for each communication transmission (Article 9(2)). In any case, the lawful processing of location data must be restricted to authorised persons acting under the authority of a service provider or of a third party providing value added service, and to the extent which is necessary for providing the value added service (Article 9(3)).

2.4.5 Exceptions

The framework of data protection shaped by the Data Protection Directive has also enabled exceptions under Article 13 that may limit the rights and obligations set forth in the Directive. Additional exceptions to the processing of traffic and location data were created by Article 15 of e-Privacy Directive. The competence for creating such restrictions, however, was given to Member States, while only general guidelines are provided by the Directives. Recital 43 of Data Protection Directive explains that restrictions on the rights of access and information and on certain obligations of the controller may be imposed by Member States in so far as they are necessary to safeguard, for example, national security, defence, public safety, or important economic or financial interests of a Member State or the

[70] Ian J. Lloyd, op. cit., p. 169.
[71] Ian J. Lloyd, op. cit., p. 170.

Union, as well as criminal investigations and prosecutions and action in respect of breaches of ethics in the regulated professions.

> Article 13 - Exemptions and restrictions
>
> 1. Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6(1), 10, 11(1), 12 and 21 when such a restriction constitutes necessary measures to safeguard:
>
> (a) National security;
>
> (b) Defence;
>
> (c) Public security;
>
> (d) The prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;
>
> (e) An important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;
>
> (f) A monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);
>
> (g) The protection of the data subject or of the rights and freedoms of others.

The grounds set forth under Article 13(1) are rather general and do not give sufficient clarity on what concrete type of restrictive legal measure would be considered legitimate. In effect, Article 13 has been used in context with other directives that build further on the general exceptions, such as the e-Privacy Directive and most case law available refers to the use of the later.

Referring to the content of Article 15(1) of e-Privacy Directive,[72] the ECJ recalled that "under that provision the Member States may adopt legislative measures to restrict the scope inter alia of the obligation to ensure the confidentiality of traffic data, where such a restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communications system, as referred to in Article 13(1) of Directive 95/46."[73] In other words, national legislators can create exceptions and restrictions for the rights provided by the e-Privacy Directive, as long as in accordance with the grounds prescribed by Article 15(1).

[72] Article 15 - Application of certain provisions of Directive 95/46/EC.
Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union.

[73] C-275/06, Promusicae [2006], ECR I-00271, paragraph 49.

As clarified in the Linqdvist case[74], the grounds of Article 15(1) concern, first, national security, defence and public security, which constitute activities of the State or of State authorities unrelated to the fields of activity of individual, and, second, the prosecution of criminal offences.[75] However, as the provision "*does not specify the rights and freedoms covered by that exception, Directive 2002/58 must be interpreted as reflecting the intention of the Community legislature not to exclude from its scope the protection of the right to property or situations in which authors seek to obtain that protection through civil proceedings*", affirmed the ECJ in *LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten*.[76]

The freedom given to Member States to restrict right to privacy, however, must fulfill certain requirements. When transposing the e-Privacy Directive into national law, Member State must do so by interpreting the law in a way that strikes a fair balance between the various fundamental rights protected by EU law. As affirmed in Promusicae and in *LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten*, "*when applying the measures transposing those directives, the authorities and courts of Member States must not only interpret their national law in a manner consistent with those directives, but must also make sure that they do not rely on an interpretation of those directives which would conflict with those fundamental rights or with the other general principles of Community law, such as the principle of proportionality*" (*Promusicae*, paragraph 70 and *LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten*, paragraph 28).

In the Promusicae case, no Spanish law had been enacted permitting copyright holders to request users' personal data directly from ISPs so as to enable authors to start civil proceedings. By contrast, in *LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten*, Austrian legislators had specifically laid down a provision to empower persons who had suffered a copyright infringement with the right to start a proceeding against the violator and to require information on this regard to intermediaries (here included ISPs). Filtering technologies, however, were found excessive by the ECJ in Scarlet and Netlog.[77] These rulings exemplify the position adopted at the ECJ that the of Article 15(1) does not limit the range of rights that can be protected by ways of restricting the right to privacy, but does require rights at hand to be given a fair balance. The proportionality principle requires that the fundamental right to privacy cannot be restricted in such a way as to impose an exceptional burden to any of the parties involved, even when such restriction would enable the exercise of another legitimate right.

To conclude, a restriction which is in line with the wording of Article 15(1) of e-Privacy Directive and Article 13(1) of Data Protection Directive is one introduced by national legislation for activities of public security, national security, defence, and criminal prosecution. Such exceptions created at national

[74] C-101/01, Lindqvist [2003], ECR I-12971, paragraph 43.

[75] C-101/01, Lindqvist [2003], ECR I-12971, paragraph 43 and C-275/06, Promusicae [2006] ECR I-00271, paragraph 51.

[76] C-557/07, LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten [2009], ECR I-01227, paragraph 26.

[77] Fanny Coudert, *ACTA's referral to the ECJ: the European Commission's response to the concerns of EU citizens on digital enforcement of copyrigh*t, 4 May 2012. Retrieved from http://www.timelex.eu/en/blog/detail/actas-referral-to-the-ecj-the-european-commissions-response-to-the-concerns-of-eu-citizens-on-digital-enforcement-of-copyright

level can be relevant to facilitate the implementation and operation of ACDC, since anti-botnet tools classify as measures on the interest of public security and may gather data which are essential to criminal prosecution. Although the Directives do not restrict the range of rights that may be protected under the exceptions, national legislators must attempt to interpret their laws in accordance with EU laws and principles. This requires legislators to ensure a fair balance between the rights involved.

2.4.6 Data Subject, Controller and Processor: allocating liability

Directive 95/46/EC enumerates three important actors in the processing of personal data: data subjects, data controllers and data processors. Data subject is the person or organisation to whom/which the data relate.[78] On the one hand, the data subject enjoys the protection of the EU data protection framework and is entitled of a series of rights. On the other hand, data controllers and processors are the two actors involved in the processing of personal data and to whom the responsibilities of complying with the privacy standards are allocated. The definition of controllers and processors is given under Article 2(d) and (e) of Directive 95/46/EC,[79] respectively. Data controller is a person or organisation who/which determines the purposes and means of data processing. Data processor is a person or organisation who/which in practice carried out the processing of data.[80] According to the Article 29 Working Party, "*the existence of data processors depend on a decision taken by the controller, who can decide either to process data within his organization or to delegate all or part of the processing activities to an external organization. Two basic conditions for qualifying as processor are on the one hand being a separate legal entity with respect to the controller and on the other hand processing personal data on his behalf*".[81]

Although not at all times clear, the distinction between controllers and processors is one of a crucial impact. Controllers hold the primary duty to comply with the data protection requirements and bear the liability for violation of data protection.[82] The rights of the data subject, enumerated under Articles 10-12 and 14, are to be exercised against the controller, who is also central in ascertaining which is the applicable national law.[83] On the other hand, The concept of 'processor' plays an important role in the context of confidentiality and security of processing (Articles 16-17), as it serves to identify the responsibilities of those who are more closely involved in the processing of personal data, either under direct authority of the controller or elsewhere on his behalf.[84] Only under the circumstances of Article 23(2) will processors be held responsible for damages caused by non-compliance with the Directive, what only takes place if the controller proves that he is not responsible for the event giving rise to the

[78] Lee A. Bygrave, op. cit., p. 20.

[79] (d) controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;
(e) 'processor' shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;

[80] Lee A. Bygrave, op. cit., p. 21.

[81] Article 29 Working Party Opinion 1/2010 on the concepts of "controller" and "processor" adopted on 16 February 2010, p. 1.

[82] Christopher Kuner, op. cit., pp. 69-70.

[83] Article 29 Working Party Opinion 1/2010, p.5.

[84] Article 29 Working Party Opinion 1/2010, p. 5.

damage. Overall, all provisions setting conditions for lawful processing are essentially addressed to the controller, even if this is not always clearly expressed.[85]

ACDC envisages an ecosystem in which multiple partners collaborate to detect and disinfect botnets in the territory of EU Member States. Here, it is particularly important to adequately allocate the legal responsibilities borne by each of the actors involved. The first step is to identify whether the agent in question is acting as a data processor or controller. Albeit the Directive brought the definition for both processor and controller, in practice this may not be perfectly clear and must be analysed case by case. To this end, the legal distinction between 'controller' and 'processor' is not dependent on whether or not there is operational control over the data, but on the factual and substantive influence of deciding upon the purpose the processing, which characterises data controllers.[86] Other elements of distinction may include the degree of actual control exercised by a party, the image given to data subjects, and reasonable expectations of data subjects on the basis of this visibility.[87]

Currently, data processing often involves a complex and multi-layered structure in which several actors are responsible for different stages of the processing. In addition, "*the likelihood of multiple actors involved in processing personal data is naturally linked to the multiple kinds of activities that according to the Directive may amount to 'processing', which is at the end of the day the object of the 'joint control'*," in the words of the Article 29 Working Party.[88] Indeed, the very possibility of shared controllership in a single processing operation is envisioned by the Directive,[89] recognising that establishing whether or not a particular entity is to be considered as data controller is an extremely difficult task in the modern data processing environment.[90]

As technologies and business models evolve, the distinction between controller and processor becomes more unclear.[91] Nevertheless, as clarified by the Article 29 Working Party, even in cases where an actor is unable to directly fulfil all controllers' obligations, he/she is not exclude from being regarded as a controller.[92] In this case, co-controllers must ensure not only compliance with the rules relating to their part of the processing, but also clearly allocate responsibilities in the case of breach of these rules. In no circumstances data protection can be undermined by the intricate allocation of responsibilities of joint control. This requires co-controllers to openly inform data subjects about who is in charge of which stage of the processing and which controller is liable for the violation of each of the data subject's rights.[93] Failing to do so gives rise to joint liability, where all controllers will be held responsible for any data protection violation taking place in the processing.

Due to the pan-European character of ACDC and in light of Article 4 of the Directive, processors and controllers must observe the standards of the applicable national data protection laws. The application of a Member State data protection law depends on: 1. the establishment of the data controller in the

[85] Article 29 Working Party Opinion 1/2010, p. 4.
[86] Article 29 Working Party Opinion 1/2010, p. 8.
[87] Article 29 Working Party Opinion 1/2010, p. 12.
[88] Article 29 Working Party Opinion 1/2010, p. 18.
[89] Christopher Kuner, op. cit., p. 70.
[90] Christopher Kuner, op.. cit., p. 70.
[91] Christopher Kuner, op. cit., p. 72.
[92] Article 29 Working Party Opinion 1/2010, p. 22.
[93] Article 29 Working Party Opinion 1/2010, p. 22.

EU, 2. the use of equipment in a Member State by a non-EU data controller, and 3. Application of EU law based on public international law.

- How to determine who is a 'controller' and who is a 'processor'?

Each partner shall evaluate their position in the project so as to define whether their responsibilities are the ones of a controller or processor. Whenever a partners contributes, even if in conjunction with other partners, to the definition of the purpose and the means of the data collection, regardless of their participation in the operation aspects of the processing, it shall be regarded as a controller. This is a test which must be carried out in a case-by-case basis.

For instance, the partner controlling the operation of the AHPS solution under the Network Sensors group tool is processing personal data and determining the purpose and means of this processing. This partner is thus required to comply with all the data protection requirements set forth by Directive 95/46 and Directive 2002/58, where applicable, and with its national legislation. Moreover, since the information is later shared with the Centralised Clearing Data House, this amounts to a second processing. Here again the partner controlling the information generated by the AHPS solution must ensure compliance with all data protection requirements. However, the partner operating the receipt of this data in the CCH may also be acting as a co-controller.

2.4.7 Applicable National Law

ACDC is a EU-wide project which involves different jurisdictions and therefore different applicable legislations. For this reason, it is important for partners to understand when and in which circumstances national or foreign laws become applicable. Aware of the central role played by national laws, the project proposal has also defined the need for a study on the barriers and obstacles that ACDC could face across certain EU Member States.

As previously mentioned, defining the national law applicable to processing of data is a matter that depends on the elements and circumstances surrounding the operation. Under Article 4(1) (a) requires the application of the national law of the country where the data controller is established. Here, the main challenge is to define when a controller is established in a territory in the view of the Data Protection Directive. This is clarified in Recital 19 of the Directive, which requires controllers to have effective and real exercise of activity through stable arrangements in that territory. In order to prevent circumventions, the Directive adopted a practical approach, disregarding the legal form as the determining factor for defining the place of the establishment. Thus, if a branch or a subsidiary effective exercises the activity which is characterises the controller, there shall be its establishment. Furthermore, the Directive imposes on multinational controllers the duty to ensure that each of the establishments fulfils the obligations imposed by the national law applicable to its activities.

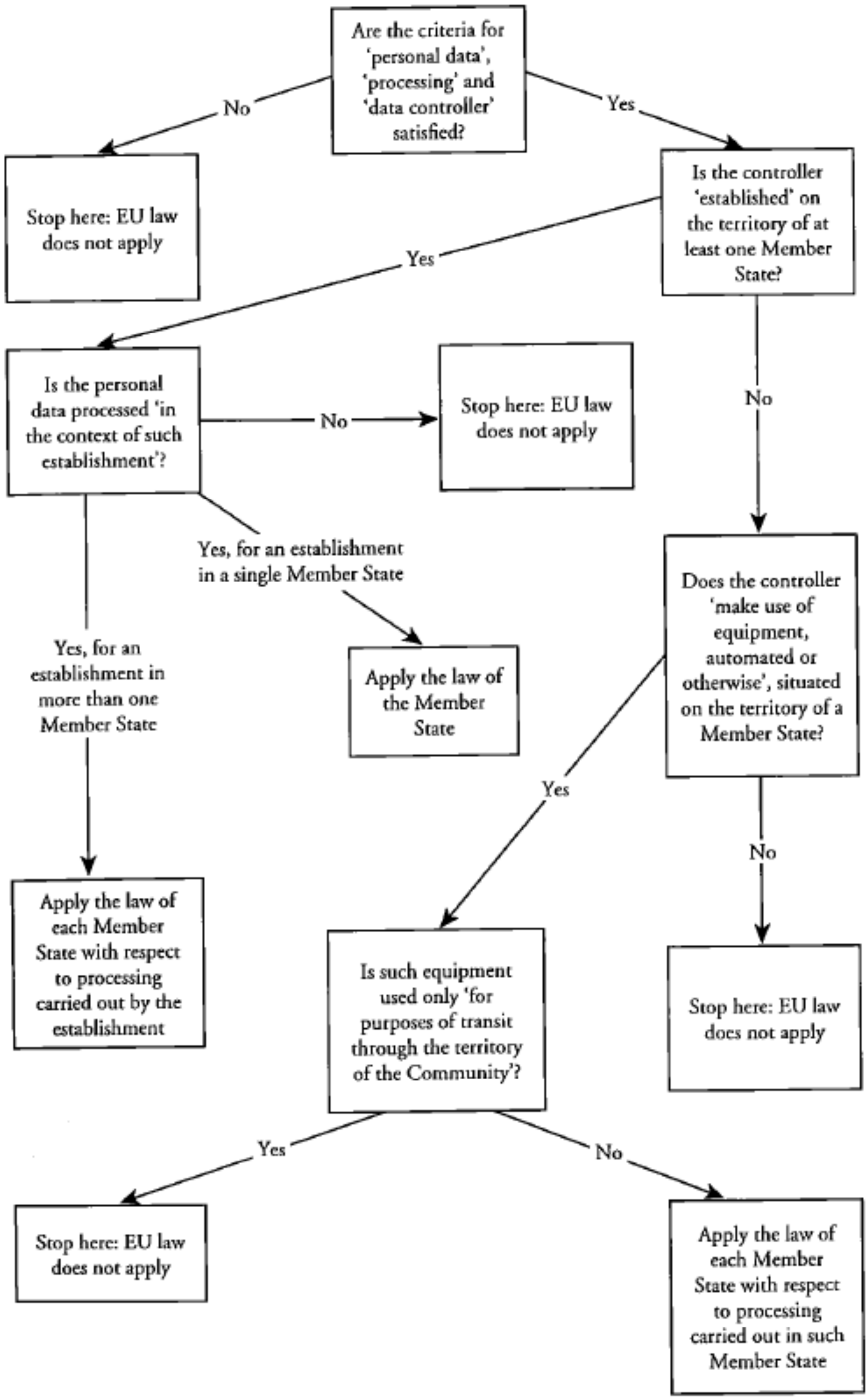
If the controller is established in a country outside the European Union, however, the first rule does not apply. In this case, the applicable national law shall be the one of the Member State where the equipment used by the controller is located, as long as such equipment is used only for purposes of transit inside the EU (Article 4(1) (c)). The Data Protection Directive does not bring a definition of equipment, but it is possible to presume that the operation or the ownership is not essential factors to characterise the use of the apparatus. The use of equipment will fall within the description of Article 4(1) (c) whenever the apparatus is used to determine the reason and the means of the control exercised by the data controller.[94]

Article 4(1) (b) deals with the possibility of application of international public law and intends to cover cases involving diplomatic and consular representations of the Union[95]. Therefore, not relevant to the context analysed.

In summary, if the controller has no establishment inside the EU and neither makes uses of any equipment placed in the territory of at least one of the Member States, or does so for the sole purpose of transit of communications, EU law does not apply to that specific processing carried out by the data controller. In all other cases, except the ones in which international law becomes relevant, controllers shall attempt to observe the data protection requirements set forth in the applicable national law, according to the criteria explained above. To this end, a practical scheme is provided below:

[94] Christopher Kuner, op. cit., pp. 120-121.

[95] Christopher Kuner, op. cit., p. 128.


Are the criteria for 'personal data', 'processing' and 'data controller' satisfied?
No
Yes
Stop here: EU law does not apply
Is the controller 'established' on the territory of at least one Member State?
Yes
No
Is the personal data processed 'in the context of such establishment'?
No
Stop here: EU law does not apply
Yes, for an establishment in a single Member State
Apply the law of the Member State
Yes, for an establishment in more than one Member State
Apply the law of each Member State with respect to processing carried out by the establishment
Does the controller 'make use of equipment, automated or otherwise', situated on the territory of a Member State?
Yes
No
Stop here: EU law does not apply
Is such equipment used only 'for purposes of transit through the territory of the Community'?
Yes
No
Stop here: EU law does not apply
Apply the law of each Member State with respect to processing carried out in such Member State

Source: Christopher Kuner, op. cit., p. 115.

2.4.8 Data protection principles

The EU Data Protection Directive 95/46/EC requires compliance with several principles relating to data quality set forth under Articles 6, 7 and 8. Only by abiding to these principles the processing of data can be regarded as legitimate. Due to the diversity of tools envisaged in the ACDC ecosystem, data processing operations will take place involving different data controllers, data subjects, and end purposes. Each group tool is composed by a set of technologies, and each of these solutions carry out their own processing with their own immediate objectives. This is to say that each processing shall be considered an individual operation. For this reason, each processing requires controllers to complying with all the data principles listed below.

2.4.8.a Fair and Lawful processing

The concept of fair processing embraces and generates other core principles of data protection.[96] Although the Data Protection Directive is silent in providing further information on what would constitute fair or unfair data processing, it is commonly acknowledge that fairness requires data controllers to take into account the interests and reasonable expectations of data subjects.[97] The concept of fairness of processing is thus linked to good faith and results in the idea that data collection must be carried out in a transparent way, as the data subject must receive the appropriate information from the person that collects the data.[98] It involves not only an examination of transparency of information about the processing, but also whether data was fairly obtained, and whether the data subject was misled or deceived about the purpose of the processing.[99] The notion of fairness also brings requirements of balance of interests and proportionality, as the collection and further processing cannot be carried out in a manner that unreasonably intrudes upon the data subjects' privacy or excessively interferes with their autonomy and integrity.[100] The proportionality element of fair processing also entails the obligation of data controllers to employ least intrusive means.

The Directive did not provide a conclusive definition of lawful processing either. Yet, it can be understood as a processing which is in accordance or not contrary to the law or is done with lawful justification or excuse.[101] The lawfulness of the processing requires: 1. data processing to be conducted only with legal basis and in compliance with all legal requirements, and 2. the right to data protection to be balanced against the interest of others in processing the data.[102] The legal grounds that legitimate data processing are brought under Article 7 of the Directive and refer to specific justification for processing:[103]

> Article 7
>
> Member States shall provide that personal data may be processed only if:

[96] Lee A. Bygrave, op. cit., p. 58.
[97] Lee A. Bygrave, op. cit., p.58.
[98] Data Privacy Commission, Belgium, http://www.privacycommission.be/de/node/6978
[99] Stewart Room, *Data Protection and Compliance in Context*, BCS, the Chartered Institute, p. 54.
[100] Lee A. Bygrave, op. cit., p.58.
[101] Lord Keith, House of the Lords in R v R, Ian Lloyd, op. cit., p. 96.
[102] Christopher Kuner, op. cit., p.90.
[103] Ian J. Lloyd, op. cit., p. 97.

> (a) The data subject has unambiguously given his consent; or
>
> (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or
>
> (c) processing is necessary for compliance with a legal obligation to which the controller is subject; or
>
> (d) processing is necessary in order to protect the vital interests of the data subject; or
>
> (e) processing 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 in a third party to whom the data are disclosed; or
>
> (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).

The exact meaning of each of the applicable legal grounds is explained into detail in section 2.4.9.

2.4.8.b Purpose Limitation

Embodied under Article 6(b) of Directive 95/46/EC the principle of purpose limitation or finality requires personal data to be 'collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.' According to the Article 29 Working Party, 'the principle of purpose limitation is designed to establish the boundaries within which personal data collected for a given purpose may be processed and may be put to further use. The principle has two components: 1. the data controller must only collect data for specified, explicit and legitimate purposes, and 2. once data are collected, they must not be further processed in a way incompatible with those purposes'.[104]

Data subjects have the reasonable expectation that their data will only be used in accordance with the purposes for which the data was first collected. The very core of purpose limitation is to ensure this legitimate expectation is respected and to restrain the use of information in forms of processing that the data subject could have not anticipated or would not agree to. For that, the purpose must be specified, explicit and legitimate. This is to say that before data can be collected, data subjects have to clearly understand what is the extent of the processing, meaning what does it include and what is not part of it. Also, it must encompass one of the legal grounds set forth under Article 7 of Directive 95/46/EC. A legitimate purpose embodies a specific justification for the data processing.[105]

The second component of the principle brings the notion of compatible re-use. It is to say that even when data is collected for a certain purpose, another lawful form of processing can take place. As long as the data is used for a compatible purpose, additional processing will not be regarded as unlawful. The criteria for compatible purpose is one of negative nature: further forms of processing cannot take place when not compatible with the original purpose that allowed collection in first place. For further

[104] Article 29 Working Party Opinion 03/2013 on Purpose Limitation adopted on 2 April 2013, p. 4.

[105] Ian J. Lloyd, op. cit., p. 97.

details on the incompatibility test, we refer readers to the Article 29 Working Party Opinion 03/2013 on Purpose Limitation. For now it suffices to say that compatible re-use requires a careful analysis and that in line of principle data controllers shall restrain from giving further processing to data that was collected for a different initial purpose.

2.4.8.c Data Minimization

Embodied in Article 6(1)(c), the principle of data minimization is double fold: it asks controllers to ensure the adequacy and relevance of the collected data while keeping the amount of personal data to the minimum necessary to achieve the purpose of the processing.[106] In addition, the adequacy and relevance components are to be interpreted strictly,[107] so as to preserve the interests of the data subject. The data minimization is not only a limit on the quantity but also on the nature and quality of personal data intended for processing.

By reducing the amount of personal data needed, data controllers can ensure better compliance with data protection requirements. Data minimization results in lesser interference in the private life of data subjects, enables greater balance of interests and proportionality, and reduces the risks of privacy and security breach.

2.4.8.d Data accuracy

Personal data should be valid with respect to what they are intended to describe, and relevant and complete with respect to the purposes for which they are intended.[108] Inserted under Article 6(d), the principle of information quality stresses the obligation of data controllers to ensure the correctness of and reliability on the data they process. Data is regarded as being inaccurate when it is incorrect or misleading to any matter of fact.[109] Finally, it requires controllers to take all the appropriate measures to enable erasure or rectification of incorrect or incomplete data in light of the purpose for which they are collected and processed.[110] This duty is of permanent character and lasts for the duration of the processing, calling for data to be kept updated, when circumstances require so.

2.4.8.e Storage limitation

Pursuant to Article 6(1)(e), personal data shall not be retained longer than necessary for achieving the purposes for which the data were first collected or further processed. The period of retention shall be specified before the start of the processing and is part of the controller’s duty of transparency, as embodied in the principle of fairness. This is because the duration of the data retention for periods beyond the required for the processing can violate the principle of proportionality: it places a burden on the data subject privacy without justification.[111] Since the Directive 95/46/EC does not establish a fixed duration for legitimate data storage, this will be defined case by case. Clearly, the period of the storage shall depend on the purpose of retention and collection, on the nature more or less sensitive

[106] Lee A. Bygrave, op. cit., p. 59.
[107] Waltraut Kotschy, op. cit., p. 45.
[108] Lee A. Bygrave, op. cit., p. 62.
[109] Ian J. Lloyd, op. cit., p. 117.
[110] Philippe Meier, *Protection des données*, Stämpfli [2010], p. 287.
[111] Philippe Meier, op. cit., p. 272.

of the data, and on aspects of security, as data protection risks increase with time.[112] In effect, the principle of storage limitation appears to require data subjects to operate some form of policy for monitoring their data controllers and removing items which are no longer of value or relevance to their activities.[113]

In order to comply with the storage limitation principle, data controllers can erase or anonymise the personal data held under their control once they are no longer essential. While the first option results in the destruction/elimination of data, the second removes the identifiability component and turns the data into non-personal. This process is called anonymisation and will be specifically discussed below.

2.4.9 Grounds for legitimate processing

The principle of lawful processing of data is complemented by Article 7 of Directive 95/46/EC, which lists six categories for the legitimate processing of data. In line of principle, the approach of the Directive is to do not permit processing of personal data, unless under the circumstances provided in Article 7. For the sake of efficiency, however, we have limited our analysis to the grounds that are reasonably applicable to ACDC, namely Article 7(a), (b), (c), and (f). .

ACDC can be described as a multi-layered project. It results that it involves five group tools with different characteristics and end results. Moreover, each of these five tools is composed by a set of multiple technology solutions intended to deal with various issues. Each data processing operation, however, regardless of position and influence in the project architecture, must ensure observance to the data quality principles as much as to all data protection rules enacted through the Data Protection Directive. This is to say that each operation must be legitimised through one of the grounds listed in Article 7.

In the joined cases C‑468/10 and C‑469/10, the ECJ examined the legitimate character of further requirements to Article 7 of the Data Protection Directive and found that Member States cannot add new principles relating to the lawfulness of the processing of personal data to Article 7 or impose additional requirements that have the effect of amending the scope of one of the six principles provided for in that article[114]. This is to say that national measures that provide for additional requirements amending the scope of a principle referred to in Article 7 of Directive 95/46 are precluded, in the words of the ECJ[115].

Finally, defining an agent to be responsible for supervising the data collection within the ACDC environment is an important step that can help partners understand which are their legal duties within the project. It will not only facilitate compliance with legislation, but enhance trust and confidence in the operated tools as well as influence the balance of interest between partners and users.

2.4.9.a Unambiguous consent (Article 7(a))

[112] Philippe Meier, op. cit., p. 273.
[113] Ian J. Lloyd, op. cit., p. 119.
[114] ECJ in joined cases C‑468/10 and C‑469/10, p. 32.
[115] ECJ in joined cases C‑468/10 and C‑469/10, p. 35.

As noted by Lloyd, consent is a fundamental element in the field of contract law since silence cannot constitute acceptance of an offer.[116] The definition of consent used in the Directive is enshrined under Article 2(h) and shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed. The requirement of data subject consent can be further explained by the risk imposed to the personality rights of an individual by the processing of personal data.[117] As expressed by Article 29 Working Party, consent is a term particularly used in contract law and, although the Directive does not refer to the validity criteria used in this field, there is no contradiction but overlap between the notions of consent in the context of data protection and contract law, and that *"in addition to the application of the general conditions for the validity of consent under civil law, the consent required in Article 7(a) must also be interpreted taking into account Article 2(h) of the Directive."*[118]

According to the Article 29 Working Party, consent needs to respect the wishes of the data subject and be freely given, meaning it is only valid "*if the data subject is able to exercise a real choice, and there is no risk of deception, intimidation, coercion or significant negative consequences if he/she does not consent*."[119] A valid consent entails the need for specificity, so as to precisely identify what purpose and use is covered by the data subject consent and what is not included in it. Consent involves also the need for disclosure of all the relevant information that may influence the judgement and the choice of the data subject, coinciding with the set of information controllers are expected to provide in the terms of Articles 10 and 11 of the Directive[120] and taking into account the context and the audience they are targeting.[121]

In the online world, the issue of consent gains greater complexity, as automation increasingly simplifies the form by which data subjects can "agree" with the processing (e.g. by marking a box or clicking in "yes, I agree" to proceed). Lloyd affirms that "*in many cases, data subjects may not read the notice or may be unaware of the full implications of what is being proposed.*"[122] For this reason, the Directive asks for unambiguous consent, raising the threshold for data controllers. A definition of unambiguous, however, is not provided by the Directive. The Article 29 Working Party clarifies the gap by ascertaining that *"for consent to be unambiguous, the procedure to seek and to give consent must leave no doubt as to the data subject's intention to deliver consent"*[123] and complements the notion by stating that "*unambiguous consent does not fit well with procedures to obtain consent based on inaction or silence from individuals: a party's silence or inaction has inherent ambiguity."*[124]

The examination of valid and unambiguous consent can only be defined in a case-by-case basis, as none of the elements are static and thus subject to the circumstances of the occasion. For example, the possibility of unambiguous consent be compatible with either an opt-out or opt-in option is a

[116] Ian J. Lloyd, op. cit., p. 97.
[117] Philippe Meier, op. cit., p. 341.
[118] Article 29 Working Party, Opinion 15/2011 on the definition of consent adopted on 13 July 2011, p. 6.
[119] Article 29 Working Party, Opinion 15/2011, p. 12.
[120] Article 29 Working Party, Opinion 15/2011, p. 19.
[121] Article 29 Working Party, Opinion 15/2011, p. 20.
[122] Ian J. Lloyd, op. cit., p. 97.
[123] Article 29 Working Party, Opinion 15/2011, p. 21.
[124] Article 29 Working Party, Opinion 15/2011, p. 24.

controversial topic. However, it the controller provides reasonable clarity on the notification,[125] meaning not only all the relevant information to data subjects in realistic format and language, but also creating reasonable opportunities for consent to be validly and timely expressed,[126] before the processing starts,[127] this could be regarded as a lawful consent in the terms of the Directive. In addition, the Article 29 Working Party clarifies that "*the notion of control is also linked to the fact that the data subject should be able to withdraw his consent. Withdrawal is not retroactive, but it should, as a principle, prevent any further processing of the individual's data by the controller.*"[128]

When collecting users' consent, at least one of the operators involved in the processing must be charged with collection and registration of such consent, ensuring legal consent requirements are satisfied. The choice of which partner shall be responsible for this task will clearly depend on the architecture of the tool. ACDC partners with a public mandate or with whom the end user has a direct contractual relationship may act as the default operator charged with collecting consent, as this position facilitates collection and registration.

2.4.9.b Necessity in a contractual or pre-contractual context (Article 7(b))

This provision covers the cases in which the processing of personal data is necessary, meaning close to essential,[129] for the performance of the contract. This possibility is interpreted by some scholars very strictly, as the necessity criteria will not be considered as such unless the processing is truly central and unavoidable in order to complete the transaction.[130]

Nevertheless, the Working Party 29 considers that by setting up filtering systems, email providers can also be considered as ensuring the performance of the service contract with their customers, who expect to receive and send emails with a certain degree of security. Accordingly, the processing of data in which email service providers are engaged when they set up a filtering systems may also be legitimised under Article 7(b) of the Data Protection Directive which foresees the processing of data 'necessary for the performance of a contract to which the data subject is a party'."

2.4.9.c Compliance with a legal obligation (Article 7(c))

This provision only applies in the case of a mandatory legal obligation and in circumstances where the data controller is truly obliged to comply with the legal requirements placed on him/her.[131] The application of this justifying ground is to be interpreted strictly and requires the existence of a true legal obligation where the controller is not given the choice to comply or not with the norm.[132] This provision is essential to ACDC, particularly to the Network Sensors and Website Analysis tools. This is because partners involved in these tools may reasonably justify the processing of personal data based on their duty to ensure security of communications, as required by Article 17(1) of Data Protection Directive and Article 4 of e-Privacy Directive.

[125] Ian J. Lloyd, op. cit., p. 98.
[126] Ian J. Lloyd, op. cit., p. 98.
[127] Article 29 Working Party, Opinion 15/2011, p. 9.
[128] Article 29 Working Party, Opinion 15/2011., p. 9.
[129] Ian J. Lloyd, op. cit., p.100.
[130] Christopher Kuner, op. cit., p. 244.
[131] Christopher Kuner, op. cit., p. 244.
[132] Christopher Kuner, op. cit., p. 244.

The screening and analysis of malicious activities is a security measure that protects the network of service providers and their users. The duty to ensure security amounts to a legal binding obligation provided by the directives and measures taken to guarantee the security of networks can of thus have its processing legitimised under Article 7(c) as discussed under 4.2 Network Traffic Sensors and Malware Website Analysis tools.

2.4.9.d Performance of a task in the public interest or in the exercise of public authority vested in a controller (Article 7(e))

The scope of this provision is twofold: it covers cases in which data controllers may be required to meet certain obligations in the public interest as well as situations in which data controllers operate as delegated authorities from government institutions.[133] Although the goal of ACDC is to protect society from botnets, the limits in which the provision was drafted and the interpretation given to it is rather restrictive. As noted by Kuner, many DPAs tend to limit the application of Article 7(e) to quasi-governmental activities only.[134] All and all, this is not applicable at large to the ACDC project, as private sector partners do not operate as delegated authorities nor exercise functions of a public nature in the public interest. However, this may be the case for CERTs, which can use such exception to legitimise their data processing.

2.4.9.e Legitimate interest of the controller and third parties, except where such interests are overridden by the fundamental rights and freedoms of data subjects (Article 7(f), "balance" provision)[135]

This provision is often used by companies seeking for a legitimate excuse in the processing of personal data.[136] The lawfulness of the operation, however, asks for a test based on the legitimacy and necessity of the processing, and balance between the interests of controllers and data subjects. The concept of legitimate processing overlaps several provisions of the Directive and works as an open-clause mainly asking for fairness of data processing.[137] Besides fair and lawful, the processing needs to be necessary to achieve the legitimate interest of the data controller. This is to say that it cannot be just convenient or helpful, but needs to be essential to the realization of the legitimate interest in question. Finally, the processing cannot be outweighed by the fundamental rights and freedoms of the data subject.[138] The application of the balance criteria is fundamentally dependant on the implementation of the Directive into national laws, and cannot be analysed in a pan-European basis.[139]

In its analysis and impact study on the implementation of Directive EC 95/46 in Member States, the European Commission noted that "*the 'balance' criterion, Art. 7 (f), is set out in the words used in the Directive or in very similar terms in the laws of only eight Member States. Several of these intend to*

[133] Christopher Kuner, op. cit.,p. 244.
[134] Christopher Kuner, op. cit.,p. 244.
[135] Douwe Korff, *Comparative Study On Different Approaches To New Privacy Challenges, In Particular In The Light Of Technological Developments*, Working paper no. 2, p. 68.
[136] Christopher Kuner, op. cit., p. 245.
[137] Christopher Kuner, op. cit., p. 245.
[138] Christopher Kuner, op. cit., p. 76.
[139] Christopher Kuner, op. cit., p. 245.

issue further clarification on its application but have not yet done so - but the kinds of matters to be taken into account are clear from other Member States: the nature of the data; the nature of the processing; whether the processing is carried out in the private sector or the public sector (with the latter being subject to a stricter assessment); and the measures which the controller has taken to protect the interests of the data subject."[140]

Finally, Article 7(f) may be used as a legal ground for the processing of personal data in ACDC, but this will largely depend on the national implementation, namely case law and interpretation of Data Protection Authorities. Article 7(f) is particularly important for being the most likely provision to be used to legitimise the sharing of personal data with of the Centralised Clearing House and their further processing by the CCH. This article implies a proportionality assessment, i.e. to weigh the legitimate interest (ensuring security of the network) of ISPs, webmasters, hosts, security companies, CERTs against the need to protect data subjects' fundamental rights (confidentiality of communications). In particular, the necessity of creating a centralised platform such as the CCH and of the tasks entrusted to such platform should be assessed. It is thus crucial to examine the implementation of article 7(f) by national legislators and the interpretation of the DPAs on the use of such provision. This is further discussed under the national comparative analysis.

2.4.10 Confidentiality and Security of processing

The duty to ensure confidentiality and security of the processed data is presented under Articles 16 and 17 of Directive 95/46/EC and has the main purpose of avoiding data breach. Article 16 requires any person acting under the authority of the controller, including not just his own immediate staff but also processors (agents), to only process personal data as instructed by the controller (unless required by law to do otherwise).[141] It is a requirement that ensures only legitimated persons can have access to the processing of data.[142]

In addition, Article17(1) instructs data controllers to put in places technical and organisational measures that guarantee an optimal level of security to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access. It is a duty to safeguard the integrity and authenticity of the data.[143] It is in the interest of both data subject and data controllers to have the processed personal data kept confidential and secured.

The burden of ensuring these standards have been accomplished, however, weights on the data controller, who must consider the state of the art and the costs to prevent risks associated with the nature of the processed data. The Directive gives controllers freedom to define, in a case by case basis, which is the appropriate level of security to be deployed. As the security principle is not static,

[140] COM(2003) 265 final, Commission's First Report on the transposition of the Data Protection Directive, Technical analysis of the transposition in the Member States [2003], p. 10.

[141] Douwe Korff, Working paper no. 2, op. cit., p. 87.

[142] Philippe Meier, op. cit., p. 301.

[143] Philippe Meier, op. cit., p. 301.

the evolution of risks and technologies obliges controllers to carry out periodic re-exams on the level of security of their processing.[144]

Finally, Article 17(2) and (3) of Data Protection Directive asks for controllers to ensure they have chosen data processors capable of providing sufficient guarantees on technical and organizational measures regarding the security of processing via contract or other legal binding act. These provisions entail the primary responsibility of controllers to certify the reliability of the processors they designate to carry on their work, while creating a secondary responsibility for processors to ensure security of the processing.

In the framework of the e-Privacy Directive, Article 4 instructs providers of communications services to take appropriate technical and organisational measures to safeguard the security of their services. Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risks associated with the processing. Article 4(1) of the e-Privacy Directive mirrors Article 17(1) of the Data Protection Directive, and a similar interpretation shall be given to the common terms and elements.

Nevertheless, due to the greater risks associated with public available networks, the e-Privacy Directive elaborates further on the service provider duty to guarantee security and confidentiality of the processing. The measures implemented by the providers must ensure at least, and without prejudice of the obligations listed in the Data Protection Directive, data access restricted to authorised personnel and only for legally authorised purposes, data security and integrity, and implementation of a security policy with respect to the processing of personal data (Article 4(1a)). As noted by Lloyd, *"the security and confidentiality obligation imposed upon service providers are twofold. First, appropriate security measures must be put in place to protect data and, second, customers must be warned of the risks involved and advised about self-help measures such as encryption which may be used and of the likely costs of such measures."*[145] This progressive approach contributes to a more proactive participation of users in safeguarding security of data processing. It is undeniable that users play a major role in the security and confidentiality of data. However, users can only do so to the extent they have been informed about the risks faced in a certain operation, as well as the reasonable remedies and alternatives they can engage to in protecting their data.

The e-Privacy Directive also innovates in sharing the responsibility of safeguarding data security between providers and national authorities. Article 4(1a), last part, establishes that the relevant national authorities shall be able to audit the measures taken by providers of publicly available electronic communication services and to issue recommendations about best practices concerning the level of security which those measures should achieve. This provision is of particular importance in recognising that self-regulation is not sufficient to ensure security of data processing, and that governments must also play a role in the supervision and control of the security standards deployed by the private sector.

[144] Philippe Meier, op. cit., p. 304.
[145] Ian J. Lloyd, op. cit., p. 166.

The duty to promote confidentiality of communications is brought under Article 5 of the e-Privacy Directive. Here Member States are called upon imposing legal sanctions to breach of confidentiality and prohibiting any form of interception or surveillance of communications without user's consent. Recital 24 highlights the prohibition of spyware, web bugs, hidden identifiers and other similar devices able to enter users' terminals without their knowledge in order to gain access to information, to store hidden information or to trace the activities of the user and may seriously intrude upon the privacy of these users. The threshold to the deployment of these technologies is the presence of a legitimate purpose allied to user's consent, which requires compliance with the grounds set forth by the Data Protection Directive.

In the e-Privacy Directive a service provider can be exempted from the confidentiality rule if: 1. Technical storage is necessary for the conveyance of a communication; 2. Legally authorised recording of communications and related traffic data are carried out in the course of lawful business practice for providing evidence of a commercial transaction; or 3. Technical storage or access is strictly necessary in order for a service provider to provide the service. In doing so, the e-Privacy Directive acknowledges the minimum ground of processing service providers need to carry out in order to perform their contractual duties. In any case, the processing of data is expected to be kept to a minimum, and in no circumstances excludes the need of compliance with all the data protection principles listed under the Data Protection Directive and in the complimentary provisions of the e-Privacy Directive.

- Are ISPs allowed to 'detect' and 'filter' malicious traffic under their network?

Albeit not addressing botnets in particular, the Article 29 Working Party opinion 2/2006 on privacy issues related to the provision of email screening services is relevant to our analysis. The conclusions achieved by the Article 29 Working Party are applicable to the ACDC tools, due to the similarity of means, object and purposes of mitigation techniques between spam and botnets:

"*In assessing the legal grounds that legitimate this practice, the Working Party 29 is of the opinion that the setting up and use of filtering systems by email providers for the purpose of detecting virus might be justified by the obligation to take appropriate technical and organisation measures to safeguard security of their services as foreseen in Article 4 of the e-Privacy Directive.*"

The Article 29 Working Party continues its report by affirming that the danger posed by emails containing malware is a threat to the service provider network, which can impair the transmission of further communications and possibly result in damage of end-user devices[146]. Therefore, by putting in place security mechanisms to filter malicious communications content, the data controller may in fact be ensuring the protection its own network and complying with the duty enshrined under Article 4 of e-Privacy Directive. Furthermore, these mechanisms are also regarded as measures undertaken to guarantee the performance of the service as contracted by the customer. This being said, the deployment of technical tools for the purpose of ensuring security and continuation of the service may fall within the legitimate grounds of Article 7(b) and (c) of the Data Protection directive.

[146] Article 29 Working Party opinion 2/2006 on privacy issues related to the provision of email screening services.

In light of the above, the implementation of mitigation mechanisms to fight botnets can be aligned to Article 4 of the e-Privacy Directive, which requires providers to take appropriate measures to safeguard the security of their services. In fact, Recital 53 of Directive 136/2009 amending the e-Privacy Directive explicitly recognised that the processing of traffic data to the extent strictly necessary for the purposes of ensuring network and information security, 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 data, and the security of the related services offered by, or accessible via, these networks and systems, by providers of security technologies and services when acting as data controllers is subject to Article 7(f) of Directive 95/46/EC. This includes preventing unauthorised access to electronic communications networks and malicious code distribution and stopping denial of service attacks and damage to computer and electronic communication systems.

As noted by the Article 29 Working Party, the damage caused by malware can be strong enough to shut down the system and impair the continuity of the transmission of communications. Mitigation measures enabling filtering, detection, and analysis are thus fair means of protecting the service provider network as well as customers' data. Malware can affect the integrity of the data processed in the network and consequently impair the performance, trustworthiness, reliability, and continuity of the service. This will hamper service providers to ensure their contractual obligations, giving them the right to proportionally and adequately respond to threats.

Security mechanisms, however, must observe the limits created by the Data Protection Directive and, when the former is not applicable, even then a user can still hold the legitimate expectation that his data will be treated fairly and in respect to fundamental rights. The Article 29 Working Party recalls that security tools, even if operating under legitimate grounds, cannot result in disclosure of the content of the communication[147]. Moreover, they should be set up automatically and only for the purpose of detecting malware[148]. This is to say that service providers shall not access the content of a communication, as this would amount to an imbalance between the right to react against malware and the data protection rights held by users. Because human intervention creates higher risks of privacy breach, such mechanisms must operate automatically. Moreover, data controllers must ensure appropriate safeguards are put in place to enable user exercise of his data subjects' rights.

Filter, sensors, immunization mechanisms and all other means put in place with the goal of fighting malware must be informed to the customer, affirms the Article 29 Working Party. This shall be included under the contractual conditions of the service, as well as any other relevant information regarding the risks of security breach, remedies and other instruments subscribers can use to protect the confidentiality of their communications.

Finally, a legal obligation may arise from the contractual terms established between the ISP and the user. Besides positive obligations, a contract also imposes on parties negative duties, such as de obligation of non-interference. Most service providers Terms of service include customer's obligation

[147] Article 29 Working Party opinion 2/2006 on privacy issues related to the provision of email screening services.
[148] Article 29 Working Party opinion 2/2006 on privacy issues related to the provision of email screening services.

to do not attempt against the security and continuity of the network and the prerogative of ISPs to disconnect users part to a malicious structure, such as botnets, for violating customer duties. ISPs' duty to provide for the continuity and security of the network may also derive from the same contractual obligations. In this case, ISPs should not be impaired from using Article 7(c), as contractual clauses create laws between the parties to the contract.

2.4.11 Data subject rights

The Directive 95/46/EC established rules not only requiring data controllers to inform data subjects about data processing operations (Articles 10-11), but also recognising data subjects rights to be exercised against data controllers (Articles 12, 14 and 15).

2.4.11.a Information rights

Articles 10 and 11 recognise the right of individuals to be directly informed by the data controller about basic aspects of processing involving their personal data, regardless of the data subjects' use of access rights.[149] The right to information exists whether or not the data was obtained from the data subject. It entails the controller and his representative's obligation to specify: (a) their identities; (b) the purposes of the processing; (c) any further information such as the categories of data concerned, the recipients or categories of recipients, and the existence of data subject's right of access and rectification. Information rights are part of the fair processing principle and must be always provided.

In the ACDC scenario, partners involved in a given group tool may agree on a standard information notice specifying all the elements requested by Articles 10 and 11. This must be presented in an accessible and understandable language, taking into account the profile of the targeted audience. Disclosure of all the relevant information is essential to obtain valid unambiguous consent from data subjects. The partner holding a contractual relationship with the data subject shall be responsible for demonstrating the collection of lawful consent as much as for putting in place mechanisms that allow data subjects to at any time withdraw their consent.

2.4.11.b Right of access

Article 12 grants data subjects access rights, which can be described as the right to obtain a set of information from data controllers. The right of access is at the core of data protection and is especially important for allowing data subjects to be in control, as they themselves are the most interested actors in ensuring data protection standards are being respected.[150] The right of access as provided under Article 12 can be broken up in:[151]

- *right to confirmation* as to whether or not data relating to the data subject are being processed by a particular controller and, if so, to be given details of the processing (Article 12(a), first indent, of the Directive);
- *right of access to one's data*, including the right to be given a copy of the data in question, with "any available information as to their source" (Article 12(a), second indent); and

[149] Lee A. Bygrave, op. cit., p. 64.
[150] Stewart Room, op. cit., p. 79.
[151] Douwe Korff, Working paper 2, op. cit., p. 76.

- *right to rectification, erasure or blocking* if the data do not conform to the Directive, in particular, if they are incomplete or inaccurate (Article 12(b) and (c)).

The right of access shall be exercised without constraint and free of charge, at any time within three months from the receipt of the request (Article 13 of Regulation (EC) No 45/2001.[152] Other aspects on the exercise of this right are defined by national laws and practical elements regarding the level of information to be provided, the application of a reasonable fee, if the information can be redacted in face of special circumstances, etc., are also to be answered by national legislators.[153]

ACDC data controllers shall put in place mechanisms to enable data subjects to enforce their right of access and related rights (right to confirmation, right of access to one's data, and right to rectification, erasure and blocking). The API key system to be used in the community platform, while designed as a data confidentiality and security mechanism, holds the potential to also be used as a tool to facilitate the exercise of data subjects rights. Through the API key system, the platform has an overview of which data is sent to the CCH and to whom the data relates. Such control is likely to help the CCH respond to the exercise of data subjects rights in a fair and responsible manner.

2.4.11.c Other rights

Additional rights are enumerated in the Directive: 1. a general right to object to the processing of one's personal data, when the processing is consented (Article 14(a)) , 2. a more specific right to object to direct marketing use of one's data (Article 14(b)); and 3. a new right not to be subject to fully automated decisions based on personality "profiles" (Article 15) combined with a right to be informed, on request, of the "logic" used in such decisions (Article 12(a), third indent).[154]

The right to object as described under Article 14(a) has the meaning of preventing at any time the processing of personal data out of the legitimate grounds of Article 7. It is clear that data processing out of the circumstances enumerated by Article 7 constitutes an unlawful processing, what shall give data subjects a clear right to stop the operation, due to its illegitimate character.

Finally, Article 15 gives individuals the right to not be subject to a decision which produces legal effects concerning or significantly affects him/her, being solely based on automated processing of data intended to evaluate personal patterns and characteristics. Such treatment can be unfair to the ones that do not match the automated profiling,[155] but every time harder to be avoided with the proliferation of information systems. Nevertheless, automated decisions are to be permitted in contracts where the outcome is favourable to the data subject or when authorised by law to safeguard the legitimate interests of the data subject himself/herself (Article 15(2)).

Albeit ACDC does not involve any activities of direct marketing, the general right to object unlawful processing of data and the right to do not be submitted to automated decisions based on patterns of

[152] European Data Supervisor, Glossary: right to access. https://secure.edps.europa.eu/EDPSWEB/edps/site/mySite/pid/86

[153] Christopher Kuner, op. cit., p. 64.

[154] Douwe Korff, Working paper no. 2, op. cit., p. 76.

[155] Ian J. Lloyd, op. cit., p. 150.

personal behaviour remain valid. This is to say partners must install safeguards that enable data subjects to exercise these rights adequately.

2.4.12 Notification of data processing to the DPAs

The Data Protection Agencies are supervisory agencies projected by Article 28 of Directive 95/46/EC as independent bodies vested with powers to investigate, to intervene and to engage in legal proceedings. In fact, the DPAs are central elements in the exercise of data subjects' rights, as they are responsible for hearing claims on the violation of privacy in the processing of personal data (Article 28(5)). As entailed by Article 18 of Directive 95/46/EC, data controllers shall bear the duty to notify the competent DPA on the nature of the processing activities. Nevertheless, Article 18 does not go as far as to give any powers to the DPAs in this matter, as it does predict the possibility of rejection of notification, although permitting the use of the notification information by DPAs to initiate enforcement actions.[156] The notification to the DPA must include but is not limited to:[157]

1. The name and address of the controller and of his representative;
2. The purpose of the processing;
3. A description of the categories of data subjects and of the data or categories of data relating to them;
4. The recipients or categories of recipients to whom the data might be disclosed;
5. The proposed transfers of data to third countries, and
6. A general description allowing a preliminary assessment to be made of the appropriateness of the measures taken pursuant to Article 17 to ensure security of processing.

Breach of the duty to notify the DPA constitutes an offence in the terms of Article 18(2).[158] Controllers are requested to keep notifications up to date in the case of any changes as defined by national law (Article 19(2)).[159] As noted by Kuner, notification to the DPA is not the same as prior checking, as the latter mandates certain types of data processing to be examined by the DPA before the activity can be conducted (Article 20). The author continues by observing that *"prior checking is specifically meant to be used in certain cases of data processing that are likely to present particular risks to individual rights."*[160]

2.4.13 Transborder data flows

Pursuant to recitals 3 and 9 of Data Protection Directive, the equivalent protection resulting from the approximation of national guarantees the free movement of data inside the EU. This is because the establishment and functioning of an internal market requires not only that personal data should be able to flow freely from one Member State to another, but also that the fundamental rights of individuals should be safeguarded. However, stringent rules apply to the transfer of personal data to countries outside the Union, as provided by Article 25 of Data Protection Directive. Cross border data flows may only be established with third countries that offer an 'adequate' level of protection, which

[156] Ian J. Lloyd, op. cit., p. 66.
[157] Christopher Kuner, op. cit., p. 248.
[158] Ian J. Lloyd, op. cit. p. 66.
[159] Christopher Kuner, op. cit., p. 249.
[160] Christopher Kuner, op. cit., p. 250.

must be assessed in the light of all the circumstances surrounding the transfer operation. The adequate level of protection is not a static concept and will depend on the nature of the data, the purpose and duration of the proposed processing operation, the country of origin and country of final destination, the rules of law of the third country and the professional rules and security measures which are complied with in that country (Article 25(2)).

The Commission recognised the presence of an adequate level of protection in Andorra, Argentina, Canada, Switzerland, Faeroe Islands, Guernsey, State of Israel, Isle of Man, Jersey, the US Department of Commerce's Safe harbor Privacy Principles, and the transfer of Air Passenger Name Record to the United States' Bureau of Customs and Border Protection as providing adequate protection.[161] The Safe Harbor framework was developed by the U.S. Department of Commerce in consultation with the European Commission[162] and ensures that transfers of personal data may take place to between the EU and U.S. companies without needing to fulfil any specific formal requirement. However, the presence of an adequate level of protection does not preclude the need for EU controllers to comply with all the data protection standards required by the Data Protection Directive.

The adequate level of protection is an open concept which shall be assessed by Data Protection Authorities in light of the circumstances of the case. Personal data transfers to certain third countries have however already been authorized by the EC. Switzerland has been acknowledged as providing an adequate level of protection, thus data transfers are authorized. However special arrangements would be required to transfer data to Japan and Australia, two potential ACDC partners. Similarly, transfers to the US are limited to organizations which have self-certified to the Safe Harbour Agreement and to transfers with commercial purposes. After the NSA scandal, the agreement is being reviewed and its application might be suspended.

The Article 29 Working Party[163] noticed the significant divergences between the legislations of the various Member States in implementing Articles 25 and 26 of the Directive and the risk that this could ultimately lead to forum shopping among the Member States. Since the directive does not specify whether an authority should be charged with assessing the adequacy of data protection in third countries, it is possible that Member States give this task to national data protection authorities, whose authorisation may be required prior to the transfer. In fact, fifteen States of the EEA require some degree of prior notification before a processing operation with third countries can occur.[164]

In the absence of an adequate level of protection, Member States may make use of derogations provided by Article 26. The first possibility is given by Article 26(1), where a set of circumstances mirroring the legitimate grounds of Article 7 will permit Members to authorise transfer of data to countries, even if they do not hold an adequate level of protection recognised by the EU. In the absence of such circumstances, one can still use paragraph 2 as alternative justification. Article 26(2) specifies that without prejudice of Article 26(1), transfer of personal data to a third country may be

[161] Ian J. Lloyd, op. cit., p. 187.

[162] Welcome to the U.S.-EU & U.S.-Swiss Safe Harbor Frameworks, http://export.gov/safeharbor/

[163] Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995. P. 3.

[164] Ian J. Lloyd, op. cit., p. 192. These countries are Austria, Bulgaria, Cyprus, Estonia, France, Greece, Iceland, Latvia, Lichtenstein, Lithuania, Malta, the Netherlands, Romania, Slovenia, and Spain.

authorised by the Member State if the controller offers adequate safeguards to the protection of data subject's fundamental rights, in particular if resultant from contractual clauses. In this regard, the Commission has issued opinion and drafted models of clauses to be used by controllers[165]. Decisions C(2004)5271[166] and 2001/497/EC[167] bring models of standard contractual clauses that if incorporated into a contract will allow data to flow outside the EU. Any exercise of Article 26(2) must be reported to the European Commission, as well as to other Member States.

Furthermore, partners shall bear in mind that all exceptions to Article 25 must be interpreted narrowly and their application will ultimately depend on implementation via national law. Therefore, the grounds for transborder data flow exceptions must be analysed at national level and with regards to the national data protection framework.

Finally, in the case bilateral agreements are difficult to achieve or whether the assessment of the adequate level of protection may not be feasible for other circumstances, a solution can be that the CCH, based in the EU, receives information free from European personal data or refrains from sharing what would classify as European personal data. In other words, the CCH would be free to share and receive data that does not fall within the scope of the Member States national legislator. Nevertheless, the applicability of such alternative may be very limited.

[165] http://ec.europa.eu/justice/data-protection/document/international-transfers/transfer/index_en.htm
[166] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:385:0074:0084:en:PDF
[167] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:181:0019:0031:en:PDF

3. COOPERATION WITH LAW ENFORCEMENT AUTHORITIES

To build a complete front against botnets, prosecution must follow detection and mitigation. The importance of having law enforcement engaged in ACDC is paramount and will play an important role in the sustainability of the project. Ensuring cybercriminals are prevented from regaining access to information systems is a task that can only be performed by legitimate government authorities. Otherwise, all mitigation efforts will be of limited effect as perpetrators can regain control and rebuilt malicious tools in a short period of time. To this end, frequent asked questions and other relevant issues are clarified below.

3.1 Compulsory network monitoring

In light of Article 15(1) of Directive 2000/31 on Electronic Commerce (herein the e-Commerce Directive), no systematic obligation of surveillance and collaboration can be imposed on ISPs to monitor the entire traffic undergoing their network. In fact, such duty would constitute an infringement to the freedom of information as well as to the confidentiality of correspondence, in the opinion of the Article 29 Working Party. In the terms of Article 1 of Directive 2006/24/EC (herein the Data Retention Directive), ISPs are requested to store certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law. The Data Retention Directive, while asking ISPs to store certain types of data from 6 months to 2 years pursuant to Member State implementation (Article 6), does not go further to contradict the prohibition of Article 15(1) of e-Commerce Directive. All and all, ISPs cannot be obliged to monitor and permanently inspect communications passing via their services.

Following the judgment of the ECJ in Linqdvist , the activities mentioned by way of example in the first indent of Article 3(2) of Directive 95/46, namely processing operations concerning public security, defence, State security and activities in areas of criminal law, are in any event activities of the State or of State authorities and unrelated to the fields of activity of individuals. While it can be argued that ISPs play an important role in ensuring network security, the processing of operations related to public security are not to be asked from them only and rely ultimately on public authorities.

The imposition of an obligation on ISPs to monitor illicit activities online has been refuted by the ECJ in the Scarlet and Netlog cases. The jurisprudence of the Court is undisputed as such duty would significantly impair the legitimate interests of ISPs and could amount to a considerable cost to providers. Moreover, by indiscriminately and preventively monitoring users, such mechanisms would significantly interfere with users' right to data protection and, finally, with the right of freedom of expression, whenever the monitoring would also be accompanied by filtering of allegedly malicious communications.

Nevertheless, ISPs are allowed to deploy monitoring mechanisms to detect and inspect suspicious traffic. In the context of ACDC and in light of the above, the contribution and participation of ISPs can only exist in a voluntary basis. To strike a fair balance between the monitoring measures and the rights of users, the monitoring must be legitimised and aligned with the Data Protection and the e-Privacy

Directive, under the grounds previously clarified. Participation in the project would not involve further costs to ISPs nor impair their business model, but, on the contrary, support them on providing a reliable and trustworthy service. Finally, ACDC must ensure mitigation tools have been perfected and before put in place and keep on being updated. This is because the filtering or reporting of a legitimate communication as malicious would violate users' rights, particularly the right to freedom of expression. Therefore, the group tools must demonstrate the highest level of trustworthiness and deploy the most developed state of art so as to prevent any incidents and misjudgements.

3.2 Botnet takedowns and takeovers

It may be possible for ISPs to promote a botnet takedown in the grounds of self-defence, but such actions should always result from cooperative works between private sector and national authorities. Common rules of self-defence require the defender to respond to an unlawful act immediately and proportionally to the danger with the purpose of protecting another legal right, which is endangered. The means used by the defender must be appropriate, adequate, and non-excessive, as the damage caused by self-defence cannot overweight the menace of the threat. The use of self-defence is thus limited to the reasonably necessary to counter or prevent the unlawful act to take place or to produce effects. Because it is difficult for an agent to decide whether their takedown classifies as self-defence, it is not prudent to conduct a takedown without prior involvement of the authorities. Therefore, it is always appropriate to contact law enforcement before such drastic measures are undertaken, especially because excessive use of self-defence is an unlawful action and may result in more harm than the initial threat. Pro-active efforts to takedown botnets can escalate and have indiscriminate or unforeseen proportions, the reasons why law enforcement should be always be notified in advance.

A botnet takeover involves large complications. The use of the botnet infrastructure even if by an agent aiming to shut down the net may have serious legal implications. For this reason, takeovers shall not be carried out by affected parties. Apart from incurring in hacking offences (unlawful access to a computer system, unlawful access to computer data, etc.), the takeover can harm the confidentiality of the communications of user-bots. For its complexity, botnet takeovers are better conducted when ordered by competent judicial authorities or operated by national CERTs with the particular mandate to do so. This is because the takeover may imply interference in the communication of third parties which do not belong to the universe of the ISP customers. In this case, the actions undertaken by the ISP are not likely to do not be excused by contractual terms or self-defence.

3.3 Duty to report incidents to the authorities

ISPs are under the compulsory duty to report every personal data breach to national authorities, as required by Article 4(3) of e-Privacy Directive. A compulsory duty to report on every illegitimate activity involving their network is a broader requirement which would inevitably oblige ISPs to permanently monitor the data traffic undergoing their services. This would contradict Article 15(1) of e-Commerce Directive, which expressly forbids Member States from imposing a general obligation to monitor the information ISPs transmit or store, as much as from imposing a general obligation for ISPs to actively seek facts or circumstances indicating illegal activity. However, this does not preclude the general duty of informing public authorities of illegitimate activities that they may come across when performing the service. Indeed, most national legislators require that whenever ISPs are aware or suspect of illegal activities involving their customers (whether as victims or authors of such), this must be reported to public authorities.

While ISPs are not obliged to permanently inspect network traffic for malicious activities, they are not forbidden to do so if such processing is aligned with the provisions of the Data Protection Directive and the e-Privacy Directive. ISPs can thus collaborate to detect and inspect malicious activities on a voluntary basis.

However, most service providers are hesitant in placing mechanisms for detection and inspection of malicious activities as they are afraid public authorities would expect them to act as 'Internet police'. This would overwhelm their activities with excessive requests, besides increasing their liability and legal duties in relation to the information they transmit or store. This situation corroborates for creating an uncooperative scenario, where ISPs willing to combat cybercrime are fearful to join forces with governments, apprehensive this would result in increased regulation and additional duties.

Finally, the ACDC project must ensure there is a safe harbour to protect collaborative ISPs preventing that the implementation of anti-botnet tools by those leads to their depiction as sources/distributers of malicious activities/content. A safe harbour within ACDC would thus create a safe and trusted environment for collaborative partners and contributors.

3.4 Duty to notify infected customers about compromised data

Under Article 4(3) of e-Privacy Directive, service providers are requested to communicate end users the event of personal data breaches which are likely to adversely affect its personal data or privacy. In these cases, the provider shall notify the subscriber or individual of the breach without undue delay, without prejudice of the regular notification of the incident to the competent national authority. If a customer has been identified as the vector or victim of a botnet, which is likely to compromise the security of the network, the service provider is allowed to notify the customer of its malicious activity/infection. This notice may be followed by solutions that would assist the hygiene of the victimized end-customer. Therefore, ISPs are allowed to redirect users to the National Support Centre of the country where users are located.

3.5 Use of ACDC data by public authorities

With regards to the scope of the Data Protection Directive, Article 3(2) explicitly informs that data processing carried out as part of activities falling beyond EU law (processing operations concerning public security, defence, national security, and activities in the area of Criminal Law) are out of the Directive 95/46 application. The same is valid for the e-Privacy Directive, as established by its Article 1(3). Articles 13(1) of Data Protection Directive and 15(1) of e-Privacy Directive reinforce the rule that privacy restrictions can be imposed to data subjects when provided by Member States' legislation and for the purposes of public security, national security, defence, and criminal prosecution, investigation and prevention.

Therefore, national authorities may be able to process personal data without the restrictions imposed by the above mentioned directives when this activity is beyond the scope of EU law, as defined by article 3(2) of Data Protection Directive. This is valid for law enforcement agencies acting for the purpose of public security and prosecution, investigation, and prevention of crime. It does not mean data protection standards are simply waived for law enforcement authorities activities: it indicates that this is a matter for national legislators to regulate. This being said, the extent of activities and restrictions to data protection in the context of public authorities activities will depend on the mandate given by them by national laws and must be analysed case-by-case.

4. GROUP TOOLS ANALYSIS

4.1 The Centralised Data Clearing House

The Centralised Data Clearing House or CCH is the main element of the ACDC project. Via this platform, data collected through the detection tools will be aggregated and further analysed with the purpose of generating data feeds to interested controllers. This single EU common report will facilitate information exchange across the Union and enabling appropriate response against malware. The CCH is thus a gathering platform which combines data collected by other group tools directly placed in public networks and personal devices to be further analysed. The findings of the CCH are thus shared with trusted partners that have previously requested to receive the news feed. To subscribe to the news feed, one must register via the community platform, which will grant access by API keys. However, access to the CCH news feed is limited in light of the specific and legitimate interest a party may hold. The relation between requests and nature of access will be measure and granted by the community platform based in the relationship and level of trust of a given party.

Before sharing any slots of data with the platform, countries are expressly requested to pay due attention to their national laws. This is to say that partners, as controllers of the processing that goes on in the network traffic sensors and malware website analysis tools, hold full responsibility with complying with national legislation before engaging in information sharing. Such duty must be borne by partners contributing with input data due to the impossibility of having the CCH verifying such compliance.

The CCH operates as a controller regarding the information received in the platform and bears responsibility for the processing thereof. The agent managing the CCH *in casu* ECO (Association of the German Internet Industry) is the controller of the platform. This control covers a three stage processing, which includes access to the data shared by data collectors (such as ISPs, end-users, computer security companies, banks, etc.), further processing relating to the analysis and aggregation of the data received, and a final processing concerning the distribution of this data with trusted parties according to the rules of the community platform. Once again, it is important to recall that the automation of the tools deployed in the CCH minimise human intervention to the maximum and information distribution in a need-to-know basis assures that only data pertaining to the network and interest of a partner is shared with such. This is also to say that only parties holding legitimate interest over personal data will receive redistribution of this data. It also means that not every partner receiving feeds from the CCH will have access to users' personal data, for the reasons explained above.

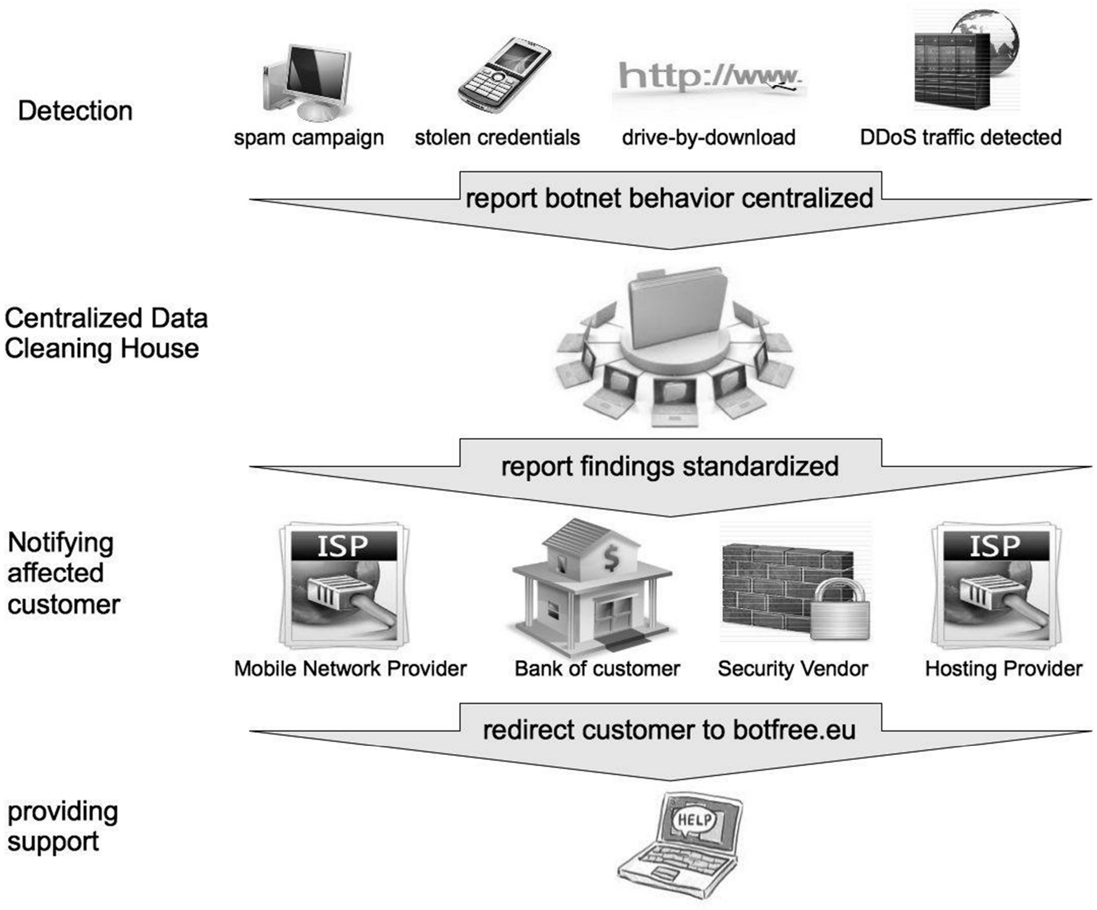


Figure 2: ACDC Proposal, part B, p. 27.

The architecture of the Centralised Clearing Data House envisions the receipt of data collected through other ACDC tools, including personal data and arguable personal data. As examined above, actors operating networks traffic sensors and website malware analysis tools can only deploy these mechanisms as far as this is necessary to protect the security of their own network or their own customers. But while it can be claimed that the CCH has the potential to deliver increased security and help developing better tools, no direct link can be established between the data sharing that takes place between tools placed at national level and the arrival of this information at the pan-European platform. This is to say that any personal data sharing between network traffic sensors and the CCH will fall short in fitting into the same legal justification/purpose that allowed the collection of the data in first place. This is because sharing the data collected by other ACDC group tools with the CCH classifies as a different processing, which requires controllers to define a new purpose and a new legitimate ground.

The legal issue faced at the CCH would be equally raised in the case outputs of a group tool would be forward to another group tool operated by different actors, whether or not this would be later transmitted to the CCH. While ISPs, webmasters and CERTs are allowed to deploy mechanisms such as network monitoring sensors and website analysis, sharing personal data with an authorised third party would amount to violation of data protection.

The legal obstacles related to sharing of personal data collected by a given group tool, be it with the CCH or with another group tool, can be overcome by allowing end-users to consent with such processing. This would necessarily be integrated to the terms of service of ISPs and webmasters in observations with the rules for obtaining consent as set forth in the data protection directives. Nevertheless, it is clear that end-users would be given the freedom whether to agree with the second-tier processing and could not be penalised for not consenting. Clearly, this creates a complication for ACDC stakeholders, as cybercriminals would undoubtedly resist to sharing such data.

While the operations carried out inside the CCH system do not necessarily conflict with the data protection standards examined in this analysis, the operations that would feed the clearing house are likely to do not fully abide to these same rules. Therefore, a **strict interpretation** of the law would consider that the most tangible solution is for the CCH to receive, store and share **non-personal data** and statistics of infections that could, nevertheless, help private actors and public authorities fight botnets. This could be achieved by omitting the source and destination of the infection, but could include limited information on place of origin and destination of the attacks (e.g. city or country), as much as details over the nature of the infection. This way partners could prepare to prevent, detect, report, and recover from similar malware. As a result, public authorities would have sufficient information to make additional requests to involved ISPs and therefore advance any necessary investigations at national level.

The EDPS Peter Hustinx clearly opposes the creation of new EU information exchange instruments, as a multiplicity of systems for the cross-border exchange of information would carry additional risks in terms of personal data protection and invasion of privacy[168]. The ACDC project will thus need to convince data protection authorities that the benefits of the CCH outweigh the impact on the fundamental rights of individuals. Network and data security are in the interest of users and of society. But limitations on the fundamental rights will not seem justified if one balances the gravity of the interference, i.e. the scale of the privacy intrusion of the mitigation tools, with the expected benefits, deterring botnets within the EU. That includes proving the absence of less intrusive means and other existing means that would allow the same results to be achieved.

However, a **more flexible** approach, coherent with the status and impact of cybercrime in the information society, should recognise the relevance of the CCH and deem its operation **legitimate under Article 7(f) of Directive 95/46/EC**. With regards to the Centralised Clearing Data, if IP addresses and domain names qualify as personal data, the data processing may be based on Article 7(f), which allows the processing carried out in legitimate interest of the controller or of third parties when such processing does not override the fundamental rights of data subjects. This article implies a proportionality assessment, i.e. to weigh the legitimate interest (ensuring security of the network; security and confidentiality of communications) of the third party to whom the data is disclosed (ISPs, webmasters, hosts, security companies, CERTs) against the need to protect data subjects'

[168] Opinion of 23 June 2008 on the proposal for a decision establishing a multiannual Community Programme on protecting children using the Internet and other communication technologies, at https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2013/13-04-29_EIXM_EN.pdf

fundamental rights (confidentiality of communications). While the need to ensure the network is protected against botnet is clearly legitimate, the proportionality assessment will bear upon the adequacy and necessity of the means used to achieve this goal, thus on the design of the CCH solution. In this case, two data processing operations should be legitimize: the sharing of IP addresses with the CCH and its further processing for the fight against botnets. This processing will be performed by the CCH on behalf of ISPs, webmasters, hosts, and other agents holding a legitimate interest in the protection of the security of the network, including end users.

Article 7(f) expressly request a **proportionality test** to verify the balance between the interests pursued by the controller or by the third party to whom the data is disclosed and the burden imposed to data subjects. The proportionality test calls for a three step test consisting on the assessment of necessity, adequacy and proportionality stricto sensu. Finally, one must also clarify how will the processing inflict the fundamental rights of data subjects and present a concrete explanation of how can these rights be impaired. According to the Article 29 Working Party, "*this balance of interest test should take into account issues of proportionality, the relevance of the personal data to the litigation and the consequences for the data subject. Adequate safeguards would also have to be put in place and in particular, there must be recognition for the rights of the data subject to object under Article 14 of the Directive where the processing is based on Article 7(f) and, in the absence of national legislation providing otherwise, there are compelling legitimate grounds relating to the data subject's particular situation.*[169]" The following paragraphs are dedicated to explore why the CCH fulfils this test.

The **necessity** of the creation of a platform such as the CCH to efficiently fight botnets is justified by the international character of cybercrime and the significant threat posed by botnets. Large scale infections cannot be tackled by providers, webmasters, hosting services, and computer security companies individually. The need for cooperation and information sharing is thus crucial. The automated and non-human operated character of the CCH reduces chances of unauthorized or abusive intervention. Securing networks without cooperation and information sharing is unfeasible,

With regard to the **adequacy** of the means used, the CCH environment consists of data processing that have a strong and concrete potential to reduce botnets across the EU. The CCH is likely to be regarded as a suitable and adequate environment to the objectives pursued: the tools deployed at the clearing house are tested and efficient mechanisms capable of promoting knowledge and sharing data of infections. This will facilitate disinfection, as the news feed provided by the CCH will enable partners to alert their infected users and redirect them to the National Support Centre for cleansing.

A look into the **proportionality stricto sensu** afforded by the system reveals that the goal of the CCH is thus protecting end users and networks from botnets, promoting prevention, detection and disinfection. This goal is made possible by ensuring that third parties which hold a legitimate interest in protecting their networks have access to this information. The information processed at the CCH is not intended to be used against individuals, left alone the possibility of ISPs, webmasters and web hosts to take the necessary legal measure to safeguard their networks against malicious users. In balance

[169] Article 29 Working Party, Working Document 1/2009 on pre-trial discovery for cross border civil litigation, February 11, 2009, p. 10.

the interests at stake, one must see a first conflict between the need to ensure network security and users' right to data protection and privacy. However, it must be recalled that in the context of widespread cybercrime users cannot fully enjoy protection of data without effective cybersecurity. Therefore, the need for security and the exercise of fundamental right to data protection are complementary. Guaranteeing the co-existence of both is the way to promote a safe online environment where data protection remains a valid and alive. Ensuring there is adequate balance when one overrides the other is the challenge but also the way to go.

The overall architecture of the CCH minimizes data protection issues in several aspects and operations. First, access to the platform is managed by a third party (community platform) and data sources are graded depending on their level of thrust. Moreover, data feeds are provided on-demand and limited in light of national laws and special interests of stakeholders. To the extent that the CCH receives and releases non-personal data, no legal obstacles can be raised. The community platform rules, together with the numb and automated character of the CCH, are mechanisms designed to ensure the minimal possible impact on the fundamental rights of data subjects. Removing the processing of personal data from this context (e.g. IP addresses, domain names, email addresses) would diminish the capability of the CCH to a level where the purpose is no longer attainable. Input and output data are controlled and ranked by the community platform, which also enables sharing preferences and restricts access to data according to partners legitimate interests. Therefore, ISPs receiving data feeds from the CCH can only have access to information related to their own range of IP addresses, never to data relating to users that are not related to their services. This guarantees sufficient levels of confidentiality of communications and lesser invasive means on user data.

To a more concrete level, it is possible to argue that data subjects whose data are being processed by the CCH do not hold a legitimate interest in preventing the processing. The first crucial element is to understand that all data reaching the CCH level relates to only two possible scenarios: 1. The data relates to a user who has been identified as a victim of an infection; 2. The data refers to a user who has been identified as a perpetrator. In case 1, a user who is a victim of a botnet wants to be notified of these circumstances which are threatening to him. In case 2, a user who has been identified as an author of a cybercrime does not hold a legitimate interest to do not be identified as such.

Finally, when it comes to assessing the legitimacy of the CCH as such, it is important to dissociate the activities that are under the umbrella of the platform itself and the ones that pertain other stages and partners of ACDC. A look into the architecture of ACDC reveals that the news feeds issued by the CCH provide only an authoritative opinion on the characterization of a user as a victim or perpetrator. ISPs and other partners holding such information hold full discretion to what measures will follow after the reception of this data. The ACDC environment recommends the issue of information notices informing the user about the nature of the malware and how to receive help for disinfection, held at the National Support Centre. All and all, the sending of the information notice is too under the discretion of the partner receiving the CCH news feeds. This partner is in the position to assess the relevance of the information received and decide on the measures to address the problem.

This brings us to the possible argument that the CCH processing undermines data subjects rights in case of a false positive, e.g. when a user is equivocally identified as a malicious or compromised user. While the tools deployed in ACDC gather the state-of-art of anti-botnet solutions and will be run in labs, prototypes and experiments to verify their accuracy and efficiency, the issue of false positives cannot be ruled out. The ACDC tools will be constantly updated and new solutions will be integrated to the project if proven more reliable than the deployed mechanisms. However, up to this moment, ACDC does ensure the state-of-art in terms of technical solutions against botnets. Even then, a user victim of a false positive will have significant means to overcome any access restriction that will be informed to him in the form of a infection notice. This is because before sending an infection notice to a user, ISPs are required to, in accordance with their national law, decide upon the remedies, sanctions and means to be given to users to enable their adequate defence. It is thus a duty of data controllers to ensure that data subjects' rights are fully respected and that the necessary remedies and opportunities for their exercise are put in place.

To conclude, the controls put in place by the CCH ensure the deployment of minimum invasive measures and the maximum balance of interests which can be expected in the context of the fight against cybercrime and from the means to achieve and maintain network security. The broader picture reveals that the interaction between the CCH and other group tools can ensure respect to data protection at different levels. Therefore, the data processing activities performed by CCH, as currently devised, are likely to be found proportionate by the competent authorities. To this end, we are investigating other anti-botnet initiatives present a list of case studies of similar tools being deployed around the world to inspire European legislators. This analysis will be presented in our next deliverable together with recommendations.

4.2 Network Traffic Sensors and Malicious and Vulnerable Website Analysis tools

As noted in D 1.5, Network Traffic Sensors are tools responsible for collecting and providing data on infected systems (bots) to the ACDC. They are one of the (primary) sources of data to the Centralized Clearing House, sharing information related to compromised systems on the Internet that are used for malicious purposes. The sensors continually monitor and analyse the data flowing on the target infrastructure of the members that choose to participate in ACDC with detection tools, in order to examine and detect any signs of infection or bot related activity to be reported to the CCH.

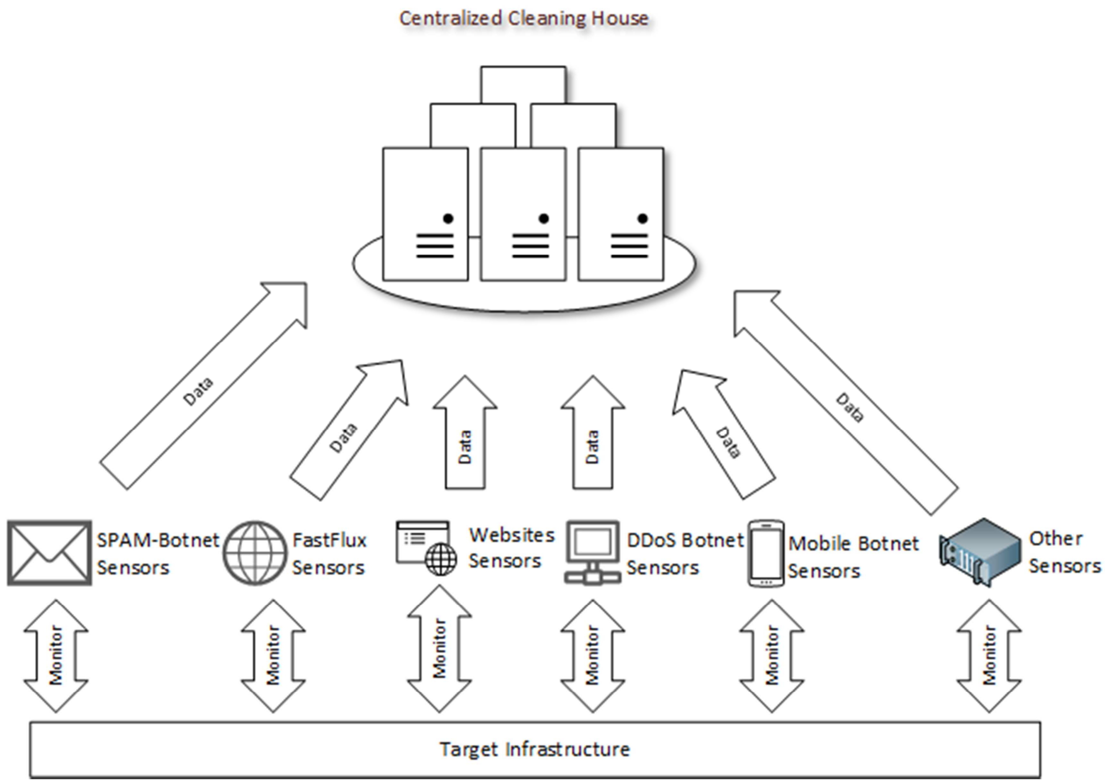


Figure 1 ACDC Network Sensors - General Architecture. Source: Deliverable 1.5 Network Traffic Sensors, p. 2.

The malware website group tools will be deployed by webmasters and hosts to scan websites searching for malicious content. These tools will help operators identifying and mitigating malware activity hosted in their servers. The architecture and the type of data processed in these operations brings legal aspects that are similar to the ones applicable to the network traffic sensors. Both group tools envision real time monitoring of internet activity and can be justified on similar legal grounds, as presented below.

The categories of data processed by sensors and website analysis tools will vary according to the source and to the solution carried by the technology put in place. This will include and is not limited to the processing of network traffic information, DNS queries, email addresses, IP addresses, and darknet traffic. Because the processing of this range of data may qualify as a processing of personal data in the terms of the Data Protection Directive, partners operating network traffic sensors and website analysis tools are required to observe the principles of legality, legitimacy and proportionality set forth by the European Directive and implemented in the form of national data protection laws. Finally, partners controlling the operation of these tools, as long as not in behalf of another partner (therefore working as a processor) shall bear the liabilities associated with the controller duties, as set forth by the Data Protection Directive. The distinction between controllers and processors is one difficult to draw before the multiplicity of partners involved in ACDC. Here, three cases are possible:

Case 1. Partners providing technology only. This type of partner does not engage in the data processing, nor overviews or influences the operations of the solution. This is the case of a partner providing only intelligence. In this case, the controller will be a second actor which will deploy the solution on his domain and overview the operation of the technology.

Case 2. Partners providing and managing technology solutions. This is the case for most partners involved in the network traffic sensors and vulnerable and malicious website analysis tools. In this case, partners are providing intelligence through a solution but remain in control of the operation of the solution, meaning the solution is not operated on behalf of a second agent. In this case, partners are considered controllers of the entire processing undergoing the tool and how the tool communicates with the CCH.

Case 3. Partners providing technology to and managing technology on behalf of a second agent. In this case, partners are responsible for the intelligence of the solution but hand in the operation of the solution to a second agent (e.g. ISP). If the partner enters an agreement with this agent whereby the partner will be deploying the tool in the network of the second agent and sharing the information processed by the solution with the agent, partner and second agent will operate joint control over the processing.

While the use of network traffic sensors and malware website analysis tools have the purpose of protecting network integrity and continuity of service, partners are still asked to comply with the data quality principles and deploy mechanisms to ensure respect to the proportionality of interests between controllers and data subjects. The discussion over the nature of IP address as personal data is one that significantly interests the operators of these tools. While monitoring online traffic through sensors and website detection tools essentially comprises processing of IP addresses, it will not restricted to this information. In fact, most solutions aim to process raw attack data, email addresses, domain names, among others. Moreover, tools that monitor online traffic indiscriminately may increase data protection risks to data subjects. Finally, the purpose of ensuring network security must fulfil one of the legitimate grounds described above under Article 7 of Data Protection Directive, that ensures the legitimacy of the purpose and means of processing. In this particular context, Article 7(b) and (c) have been identified as concrete legal basis for the processing conducted by both sensors and malware detection tools.

Article 7(b) may justify the deployment of networks sensors as well as the processing carried out by website malware analysis tools, in the circumstances described by the Article 29 Working Party in its Opinion 2/2006. In the view of the Article 29 Working Party, the setting up filtering systems by data controllers may be considered a step towards ensuring the performance and continuity of the service contracted by the customer with a reasonable level of security and confidentiality, characterizing thus a legitimate processing of the personal data involved in the operations. The Article 29 Working Party clarifies that a data controller using Article 7(b) as a legal ground in the context of the conclusion of a contract cannot extend it to justify the processing of data going beyond what is necessary[170]. In the words of the Article 29 Working Party, "the necessity test requires a close and substantial connection between the data subject and the purposes of the contract"[171]. They call for a strict interpretation on

[170] Article 29 Working Party, Opinion 15/2011 on the definition of consent, July 13, 2011, p. 8.
[171] Article 29 Working Party, Working document on a common interpretation of Article 26(1) of Directive

the use of this exception, which can only be used if truly necessary to the purpose of the performance of this contract or of these pre-contractual measures[172].

Furthermore, Article 7(c) can also be used to legitimise the operations of these two group tools. The legal obligation enshrined under Art. 4 Directive 2002/58/EC and Article 17(1) Directive 95/46/EC for data controllers to provide security of their networks is in fact the most central element to justify the processing of personal data under ACDC for network sensors and malware website analysis. Therefore, it is paramount to define to what extent ISPs, webmasters and hosts can make use of the above provisions under national law, namely whether the collection and analysis of customer data flows and later sharing of IP addresses and other personal data with the ACDC platform for the purpose of fighting botnets would be allowed as a measure taken to comply with the legal obligation to provide for security of their services.

Several mechanisms are already being deployed by ISPs and webmasters to minimize malicious user activity. Malware mitigating solutions are thus essential tools in the protection of network security. To the that extent such mechanisms are used with the only purpose of safeguarding security of the network and in compliance with the data protection standards, the processing is likely to take place without further complications. One important aspect of the legal requirements is to ensure data subjects' information rights are being respected. This includes informing users in the terms of agreement of the service about the existence of sensors and the purpose of their placement.

4.3 National Support Centre

Support centres will be established in partner countries as the first point of contact for infected users and the main resource of information and knowledge for prevention, immunization, and awareness regarding infections. The support centres represent the initiative to the broad public by interacting directly with end-users. ISPs will be informed if their user is infected by botnet via the newsfeeds distributed by the CCH as well as via the traffic sensors placed in their networks. After a user has been identified as a victim of a botnet infection, the ISP will redirect the user to the National Support Centre for disinfection.

The processing that results in the detection of an end-customer as a victim of cybercrime belongs to the architecture of the respective tools that lead to detection (networks traffic sensors, malware website analysis tools and end-customer plugins). Therefore, the processing conducted by the National Support Centres comprises the treatment given and communication established with the victim that arrives in the platform after being forwarded by a provider. This is the processing under examination here.

The operation of the support centre was provided by ECO in the Deliverable 1.3.1 and goes as follows:

95/46/EC of 24 October 1995, November 25, 2005, p. 13.

[172] Article 29 Working Party, Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995, November 25, 2005, p. 13.

1. Providers operate networks traffic sensors that enable detection of infected users in almost real time. Only providers can identify their customers from the IP-address at that particular point in time.

2. Providers inform the particular customers about the detection according to the process determined by the providers themselves. In the first phase, customers are informed that they have been infected with malicious software (bot). Customers are then referred to the central help website (National Support Centre) where disinfection instructions are available.

3. If the customer does not succeed to disinfect his/her device via the instructions received at support centre, he/she can contact his/her provider for further assistance. The provider can then decide if the customer needs to be referred to the support centre call centre for further help with removing the malware. In this case, the provider gives the customer a pseudonym created trouble ticket number that contains coded information about the infection.

4. Users arrive at the call centre with a ticket number that will allow him/her to get tailored help. Should this first phase also fail to lead to the desired disinfection, the caller is forwarded to a specialist, going from a Level 1 to a Level 2 support, with further recommendations on how to proceed.

The information exchange established between the infected user and the national support centre is made possible via the ticket system. Once a customer infection is detected, this circumstance will be informed by the ISP the support centre detected. This step generated an individual ticket containing a timestamp of the incident, name of the suspected malware and a voucher/ticket number for the customer. The ticket has been specifically designed to enable disinfection via national support centres while preserving user’s secrecy. In the case disinfection is not achieved via the solutions presented in the website and the victim decides for phone support, the ticket system remains privacy protective. Help desk staff do not hold access to the device of the caller nor need personal information to provide assistance. Phone support is thus a trusted system based only on the characteristics of the infection registered and detected by the ISP. The national support centre does not store, trace or receive any personal data from an infected user or from his/her computer, whose identity is kept anonymised.

In light of the above, the processing conducted in the frame of the national support centres is not one that qualifies as a processing of personal data in the terms of the Data Protection Directive. Finally, even if one considers that the National Support Centre could be responsible for the data processing that undergoes the solutions that are made available for download in the website, a deeper consideration of the matter reveals that the National Support Centre is a completely external actor with no power, influence or overview on the information processed by these solutions. Therefore, the operations of national support centre are out of the scope of the data protection legislation.

4.4 End Customer Tools

The End customer tools aims at enabling users to generate threat reports about suspicious content and infections. Botnets can manifest through spam, phishing and malicious websites. With the help of end customer tools, each time a user comes across one of these threats, he/she will be able to report the suspicious content, allowing ACDC to collect botnet related intelligence. To this end, four sets of tools have been developed: 1. Web browser plugins; 2. Email client plugins; 3. Mobile devices reporting tools; 4. Third parties data sharing tools. The four sets of tools will collect infection data to identify compromised devices and gather intelligence about malware. Partners responsible for controlling the operation of such tools are regarded as data controllers in regard with the processing undertaken by such technologies.

Because the reports include personal data or arguable personal data about users, such as IP addresses and URLs, the processing falls into the scope of the Data Protection Directive. Therefore, partners operating end customer tools must ensure respect to all the requirements set forth by the directive and their national data protection laws. Regarding legitimation grounds, the software plugins will operate by user consent, in the terms of Article 7(a), Directive 95/46/EC, which will be collected prior to the plugin download. Partners must thus include all relevant information such as the purpose of sharing intelligence data with the Centralised Clearing Data House under the terms of use of the tool, and abide to all the requirements related to obtaining unambiguous user consent and respect to data subject rights, as described in the previous sections.

5. NATIONAL LEGAL ANALYSIS

The task description of the ACDC legal requirements included a national comparative study of the obstacles to be faced for the implementation of ACDC at national level. Selected countries included Belgium, Croatia, France, Germany, Italy, Portugal, Slovenia, Spain and The Netherlands. To this end we have contacted the responsible partners, as described in the project proposal and as agreed in the WP1 phone conferences, namely KU Leuven, CERT-RO, SignalSpam, ECO, TelecomItalia, FCCN, Xlab, Inteco and TU Delft. A legal comparative questionnaire was drafted and shared with partners during M6 to M9 and the answers were compiled as inputs to the backing of this analysis. Partners have answered to legal and legal-related questions regarding data protection and anti-cybercrime legislation and practice in the country.

The first issue to consider at this point is that the inputs received from partners presented an uneven level of information. This has impacted the study to the extent that only a partial volume of the data received was considered appropriate for the purpose of the analysis. Therefore, the most reasonable options was to narrow down the main legal issues presented by ACDC and focus the comparison in the possible interpretation of these issues before the national framework of the selected countries. Given that a detailed national analysis would have only been possible with the effective contribution of national legal experts, this study cannot deliver an in-depth examination and is subject to the interpretation of the law by the national protection authorities. Nevertheless, it does cover the major impediments verified among the selected Member States based on the text of the law and on the legal instruments reported by countries in their answers to the legal questionnaire (annexed to this document) and as derived from our expertise in the field. B-CCENTRE/KU Leuven has been working on solutions for this issue, what have included reaching out to national DPAs to conduct a pre-assessment of their opinions on ACDC and a cooperative relation with ENISA and their local contact points.

This national analysis addresses the following legal issues before the laws of Belgium, Croatia, France, Germany, Italy, Portugal, Slovenia, Spain and the Netherlands:

- 1. Classification of IP address as personal data before data protection law and the opinions issues by national Data Protection Authorities
- 2. Implementation of Article 7 of Directive 95/46/EC, with especial attention to paragraphs (a), (b), (c) and (f), including the interpretation of balance of interests between data controllers and data subjects;

1. Classification of IP address as personal data

This will clarify in which circumstances IP addresses, whether dynamic or static, will be considered as personal data by national law. This is particularly important as IP addresses lay in the centre of the data flows operated by ACDC and the debate of their classification can influence the assessment of other types of data, such as domain names, as personal data. If regarded as such, either by case law or in the DPA’s opinion, the majority of the ACDC processing will fall within the scope of the Data

Protection Directive. This implies a higher threshold for the processing and further consequences in terms of demonstrating compliance with data quality standards and legitimation grounds.

2. Implementation of Article 7 of Directive 95/46/EC, with especial attention to paragraphs (a), (b), (c) and (f), including the interpretation of balance of interests between data controllers and data subjects;

Due to the variety of tools and technologies covered by the ACDC environment, different legitimate grounds may apply. So far, Article 7(a), (b), (c), and (f) are believed to be applicable in different contexts of ACDC. The application of Article 7(a), unambiguous consent, is quite straightforward to legitimise the plugins envisioned by the End customer tools and is likely to have a harmonised use through the Union. As discussed above, Article 7(b) and 7(c) can be used as the basis for legitimising two group tools, the network traffic sensors and the vulnerable and malicious website analysis. Finally, article 7(f) is particularly important for being the most likely provision to be used to legitimise the further analysis and sharing of personal data by the CCH. The use of Article 7(f), however, is one of exceptional nature which implies a proportionality assessment, i.e. to weigh the legitimate interest (ensuring security of the network) of ISPs, webmasters, hosts, security companies, CERTs) against the need to protect data subjects' fundamental rights (confidentiality of communications). It is thus crucial to examine the implementation of Article 7 (a), (b), (c) and (f) by national legislators and the interpretation of the DPAs on the use of such provision.

	IP address: Classifying IP address as personal data	Article 7(a): Use of Article 7(a) to legitimate end-customer tools	Article 7(b): Use of Article 7(b) to legitimate sensors and website analysis tools	Article 7(c): Use of Article 7(c) to legitimate sensors and website analysis tools	Article 7(f): Use of Article 7(f) to legitimate the operation of the CCH
Belgium	Yes, see Opinion n° 34/2000 on the protection of privacy in the context of ecommerce and Opinion n° 44/2001 on copyright infringement investigations	Article 5(a), Data Protection Law	Article 5(b), Data Protection Law	Article 16§4, Data Protection Law and Articles 114, Law on electronic communications, combined with Article 5(c), Data Protection Law,	Article 5(f), Data Protection
France	Yes, see the CNIL statement on "IP-addresses are personal data for all European CNILs", and the Supreme Court ruling in Case nr. 07-80267,	Article 7, caput, Privacy Act	Article 7(4), Privacy Act	Article 34, Privacy Act, Article D98-5(III), Post and Electronic Communications Code, combined with Article 7(1), Privacy Act	Article 7(5), Privacy Act

Germany	Yes, see the Federal Commissioner for Data Protection and Freedom of Information Activity Report for 2007-2008 and the Decision by the supreme data protection authorities for the non-public sector on 26/27 November 2009.	Section 4(1), Federal Data Protection Act	Section 28(1)(1), Federal Data Protection Act	Section 9 and Annex, Federal Data Protection Act and Section 109(1) and (2), Telecommunications Act (TKG), combined with Section 28(1)(1), Federal Data Protection Act	Section 28(2)(2), Federal Data Protection Act
Italy	Yes, see Italian Privacy Authority decision 1482111 of 17/1/2008 (amended by decision 1538224 of 24/7/2008)	Article 23, Data Protection Code	Article 24(b), Data Protection Code	Articles 31 and Articles 32, 33, 34 of Data Protection Code, combined with Article 24(a), Data Protection Code	Article 24(g), Data Protection Code
Portugal	Yes, following the opinion of the Article 29 Working Party	Article 6, caput, Data Protection Law	Article 6(a), Data Protection Law	Article 14, Data Protection Law and Article 3, Law 41/2004, combined with Article 6(b), Data Protection Law	Article 6(e), Data Protection Law
Romania	Yes, following the opinion of the Article 29 Working Party	Article 5(1), Data Protection Law	Article 5(2)(a), Data Protection Law	Article 20, Data Protection Law and Article 3, e-Privacy Law, combined with Article 5(2)(c), Data Protection Law	Article 5(2)(e), Data Protection Law
Slovenia	Yes, see Opinions 0712-2/2010/1484, 0712-423/2006/2 and 0712-8/2007/2 of the Data Protection Authority	Article 10(1), Personal Data Protection Act	Article 10(2), Personal Data Protection Act	Article 24 and 25, Personal Data Protection Act, and Article 101, Electronic Communications Act, but no legitimate ground	Article 10(3), Personal Data Protection Act
Spain	Yes, see Report of the Spanish Data Protection Agency No. 327/2003	Article 6(1), Data Protection Law	Article 6(2), Data Protection Law	Article 9, Data Protection Law and Article 36bis, General Telecommunications law, combined with	Article 6(2), Data Protection Law

				Article 10(2)(a), Royal Decree 1720/2007	
The Netherlands	Yes, see the Dutch Data Protection Commission Guidelines of December 2007, Opinion n° z2008-01174 on the collection of IP addresses and Opinion n° z2003-1660 on the collection of IP addresses by the BREIN foundation, and the ruling of the District Court of Utrecht in KG-nr: 194741/KGZA 05-462	Article 8(a), Personal Data Protection Act	Article 8(b), Personal Data Protection Act	Article 13, Personal Data Protection Act and Articles 11.3(1) and 11a.1, Telecommunications Act, combined with Article 8(c), Personal Data Protection Act, and Article 11.2a(2)(b), Telecommunications Act	Article 8(f), Personal Data Protection Act

Table 1 – Legal comparative analysis

5.1 Classification of IP addresses as personal data

As discussed, the processing of personal data is an element present in multiple operations of ACDC, at different stages. Our analysis has revealed that albeit no law currently exists regulating the issue, most national data protection authorities are of the opinion that IP addresses classify as personal data. In fact, except for Portugal and Romania, all DPAs have issued formal documents or public statements informing their position on the matter, where the classification of IP addresses inevitably fall within the category of personal. Furthermore, some of these DPAs have explicitly declared that IP addresses are personal data per se, or in other words, that IP addresses are personal data regardless of whether the processing is conducted by an ISP or in connection with an ISP or by a technical partner with no privileged information about the user behind the protocol. Although no specific public documents addressing the issue were found in Portugal and Romania, considering that all DPAs participate in decisions issues by the Article 29 Working Party and that the opinions issued by this body are applicable and authoritative in all Member States, IP addresses will also be regarded as personal data in Portugal and Romania, unless a controller is in a position to prove that he/she has no means to identify the user behind the protocol.

Therefore, the conclusion reached after the comparative legal analysis is the same found at European level. We advise partners to treat IP addresses as personal data, even if the processing does not directly involve an ISP. In fact, the classification of a controller as ISP loses it meaning in ACDC, since the end-to-end approach adopted in the project will inevitably communicate IP addresses to the interested ISPs. Control mechanisms to avoid such communications are not only not envisioned as well as undesired. The very purpose of ACDC is to aggregate and correlate data regarding infections related to multiple providers and be able to inform ISPs on the existence and characteristics of the malware installed in their IP range. To conclude, all ACDC partners are asked to process IP addresses in compliance with the standards of Directive 95/46/EC and implementing national data protection laws.

5.2 Implementation of Article 7(a) – End customer tools

In line of principle, consent is the main ground for allowing the processing of personal data. In effect, it is only with the conscious, freely given and informed permission of the data subject that a controller shall be able to process the data that relates to that person. The functioning of the ACDC End customer tools will be based in user consent and shall respect the national laws applicable to the processing of personal data. The user must be informed of all the relevant aspects of this processing, such as what type of data will be collected and for what purposes, the identity of the processor, the third parties that will have access to the data, as well as of their data subject rights and the means to exercise them. Although countries had discretion to implement this provision, no major differences were found that would impair a similar application of consent as a legitimate ground to authorise the deployment of end customer tools in the countries analyzed. Therefore, the use of consent, in the terms made explicit by the Directive and in respect with specificities created by national law, shall be sufficient and adequate to legitimise the use of end customer tools across ACDC.

5.3 Implementation of Article 7(b) – Network traffic sensors and Vulnerable and malicious website analysis tools

As discussed, Article 7(b) may be used to legitimise the operations of two group tools: 1. Networks traffic sensors and 2. Vulnerable and malicious website analysis tools. Article 7(b) authorizes a controller to process personal data if the processing is necessary to pre-contractual measures or to the performance of a contract. In the case of ACDC, only the second part (performance of a contract) is applicable. The laws of Belgium, France, Italy, Portugal, Romania, Spain and the Netherlands have transposed the exact terms of Article 7(b) into national legislation. Therefore, the deployment of the two above mentioned group tools in these countries does not present additional barriers besides the ones already clarified in this examination (e.g. the necessity test, as clarified by the Article 29 Working Party).

Although the German Federal Data Protection Act does not explicitly refer to the term “contract”, Section 28(1)(1) of the act considers lawful the processing that is necessary to create, perform or terminate a legal obligation or quasi-legal obligation with the data subject. In terms of result, this provision is equivalent to other examples of implementation of Article 7(b), as the terms of a contract amount to a legal obligation between the parties.

Slovenian law (Article 10(2), Personal Data Protection Act) requires the processing to be not only necessary but also appropriate to the performance of the contract. The definition of appropriateness is one that must be analysed in a case-by-case basis and shall be assessed in the light of Slovenian jurisprudence. In general terms, a processing is considered appropriate if sufficient to achieve the purpose of the operation and non-excessive. Appropriateness is an element comprised in the concept of fair processing of data and therefore is already an implicit aspects of every processing. To conclude, despite requiring the processing to be necessary and appropriate, Slovenian law does not create relevant issues to the deployment of the tools.

5.4 Implementation of Article 7(c) – Network traffic sensors and Vulnerable and malicious website analysis tools

The use of Article 7(c) in the context of ACDC is one that looks at three different provisions that, combined, will offer a fair basis for the use of this legitimate ground. First, a general duty that requests controllers to ensure security of the processing (following the implementation of Article 17 of the Data Protection Directive). Second, a specific obligation that requires ISPs to provide for security of their networks (following Article 4 of e-Privacy Directive). Third, a national provision implementing Article 7(c) itself. In some cases, countries have extended the nature of this controller duty to provide for security of the processing and the ISP's obligation to secure networks against threats. Albeit these may enhance the level of specificity and clarity about the level and standards of security expected in the country, the provisions of the Directives are already sufficient to legitimise the operation of the tools in the circumstances previously clarified in this document.

Concerning the general duty imposed on controllers to guarantee the security of the processing, the laws of Belgium, France, Italy, Portugal, Romania, Spain and the Netherlands have transposed Article 17 of Data Protection Directive with minor differences. Section 9 of the German Federal Data Protection Act transposes the terms of Article 17 by adding a necessity test on the measures to be deployed by controllers. According to the German legislator, necessary measures are only the ones where there is a reasonable proportion between the effort required from the controller and the desired purpose of protection. A brief analysis of the aim of the necessity test reveal that this complement tries to prevent that burdensome standards would be required from data controllers, what is also covered by Article 17. Further security requirements imposed by German law are covered under Annex to Section 9 (first part) and include different aspects of security control. The detailed elements specified by German law under the Annex do not hinder the application of Section 9 to ACDC. On contrary, they actually enhance the need for security of processing and provide an even more solid ground for the deployment of botnet mitigation tools. The Slovenian Personal Data Protection Act also provides for further details on which elements shall be secured by the controller, but does not create any barriers to the use of the general duty to provide for security.

The ISP obligation to provide for security of the networks (Article 4, e-Privacy Directive) is to be mostly found in instruments other than the Data Protection Law[173]. It is worth to recall that the use of Article 7(c) in the circumstances of the implementation of Article 4 of Directive 2002/58 is only relevant and applicable to ISPs. The laws of Belgium, France, Germany, Italy, Portugal, Romania, Slovenia, Spain and the Netherlands have transposed the terms of the Directive with minor differences. Every country analysed has implemented the terms of Article 4 and many have deepened the nature of this security

[173] See Table 1.

obligation and imposed further technical and organizational requirements to be taken into account by ISPs. Without entering into detail on the elements of each of the security obligations created by national laws, it suffices to say that our study has verified that each of the examined countries do impose a legal obligation on the ISPs operating in public networks to guarantee the security of their networks.

While the previous categories of provisions create a security obligation for controllers, they are not sufficient to legitimise the operation of the network sensors and vulnerable and malicious malware analysis tools. Once again, to be lawful a processing must fall within one of the legitimate grounds created by Article 7 of Data Protection Directive. Only the existence of a duty to provide for security of processing (applicable to all controllers) and of a duty to ensure security of networks (applicable to ISPs) can trigger the use of Article 7(c) in the context of ACDC. The grounds and elements relating to the use of this provision have been exposed above. Finally, the laws of Belgium, France, Italy, Portugal, Romania, Slovenia, Spain and the Netherlands have transposed the terms of the Directive without significant differences.

Our analysis has revealed that the laws of Germany and Slovenia have not transposed the terms of Article 17 in conformity with the Data Protection Directive. Both Member States seem to lack implementation of a legitimate grounds authorizing the processing of personal data where the processing is carried out as a necessary measure to comply with a legal obligation to which the controller is subject.

The German Federal Data Protection Law establishes that a processing shall be lawful if permitted or required by law (Section 4(1)) or if necessary to perform a legal obligation with the data subject (Section 28(1)(1)). This construction restricts the possibility of having a controller processing personal data to fulfil an obligation created by a law which does not explicitly prescribes that the necessary processing is allowed or permitted. Such is the case of the general duty to provide for security of processing (Section 9 and Annex, Federal Data Protection Act) and the ISP’s obligation to ensure security of its networks (Section 109(1) and (2), Telecommunications Act (TKG)). Finally, Article 10 of the Slovenian Personal Data Protection Act does not foresee compliance with a legal duty as a legitimate ground for processing of personal data by entities in the private sector.

The exhaustive and restrictive list[174] created by Article 7 ensures that a processing conducted in accordance with these legitimate grounds is a lawful operation. In the Joined Cases C‑468/10 and C-469/10 that examined the nature of Article 7, the ECJ recalled that “*Member States cannot add new principles relating to the lawfulness of the processing of personal data to Article 7 of Directive 95/46 or impose additional requirements that have the effect of amending the scope of one of the six principles provided for in Article 7*”[175]. This being said, if a restriction created by national law constitutes a barrier to the free movement of personal data, such restriction is incompatible with Directive 95/46. Therefore, any implementation that fails to deliver the same amount of protection provided by the Directive 95/46 or that adds extra obstacles that prevent the use of the norms created by the Directive may be

[174] Joined Cases C‑468/10 and C‑469/10, para. 30.

[175] Joined Cases C‑468/10 and C‑469/10, para 32.

considered void by the ECJ. To conclude, the absence of a corresponding provision in the laws of Germany and Slovenia shall not prevent the deployment of network sensors or vulnerable and malicious website analysis tools when such processing is in accordance with Article 7(c) of Directive 95/46. Finally, even if the use of Article 7(c) would not be possible in this case, controllers operating network sensors and vulnerable and malicious malware website analysis tools can still legitimise the processing by fulfilling the requirements of the use of Article 7(f), as described below.

5.5 Implementation of Article 7(f) – Centralised Clearing Data House

The application of Article 7(f) – balance criterion - to ACDC is key. Since the Centralised Clearing Data House operates as a data controller but, given its constituency, does not hold a duty or a direct interest related to the security of public networks, the only legitimate grounds available to justify the operations of the platform are provided by 7(f) – a processing that is necessary for the purpose of the legitimate interest of a third party to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject. The laws of Belgium, France, Portugal, Romania and the Netherlands have transposed exact the terms of the Directive. By contrast, the analysis has revealed that the laws of Germany, Italy, Slovenia and Spain have created additional obstacles to the use of the provision, which are not necessarily in line with the terms of the Directive. As noted by Korff, there are notable differences in approach to the balance criterion in the Member States[176].

The processing carried out in the CCH can make use of Section 28(2)(2)(a) and (b), since the CCH does not hold an own commercial purpose. In fact, the processing is necessary to safeguard the interests of a third party (a) and also necessary to prevent threats to public security and to prosecute crimes (b). In addition, German law requires that a processing falling within Section 28(2)(a) or (b) demonstrates that no reason exists to believe that the data subject has a legitimate interest in ruling out the processing. Albeit using a specific wording, the application of Section 28(2)(2)(a) and (b) to the processing conducted by the CCH is clear and the balance test is also fulfilled. As explained above, data subjects whose data are being processed under the CCH do not hold a legitimate interest in ruling out this processing. They either hold a legitimate interest in being informed about their condition as a victim and having access to disinfection or hold an illegitimate interest of not having their criminal activities dismantled. To this end, the CCH should not face major difficulties under German law. Finally, a minor obstacle can be created by the limitations in the processing created by Section(2)(2) caput, which only allows for use and transfer of data in the circumstances of the *alineas* (a) and (b). It is not clear whether use comprises other types of processing or requires the data to be processed without alterations. Limiting the types of processing allowed by such exception, however, would contradict the expectation of direct effect of Article 7(f), as ruled by the ECJ in the joined cases C-468/10 and C-469/10. This is because Article 7(f) does not restrict the types of processing that shall be allowed by the balance provision and restricting the scope of the provision could result in a invalid limitation.

[176] Korff, Working paper no. 2, op. cit., p. 72.

Terminology is also the issue presented by the Spanish and Slovenian Data Protection Laws. The first requires the use of Article 6(2) to be made without making the rights and freedoms of data subjects vulnerable. The second requires the controller' and the third party's interest to "clearly" overweight the interests of data subjects (Article 10(3)). In light of the ECJ appreciation of Article 7(f) and its direct effect, the most reasonable option is to interpret such provision in conformity with the intention of the Directive. Any other interpretation that would limit the application and scope of the balance provision would inevitably be in contradiction with the terms of the Directive and with the case law of the ECJ.

Finally, the limitation imposed by the Italian legislator under Article 24(g), which restricts its use to the cases specified by the DPA (Garante) is clearly in incompliance with the Data Protection Directive. As already clarified by the ECJ, "*Article 7(f) sets out two cumulative conditions that must be fulfilled in order for the processing of personal data to be lawful: firstly, the processing of the personal data must be necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed; and, secondly, such interests must not be overridden by the fundamental rights and freedoms of the data subject.*

It follows that, in relation to the processing of personal data, Article 7(f) of Directive 95/46 precludes any national rules which, in the absence of the data subject's consent, impose requirements that are additional to the two cumulative conditions set out in the preceding paragraph."

In fact, giving Member States discretion to implement Article 7(f) in a flexible manner would undermine the value of the provision. Article 7(f) has direct effect and precludes any national rules in contradiction with the terms of the Directive. To conclude, once the CCH fulfils the criteria of Article 7(f) as set forth by the Data Protection Directive, no obstacles should be raised by national rules so as to hamper this outcome.

6. CONCLUSION

This deliverable analysed the legal requirements of the Advanced Cyber Defence Centre in light of the current and applicable EU data protection framework. Section 2 clarified the requirements and standards of data protection law in the EU, including issues of data quality, legitimation grounds, allocation of liability between controllers and processors, the duty to ensure network security, transborder data flows, among others. Section 3 clarified frequent questions on the cooperation between ACDC partners and law enforcement. Section 4 brought a detailed explanation of the functioning and key legal requirements involved in the lawful implementation of the 5 group tools. Finally, Section 5 summarized the main legal issues and verified the feasibility of ACDC before the national laws of selected countries members.

In light of the information received and collected from partners, our analysis has verified the compatibility of ACDC with the current EU data protection framework and the laws of the sampled Member States. In the course of this analysis, a series of specific requirements is asked from partners in order to make the implementation of the project smoother and in compliance with the law. The findings included conflicts in terminology and requirements that could hamper the successful deployment of ACDC but that cannot be maintained in face of the jurisprudence of the European Court of Justice.

7. ANNEX - WP1 - ACDC Legal Questionnaire

Task 1.2.1 – Legal Requirements

Introduction

Under the Advanced Cybercrime Defence Centre project, KU Leuven has been charged of clarifying the legal rules applicable to each of the five group tools created to fight botnets. This task involves the study of how these tools will be received by national legal frameworks (Belgium, France, Germany, Portugal, Romania, Slovenia and The Netherlands). To this end, this questionnaire will be used to understand and identify the legal provisions applicable to the overall project and to each tool individually. The analysis of the responses will generate an input that will feed legal requirements and will other stages of the project.

The answers provided by you will be essential to our informed analysis. The questionnaire has 25 questions divided in five sections, where Section 1 is an overview of data privacy and cybercrime rules and Section 2 aims to identify whether ACDC Monitoring Sensors and Malware Analysis tools are to be considered legitimate means for detection and mitigation according to national laws. Section 3 on the Centralised Clearing Data House and the National Support Centre targets:

1. Whether ISPs and CERTs are allowed to share data of infections;
2. Who is allowed to receive this data;
3. If this sharing shall be limited to certain types of data
4. Which elements must be put in place to ensure the Centralised Clearing Data House and National Support Centre are compliant with multiple data privacy frameworks

Finally, Section 4 on End Customer tools examines how national laws deal with liability issues in cleaning software tools and customer consent and Section 5 brings an open question for additional contribution.

This questionnaire is sent to the following ACDC partners, which shall fill in the questions according to their national laws:

- B-CCENTRE/KUL (Belgium)
- Signal Spam (France)
- ECO (Germany)
- Telecom Italia (Italy)
- FCCN (Portugal)
- CERT-RO (Romania)
- XLAB (Slovenia)
- Inteco (Spain)
- TU Delft (The Netherlands)

Please answer the questions with the consolidated law in the format of a hyperlink (preferably in English) and indicate the relevant articles, when applicable.

Do not hesitate to contact us in the case you further assistance.

Deadline: September 6, 2013.

Best regards,

B-CCENTRE, KU Leuven

7.1 BELGIUM

Section 1 - Overview

This section calls for the major national instruments with regards to data privacy and cybercrime.

1) **Which law(s) has/have implemented Directive 95/46 (Data Protection Directive) in your jurisdiction?**

Act of 11 December 1998 implementing directive 95/46/EG 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.

2) **Which law(s) has/have implemented Directive 2002/58 (e-Privacy Directive) in your jurisdiction?**

Act of 18 Mai 2009 relating to various provisions on electronic communications

Act of 10 July 2012 relating to various provisions on electronic communications

3) **Which law(s) has/have implemented the Council of Europe Convention – 185 on Cybercrime (Budapest Convention) in your jurisdiction?**

Ratification: Act of 3 August 2012 ratifying the Convention on Cybercrime.

Similar to the provisions of the Convention on Cybercrime: Act of 28 November 2000 on cybercrime.

4) **Is there specific national legislation criminalising botnets?**

☐ No
☒ Yes - art. 550 bis & 550 ter Criminal Code (Hacking & IT sabotage) (French version: here)

5) **Has your country implemented the exceptions provided by article 13(1) of Directive 95/46?**[177]

[177] Article 13 - Exemptions and restrictions
1. Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6 (1), 10, 11 (1), 12 and 21 when such a restriction constitutes a necessary measures to safeguard:
(a) national security;
(b) defence;
(c) public security;
(d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;
(e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;

☐ No

☒ Yes – it is addressed in Article 3 of the Act of 8 December 1992 regarding the protection of privacy with respect to the processing of personal data

6) **Has your country implemented the exceptions provided by article 15(1) of Directive 2002/58[178]?**

☐ No

☒ Yes - it is addressed in Articles 122, 125, 126 and 127 of the Act of 13 June 2005 regarding electronic communication.

7) **Which actors are involved in the prevention and detection of cybercrime in your country? Please describe their roles and cooperation with law enforcement.**

(f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);

(g) the protection of the data subject or of the rights and freedoms of others.

[178] Article 15 - Application of certain provisions of Directive 95/46/EC

1. Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union.

BelNIS – The national consultation platform for information security – created by the Ministerial Committee for Intelligence and Security – brings together key departments within the government who are in charge of matters relating to information security. This consultation platform has been very active in the creation of CERT.be and the drafting of the national cyber security strategy. Permanent members are a.o. FCCU, the military intelligence service (ADIV), the national centre for crisis management (ADCC), Security of the State, national anti-terrorism centre (OCAD-OCAM), the board of Prosecutors-general.

FCCU – The Federal Computer Crime Unit (FCCU) is the unit of the federal judicial police in charge of providing specialised support to the central investigation services or regional computer crime units for the investigation of ICT-systems in traditional cases. It also supports the regional computer crime units in the investigation of complex cybercrime cases. Finally, the FCCU has dedicated R&D activities for digital forensic analysis.

CERT.be – The Federal Cyber Emergency Team is operated by Belnet, the Belgian national research network, on behalf of Fedict. It is the national CERT and as such member of the global CERT-network. Its main task is to provide assistance to companies and individuals in the handling of cyber security incidents.

Fedict – The Federal Public Service (FPS) Information and Communication Technology is mainly responsible for the implementation of e-government services.

B-CCENTRE – The Belgian Cybercrime Centre of Excellence for Training, Research and Education is the central coordination and collaboration platform in the fight against cybercrime, combining expertise of academic research groups, industry players and public organisations. The B-CCENTRE is a member of the 2CENTRE network, a pan European network of national cybercrime centres, dedicated to the dissemination of trainings and research results in the area of cybercrime.

Prime Minister’s Office – The Prime Minister is responsible for the implementation of the national cyber security strategy, making him the main driver behind policy initiatives in that area.

Others – the national supervisory authority for the telecoms industry (BIPT), the national bank (NBB), the Internet Service Providers Association (ISPA), the financial sector federation Febelfin, the national data protection authority (Privacycommissie), …

8) How does your law address the cooperation of ISPs in criminal investigation?

Art. 46 bis Code of Criminal Procedure obliges operators of an electronic communication network and providers of an electronic communication service to cooperate upon request of the public prosecutor in order to:
- identify the subscriber or user of an electronic communication service or
- identify electronic communication services on which a specified person has been a subscriber or user.

Noncompliance is punishable by a fine of 26-10000 euros.

Art. 88 bis Code of Criminal procedure obliges operators of an electronic communication network and providers of an electronic communication service to cooperate upon request of the investigating judge in order to:
- trace traffic data of telecommunication means which is the source or destination of a communication.
- locate the sender or receiver of telecommunication.

Noncompliance is punishable by a fine of 26-10000 euros.

Art. 88 quarter Code of Criminal Procedure obliges to cooperate during an investigation upon request of the investigating judge.
Who? Persons who have special capacities/knowledge concerning the computer system, which is the object of an investigation or of services used to store, process, encrypt or transfer data.
What?
(1) Obligation to provide information concerning how the system works or how one can get access to the stored data in an understandable format.

(2) Obligation to operate the system to deliver the data or to search it and to give access, copy the data or to make them inaccessible or delete them.
Noncompliance is punishable by 6 months to 1 year of imprisonment and/or a fine of 26-20000 euros.

Art. 90 quarter §2 Code of Criminal Procedure obliges operators of an electronic communication network and providers of an electronic communication service to provide technical assistance to a data tapping measure upon request of the investigating judge.
Noncompliance is punishable by a fine of 26-1000 euros.

Art. 90 quarter §4 Code of Criminal Procedure: similar to art. 88 quarter, concerning data tapping measure.
Noncompliance is punishable by 6 months to 1 year of imprisonment and/or a fine of 26-20000 euros.

Like criminal fines, laid down by the Criminal Code, these fines have to be multiplied by a factor to counter the effects of currency inflation. The '*décimes additionnels*' ('opdeciemen') were recently raised to fifty décimes (5 units) by the Act of 28 December 2011 concerning diverse provisions relating to justice II. (→ fine multiplied by 6)

Section 2 - Monitoring Sensors and Malware Analysis Tools

9) ACDC sensors and detection tools will make 19 solutions available to partners. Are any of the following technologies or similar tools being used in your country (please check D.2.3 - Annex 1)?

1) ☐ Wildfire (LSEC)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

2) ☐ Spamtrap and low interaction honeypot(s) multipurpose appliance (CARNet)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

3) ☐ Passive DNS replication appliance (CARNet)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

4) ☐ Mediation server for sensors and Near real-time drive by download component (CARNet)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

5) ☐ HoneyNetRO (CERT-RO)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

6) ☐ Spam Analysis Tool (CERT-RO)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

7) ☐ Fortigate (CERT-RO)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

8) ☐ SPAM-BOT detection (TID)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

9) ☐ DNS-based BOT detection (TID)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

10) ☐ Smart BOT Detector (TID)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

11) ☐ SDN Malware Detector (TID)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

12) ☐ MonitoringHub and Accounting Manager (XLAB)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

13) ☐ Suricata Engine (XLAB)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

14) ☐ KB-IDS for Android (XLAB
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

15) ☐ AHPS (ATOS)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

16) ☐ Montimage Monitoring Tool (MI)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

17) ☐ Honeynet Network (TI)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

18) ☐ Operational Intelligence Centre (CASSIDIAN)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

19) ☐ Cyber threat detection (ECO)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

10) ACDC malware analysis tools will make 7 solutions available to partners. Are any of the following technologies or similar tools being used in your country (please check D.2.3 - Annex 1)?

1) ☐ WebCheck (CyDef)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

2) ☐ SiteVet (CyDef)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

3) ☐ HoneyUnit (FKIE)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

4) ☐ PDF Scrutinizer (FKIE)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

5) ☐ HoneyclientDispatcher (FKIE)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

6) ☐ Skanna (INTECO)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

7) ☐ Initiative-S (ECO)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

A – Internet Service Providers

11) Does your law enable ISPs to detect infections and identify infected users?

☐ No - (see question 11.1)
☒ Yes – Article 114 of the Act of 13 June 2005 regarding electronic communication (see questions 11.2 to 11.3)

11.1) Do ISPs in practice do so?

☐ No
☒ Yes - (see questions 11.2 to 11.3)

11.2) What kind of data is processed by ISPs in these detections and identifications?

11.3) Do they deploy monitoring sensors?

☐ No
☐ Yes – **If so, which aspects of this monitoring sensors make it data privacy compliant?**

B – National Computer Emergency Response Teams

12) Is there a national or research CERT established in your country?

☐ No
☒ Yes – (CERT.be, the federal cyber emergency team, was set up in 2009 and is operated by Belnet, the Belgian national research network, on behalf of Fedict. https://www.cert.be/pro/ (see questions 12.1 to 12.2)

12.1) Do they deploy monitoring sensors?

☐ No
☐ Yes – **If so, which aspects of this monitoring sensors make it data privacy compliant?**

12.2) What kind of data is processed by CERTs in these detections?

Section 3 - Centralised Clearing Data House and National Support Centre

13) **Are there private or public-private partnerships established in your country where data concerning malware infections is exchanged?**

☐ No

☐ Yes – How is data collected and what kind of data is shared among partners?

14) **Are there other private or public-private partnerships dealing with other aspects of cybersecurity (besides malware infections data sharing)? Please explain how they operate.**

Belgian Cyber Security Round Table (BCSRT) – a PPP initiative co-organised by Febelfin and B-CCENTRE in response to the envisaged PPP objective in the national Cyber Security Strategy.

15) **In which circumstances are IP-addresses, whether dynamic or static, considered as personal data in your country?**

In Belgium, IP address is considered personal data (but debatable). Art. 1 Act of 8 December 1992 (French: here) : personal data shall mean any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. Opinion 4/2007 of the art. 29 data protection working group is considered important in understanding the concept of personal data.

16) For how long are ISPs required to retain data in the terms of article 6 of Directive 2006/24/EC (Data Retention Directive)[179]?

The Data Retention Directive has not been transposed into Belgian law.

17) Are there circumstances in which the monitoring of communications by ISPs will not be considered an offence or a violation of privacy?

☐ No
☒ Yes, there are several circumstances described in article 125 of the Act of 13 June 2005 regarding electronic communication where monitoring is indeed legitimate and is not considered an offence nor a violation of privacy.

18) Are ISPs allowed to share data of infections with other service providers?
☐ No
☒ Yes – if so, is this limited to a certain type of data? Not explicitly, but there are additional safeguards in place where it concerns personal data. (see article 114 of the Act of 13 June 2005 regarding electronic communication)

19) Are ISPs allowed to directly communicate to a customer identified as victim or author of an infection?

☐ No
☒ Yes – see article 114/1 of the Act regarding electronic communication.

20) Are ISPs required to communicate detections/identifications to law enforcement agencies or other public authorities?

☐ No
☒ Yes - Art. 21 §2 act of 11 March 2003 concerning certain legal aspects of information society services.

21) Are CERTs allowed to share data of infections with actors others than law enforcement?

☐ No
☒ Yes – if so, is this limited to a certain type of data? Regard must be had for where it concerns personal data, since specific safeguards apply.

22) Are CERTs allowed to directly communicate to a user identified as victim or author of an infection?

☐ No
☒ Yes – The CERT does not have a specific legal framework in which to operate, so it falls under general legal framework.

[179] Article 6 - Periods of retention
Member States shall ensure that the categories of data specified in Article 5 are retained for periods of not less than six months and not more than two years from the date of the communication.

Section 4 - End customer tools

Concerning the practice of malware cleaning software in your country:

23) **How do they assign liability for damages caused to customers and other users (non-customers)?**

24) **How do they ask, record and store user's consent?**

Section 5 – Additional information

25) **Is there any additional information you would like to add that could help us with the analysis or any legal challenge that has not been addressed?**

End of questionnaire

7.2 FRANCE

Section 1 - Overview

This section calls for the major national instruments with regards to data privacy and cybercrime.

1) **Which law(s) has/have implemented Directive 95/46 (Data Protection Directive) in your jurisdiction?**

ACT N°78-17 OF 6 JANUARY 1978 ON INFORMATION TECHNOLOGY, DATA FILES AND CIVIL LIBERTIES « Loi Informatique et libertés »

2) **Which law(s) has/have implemented Directive 2002/58 (e-Privacy Directive) in your jurisdiction?**

The Directive 2002/58/EC was implemented throught **Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (1), notably article 6,** and **Ordnance N°** 2011-1012 of 24 August 2011 on e-communications.

The Ordnance was implemented in numerous preexistent laws, the most important for our issues are:

Amendment of the "Loi Informatique et libertés », which is the French Data protection Act :

Article 32 II amended by **Ordnance N°** 2011-1012 of 24 August 2011 on e-communications (art 37) / Information concerning cookies (technical cookies or tracking cookies)

Article 34 II amended by **Ordnance N°** 2011-1012 of 24 August 2011 on e-communications (art 38) / Notification of security breach involving personnel data

Amendment of the French "Code pénal" which is the French criminal code which contains rules of substantive criminal law:

Article 226-17-1 amended by **Ordnance N°** 2011-1012 of 24 August 2011 on e-communications (art 39)

Article 226-3 amended by **Ordnance N°** 2011-1012 of 24 August 2011 on e-communications (art 44)

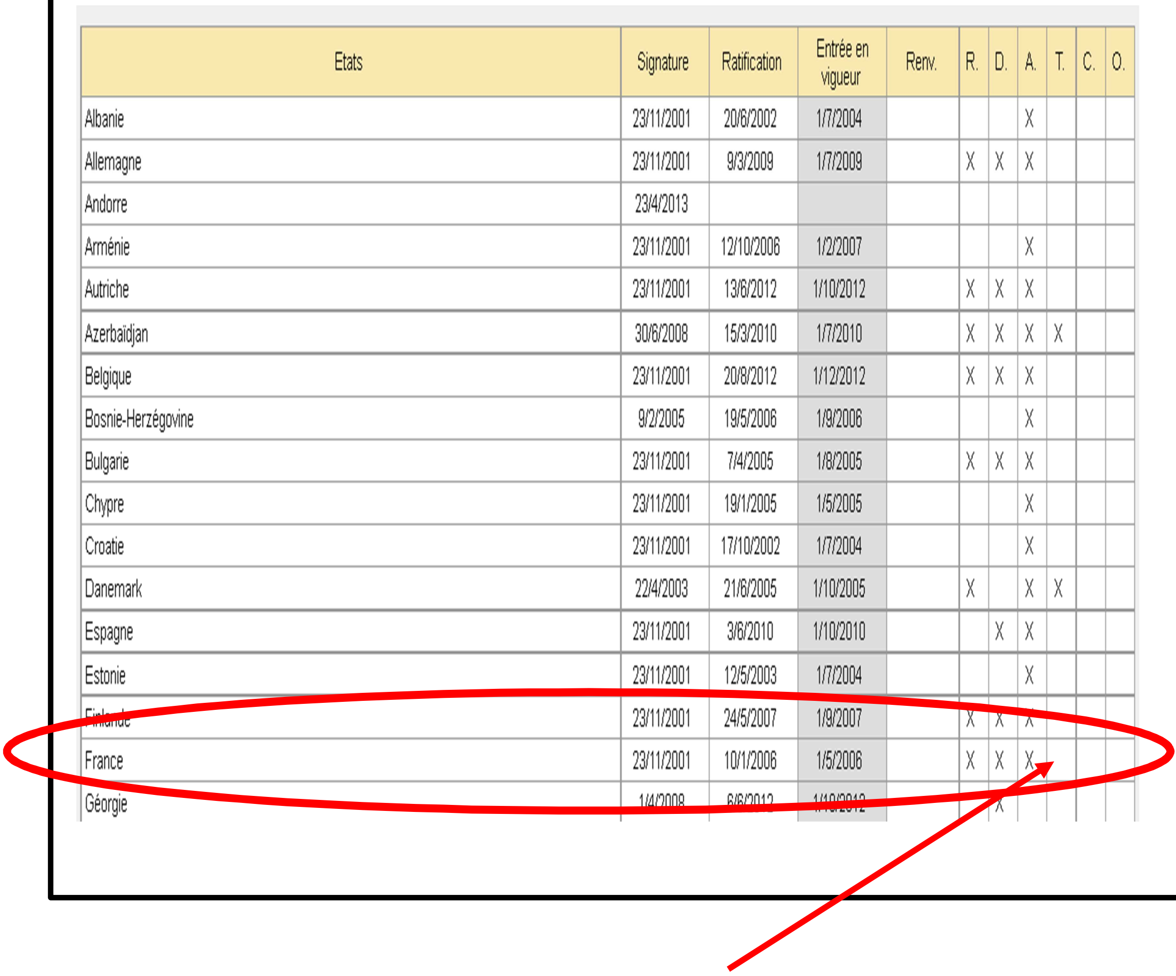
Amendment of the French "Code des postes et des télécommunications » which is the French Post and Electronic Communications Code by **Ordnance N°** 2011-1012 of 24 August 2011 on e-communications (art 1 to 31 and 40 to 43 and 47 to 56)**, notably concerning security issues:**

Articles L.32, L.32-1, L.33-4 and L.33-1 (especially the a)), L.33-10, L.34-1 (especially the I), L.34-5, L. 34-8-3 and L. 34-8-4, L.36-6, L.42,

Amendment of the French "Code de la Consommation" which contains rules to protect consumers and costumers. by **Ordnance N°** 2011-1012 of 24 August 2011 on e-communications (art 32 to 36)

3) **Which law(s) has/have implemented the Council of Europe Convention – 185 on Cybercrime (Budapest Convention) in your jurisdiction?**

France didn’t already territorial application: clic here to access the detailed list



Etats	Signature	Ratification	Entrée en vigueur	Renv.	R.	D.	A.	T.	C.	O.
Albanie	23/11/2001	20/6/2002	1/7/2004				X			
Allemagne	23/11/2001	9/3/2009	1/7/2009		X	X	X			
Andorre	23/4/2013									
Arménie	23/11/2001	12/10/2006	1/2/2007				X			
Autriche	23/11/2001	13/6/2012	1/10/2012		X	X	X			
Azerbaïdjan	30/6/2008	15/3/2010	1/7/2010		X	X	X	X		
Belgique	23/11/2001	20/8/2012	1/12/2012		X	X	X			
Bosnie-Herzégovine	9/2/2005	19/5/2006	1/9/2006				X			
Bulgarie	23/11/2001	7/4/2005	1/8/2005		X	X	X			
Chypre	23/11/2001	19/1/2005	1/5/2005				X			
Croatie	23/11/2001	17/10/2002	1/7/2004				X			
Danemark	22/4/2003	21/6/2005	1/10/2005		X		X	X		
Espagne	23/11/2001	3/6/2010	1/10/2010			X	X			
Estonie	23/11/2001	12/5/2003	1/7/2004				X			
Finlande	23/11/2001	24/5/2007	1/9/2007		X	X	X			
France	23/11/2001	10/1/2006	1/5/2006		X	X	X			
Géorgie	1/4/2008	6/6/2012	1/10/2012			X				

4) Is there specific national legislation criminalising botnets?

☑ No

☐ Yes - ____

5) Has your country implemented the exceptions provided by article 13(1) of Directive 95/46?[180]

☑ No for articles 6§1 , 10, 11§1 and 21

☑ Yes for article 12 – it is addressed in articles 41 and 42 of the French Data protection Act

6) Has your country implemented the exceptions provided by article 15(1) of Directive 2002/58[181]**?**

☐No

☑ Yes it is mostly addressed in :

- the French « Code Pénal »
- article 47 **Ordnance N°** 2011-1012 of 24 August 2011 on e-communications
- « *Décret n° 2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne* ».

[180] Article 13 - Exemptions and restrictions
1. Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6 (1), 10, 11 (1), 12 and 21 when such a restriction constitutes a necessary measures to safeguard:
(a) national security;
(b) defence;
(c) public security;
(d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;
(e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;
(f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);
(g) the protection of the data subject or of the rights and freedoms of others.

[181] Article 15 - Application of certain provisions of Directive 95/46/EC
1. Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union.

7) Which actors are involved in the prevention and detection of cybercrime in your country? Please describe their roles and cooperation with law enforcement.

France has taken account of the emergence of the use of the internet and cybercrime.

For exemple, the Act of 5 March 2007 relating to the prevention of delinquency has thus set up cyberpatrols whose objective is to prevent certain offences and combat them more effectively, to gather evidence about them and to seek out the perpetrators when the offences are committed by electronic means.

The French Government is taking this problem very seriously and has created the Central Office for Action to Combat Crime connected with Information Technology and Communication, for example, which has had:

- a national database to identify illicit content since 1 September 2006.
- a national network of special investigators (261 investigators)

The Central Office for Action to Combat Crime is in a partnership with:

- for the national issues: the investigators of Gendarmerie (the N'TECH)
- fort the internationals issues: the following networks H24 du G8, EUROPOL et INTERPOL

From an organizational standpoint, improvement focused on three areas:

- Operational section: processes only specifics and complex cases for example concerning payment cards issues
- Technical section: support services and investigate thanks to a high level software and hardware to collect information
- Processing of interlinks alerts: lunched in 6 January 2009, the platform "PHAROS" and "Info-escroqueries" to report illicit behaviours.

The ANSSI (Public Network Security National Agency) is the main governmental Agency to focus on Botnet issues.

Signal Spam is a public private partnership in charge of collecting data from citizen on spam and other cyber crime threats and sharing the data among stakeholders.

8) How does your law address the cooperation of ISPs in criminal investigation?

Except specific cooperation concerning terrorism, the following law address the cooperation of IPSs in criminal investigations:

Article 6 of the LCEN « Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (1) » and *Décret n° 2011-219 du 25 février 2011* organize the condition of the:

- Communication of the data from the ISP to the national authorities.
- Prevention from internet security failures.
- Prevention from penal infractions (ex : Article L.336-3 of CPI)

Article 34 bis of the French Data Protection Act create a new process on the CNIL website :

In the event of a breach of personal data, the provider of public electronic communication services shall notify forthwith the Commission Nationale de l'Informatique et des Libertés (CNIL). Whenever said violation is likely to breach personal data security or the privacy of a subscriber or any other individual, the provider shall also notify the party affected forthwith.

Notification of a breach of personal data to the affected party shall however not be required if the CNIL has found that appropriate protection measures have been implemented by the service provider to ensure that the personal data are made undecipherable to any unauthorized individuals and have been applied to the data affected by said breach.

Failing this, the CNIL may serve the service provider with a formal notice to inform the affected parties as well, after investigating the severity of the breach.

Each provider of electronic communication services shall keep an updated record of all breaches of personal data, listing in particular the conditions, effects and measures taken as remedies, and shall make said record available to the Commission upon request.

Section 2 - Monitoring Sensors and Malware Analysis Tools

9) ACDC sensors and detection tools will make 19 solutions available to partners. Are any of the following technologies or similar tools being used in your country (please check D.2.3 - Annex 1)?

1) ☐ Wildfire (LSEC)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

2) ☐ Spamtrap and low interaction honeypot(s) multipurpose appliance (CARNet)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

3) x Passive DNS replication appliance (CARNet)
By x ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

4) ☐ Mediation server for sensors and Near real-time drive by download component (CARNet)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

5) ☐ HoneyNetRO (CERT-RO)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

6) ☐ Spam Analysis Tool (CERT-RO)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

7) ☐ Fortigate (CERT-RO)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

8) ☐ SPAM-BOT detection (TID)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

9) ☐ DNS-based BOT detection (TID)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

10) ☐ Smart BOT Detector (TID)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

11) ☐ SDN Malware Detector (TID)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

12) ☐ MonitoringHub and Accounting Manager (XLAB)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

13) ☐ Suricata Engine (XLAB)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

14) ☐ KB-IDS for Android (XLAB
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

15) ☐ AHPS (ATOS)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

16) ☐ Montimage Monitoring Tool (MI)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

17) ☐ Honeynet Network (TI)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

18) ☐ Operational Intelligence Centre (CASSIDIAN)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

19) ☐ Cyber threat detection (ECO)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

10) ACDC malware analysis tools will make 7 solutions available to partners. Are any of the following technologies or similar tools being used in your country (please check D.2.3 - Annex 1)?

8) ☐ WebCheck (CyDef)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

9) ☐ SiteVet (CyDef)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

10) ☐ HoneyUnit (FKIE)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

11) ☐ PDF Scrutinizer (FKIE)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

12) ☐ HoneyclientDispatcher (FKIE)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

13) ☐ Skanna (INTECO)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

14) ☐ Initiative-S (ECO)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

A – Internet Service Providers

11) Does your law enable ISPs to detect infections and identify infected users?

☑ No - (see question 11.1)
☐ Yes - (see questions 11.2 to 11.3)

11.1) Do ISPs in practice do so?

☐ No
☑ Yes - (see questions 11.2 to 11.3)

11.2) What kind of data is processed by ISPs in these detections and identifications?

Thanks to SIGNAL SPAM actions, ISPs may proceed to those investigations.

ISPs need formal reports from citizen to investigate a device infection : Signal Spam provides ISPs with reports from end users

11.3) Do they deploy monitoring sensors?

X No
☐ Yes – **If so, which aspects of this monitoring sensors make it data privacy compliant?**

B – National Computer Emergency Response Teams

12) Is there a national or research CERT established in your country?

☐ No
X Yes - ______________(CERT name)_ANSSI________(see questions 12.1 to 12.2)

12.1) Do they deploy monitoring sensors?

☐ No
☐ Yes – **If so, which aspects of this monitoring sensors make it data privacy compliant?**

12.2) What kind of data is processed by CERTs in these detections?

Section 3 - Centralised Clearing Data House and National Support Centre

13) Are there private or public-private partnerships established in your country where data concerning malware infections is exchanged?

☐ No

X Yes – How is data collected and what kind of data is shared among partners?

Reports on spam from End users

Shared through data feed to duly authorized members of Signal Spam

14) Are there other private or public-private partnerships dealing with other aspects of cybersecurity (besides malware infections data sharing)? Please explain how they operate.

Phishing Inititiative : reports of phishing URL on internet

AFA : abusive contents on internet (private / European fundings)

Pharos

15) In which circumstances are IP-addresses, whether dynamic or static, considered as personal data in your country?

IP-addresses, whether dynamic or static, are considered as personal data in France in major part of cases.

The only exception could be if no one may be identifying directly or indirectly.

16) **For how long are ISPs required to retain data in the terms of article 6 of Directive 2006/24/EC (Data Retention Directive)[182]?**

1 year mostly

17) Are there circumstances in which the monitoring of communications by ISPs will not be considered an offence or a violation of privacy?

☐ No
☑ Yes

18) Are ISPs allowed to share data of infections with other service providers?
☐ No
☑ Yes – if so, is this limited to a certain type of data? Datas mentioned in Q11-2

19) Are ISPs allowed to directly communicate to a customer identified as victim or author of an infection?

☐ No
☑ Yes

20) Are ISPs required to communicate detections/identifications to law enforcement agencies or other public authorities?

☐ No
☑ Yes, as mentioned in Q8 (Article 34 bis of the French Data Protection Act create a new process on the CNIL website)

21) Are CERTs allowed to share data of infections with actors others than law enforcement?

☑ No
☐ Yes – if so, is this limited to a certain type of data? ____________________________

22) Are CERTs allowed to directly communicate to an user identified as victim or author of an infection?

☐ No
☑ Yes

Section 4 - End customer tools

[182] Article 6 - Periods of retention
Member States shall ensure that the categories of data specified in Article 5 are retained for periods of not less than six months and not more than two years from the date of the communication.

Concerning the practice of malware cleaning software in your country:

23) **How do they assign liability for damages caused to customers and other users (non-customers)?**

24) **How do they ask, record and store user's consent?**

No instruction is required by law, only general recommendation. The consent must be stored and save in sufficient conditions to be used as a legal proof.

Section 5 – Additional information

25) **Is there any additional information you would like to add that could help us with the analysis or any legal challenge that has not been addressed?**

End of questionnaire

7.3 GERMANY

Section 1 - Overview

This section calls for the major national instruments with regards to data privacy and cybercrime.

1) **Which law(s) has/have implemented Directive 95/46 (Data Protection Directive) in your jurisdiction?**

Gesetz zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze. 18.5.2001: regularizes together with the Data Protection Acts of the German federal states and other area specific regulations the exposure to personal data which are manually processed in IT systems.

Federal Data Protection act. http://www.iuscomp.org/gla/statutes/BDSG.htm

2) **Which law(s) has/have implemented Directive 2002/58 (e-Privacy Directive) in your jurisdiction?**

Telekommunikationsgesetz-Reform 2004 : Telecommunication Act
http://www.bfdi.bund.de/cae/servlet/contentblob/411286/publicationFile/

On 15 October the German Federal Government adopted a draft new telecommunication act. The draft aims, inter alia, at implementing the European Directive on privacy and electronic communications (2002/58/EC), but will not introduce the spam-ban described in Article 13 of the Directive. In Germany spam will be banned through an update of the Act against Unfair Competition, and remain subject only to civil law.

3) **Which law(s) has/have implemented the Council of Europe Convention – 185 on Cybercrime (Budapest Convention) in your jurisdiction?**

http://www.gesetze-im-internet.de/englisch_stgb/

German Criminal Code (StGB): The StGB constitutes the legal basis of criminal law in Germany.

§§202b, 202c

§§303a, 303b

4) **Is there specific national legislation criminalising botnets?**

☐ **No (X) – but it is planned in the future**
☐ Yes - ____

5) **Has your country implemented the exceptions provided by article 13(1) of Directive 95/46?[183]**

□ **No (X)**
□ Yes – it is addressed in ______________________________

6) **Has your country implemented the exceptions provided by article 15(1) of Directive 2002/58[184]?**

□ **No (X)**
□ Yes - it is addressed in ______________________________

7) **Which actors are involved in the prevention and detection of cybercrime in your country? Please describe their roles and cooperation with law enforcement.**

- Politicians
- Executive
- Companies

8) **How does your law address the cooperation of ISPs in criminal investigation?**

The state has a right to request information from the ISPs during criminal investigations to receive IP-Adresses and other Meta-Information

[183] Article 13 - Exemptions and restrictions
1. Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6 (1), 10, 11 (1), 12 and 21 when such a restriction constitutes a necessary measures to safeguard:
(a) national security;
(b) defence;
(c) public security;
(d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;
(e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;
(f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);
(g) the protection of the data subject or of the rights and freedoms of others.

[184] Article 15 - Application of certain provisions of Directive 95/46/EC
1. Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union.

Section 2 - Monitoring Sensors and Malware Analysis Tools

9) ACDC sensors and detection tools will make 19 solutions available to partners. Are any of the following technologies or similar tools being used in your country (please check D.2.3 - Annex 1)?

1) ☐ Wildfire (LSEC)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

2) ☐ (X) Spamtrap and low interaction honeypot(s) multipurpose appliance (CARNet)
By ☐ **(X) ISPS**, ☐ webmasters, ☐ hosts, ☐ (X) **CERTs**, ☐ Law enforcement, ☐ end-users

3) ☐ Passive DNS replication appliance (CARNet)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☒ **CERTs**, ☐ Law enforcement, ☐ end-users

4) ☐ Mediation server for sensors and Near real-time drive by download component (CARNet)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

5) (X) HoneyNetRO (CERT-RO)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☒ **CERTs**, ☐ Law enforcement, ☐ end-users

6) ☒ Spam Analysis Tool (CERT-RO)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☒ **CERTs**, ☐ Law enforcement, ☐ end-users

7) ☐ Fortigate (CERT-RO)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

8) ☒ SPAM-BOT detection (TID)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☒ **CERTs**, ☐ Law enforcement, ☐ end-users

9) (X) DNS-based BOT detection (TID)
By **(X) ISPS,** ☐ webmasters, ☐ hosts, ☒ **CERTs**, ☐ Law enforcement, ☐ end-users

10) ☐ Smart BOT Detector (TID)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

11) ☐ SDN Malware Detector (TID)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

12) ☐ MonitoringHub and Accounting Manager (XLAB)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

13) ☐ Suricata Engine (XLAB)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

14) ☐ KB-IDS for Android (XLAB
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

15) ☐ AHPS (ATOS)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

16) ☐ Montimage Monitoring Tool (MI)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

17) **(X) Honeynet Network (TI)**
By ☒ **ISPS**, ☐ webmasters, ☐ hosts, ☒ **CERTs**, ☐ Law enforcement, ☐ end-users

18) ☐ Operational Intelligence Centre (CASSIDIAN)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

19) ☒ **Cyber threat detection (ECO)**
By ☒ **ISPS,** ☒ **webmasters,** ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

10) ACDC malware analysis tools will make 7 solutions available to partners. Are any of the following technologies or similar tools being used in your country (please check D.2.3 - Annex 1)?

15) ☒ **WebCheck (CyDef)**
By ☒ **ISPS,** ☒ **webmasters**, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☒ **end-users**

16) ☒ **SiteVet (CyDef)**
By ☒ **ISPS,** ☒ **webmasters,** ☒ **hosts,** ☒ **CERTs**, ☐ Law enforcement, ☒ **end-users**

17) ☐ HoneyUnit (FKIE)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

18) ☐ PDF Scrutinizer (FKIE)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

19) ☐ HoneyclientDispatcher (FKIE)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

20) ☐ Skanna (INTECO)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

21) ☒ **Initiative-S (ECO)**
By ☒ **ISPS,** ☒ **webmasters,** ☒ **hosts**, ☐ CERTs, ☐ Law enforcement, ☒ **end-users**

A – Internet Service Providers

11) Does your law enable ISPs to detect infections and identify infected users?

☐ No - (see question 11.1)
☐ Yes - ____(see questions 11.2 to 11.3)

11.1) Do ISPs in practice do so?

☐ No
(x) **Yes - (see questions 11.2 to 11.3)**

11.2) What kind of data is processed by ISPs in these detections and identifications?

- ISPs implemented server side measures: Anti-Spam
- Data from honeypots and 3rd parties is processed and given IP addresses are correlated with user data (usually only possible within the first 24hrs after the user gets an IP-address)
- Scan on websites (server forms, hosters) are performed

12.4) Are ISPs required to mention the existence of such detection/ identification mechanisms in their contract?

☐ No
☐ Yes - _________________________________(please provide a concrete example)

11.3) Do they deploy monitoring sensors?

☐ No
☒ **Yes – If so, which aspects of this monitoring sensors make it data privacy compliant?**

Sensors have no possibility to assign a customer to a IP, anonymisation / user stays unrecognized by sensor

Sensors have no customer data

B – National Computer Emergency Response Teams

12) Is there a national or research CERT established in your country?

☐ No
☐**x Yes – DFN-CERT_ & Bürger-CERT** (CERT name)___________________(see questions 12.1 to 12.2)

12.1) Do they deploy monitoring sensors?

☐ No
☒ Yes – **If so, which aspects of this monitoring sensors make it data privacy compliant?**

DFN-CERT can provide that data better than ECO.

12.2) What kind of data is processed by CERTs in these detections?

Section 3 - Centralised Clearing Data House and National Support Centre

13) **Are there private or public-private partnerships established in your country where data concerning malware infections is exchanged?**
☐ No
☐**X Yes – How is data collected and what kind of data is shared among partners?**

Data gets collected by 3rd party sensors

IP+Timestamp is submitted to ISPs

ISP is confirms / identifies user by Timestamp and IP

14) **Are there other private or public-private partnerships dealing with other aspects of cybersecurity (besides malware infections data sharing)? Please explain how they operate.**

Anti-spam organisations sharing data on spam mails

15) **In which circumstances are IP-addresses, whether dynamic or static, considered as personal data in your country?**

§111 & §113 Telekommunikationsgesetz

new law to be implemented

16) **For how long are ISPs required to retain data in the terms of article 6 of Directive 2006/24/EC (Data Retention Directive)[185]?**

Not yet implemented in Germany

17) **Are there circumstances in which the monitoring of communications by ISPs will not be considered an offence or a violation of privacy?**

☐ No
☒ **Yes – If it is transparent to the end-customer**

18) **Are ISPs allowed to share data of infections with other service providers?**
☐ No
☐**x Yes – if so, is this limited to a certain type of data?**
Anonymized, no customer data

[185] Article 6 - Periods of retention
Member States shall ensure that the categories of data specified in Article 5 are retained for periods of not less than six months and not more than two years from the date of the communication.

19) **Are ISPs allowed to directly communicate to a customer identified as victim or author of an infection?**

☐ No
(x)Yes - ____

20) **Are ISPs required to communicate detections/identifications to law enforcement agencies or other public authorities?**

☒ **No**
☐ Yes - ____

21) **Are CERTs allowed to share data of infections with actors others than law enforcement?**

☐ No
☒ **Yes** – if so, is this limited to a certain type of data? ISP

22) **Are CERTs allowed to directly communicate to an user identified as victim or author of an infection?**

☐ No
☒ **Yes - If possible**

Section 4 - End customer tools

Concerning the practice of malware cleaning software in your country:

23) **How do they assign liability for damages caused to customers and other users (non-customers)?**

Use of the tools at own risk and policy

24) **How do they ask, record and store user's consent?**

Very transparent, customer needs to opt-in on their own, otherwise it is not recorded, stored or submitted.

Section 5 – Additional information

25) **Is there any additional information you would like to add that could help us with the analysis or any legal challenge that has not been addressed?**

End of questionnaire

7.4 Italy

Section 1 - Overview

This section calls for the major national instruments with regards to data privacy and cybercrime.

1) **Which law(s) has/have implemented Directive 95/46 (Data Protection Directive) in your jurisdiction?**

Decreto Legislativo 196/03 – Codice Trattamento Dati Personali

http://www.garanteprivacy.it/documents/10160/2012405/DataProtectionCode-2003.pdf

2) **Which law(s) has/have implemented Directive 2002/58 (e-Privacy Directive) in your jurisdiction?**

Decreto Legislativo 196/03 – "Codice Trattamento Dati Personali"
(TITLE X – ELECTRONIC COMMUNICATIONS)

http://www.garanteprivacy.it/documents/10160/2012405/DataProtectionCode-2003.pdf

Decreto Legislativo 69/12 (Recepimento direttiva 2009/136/CE)

www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2012-05-

3) **Which law(s) has/have implemented the Council of Europe Convention – 185 on Cybercrime (Budapest Convention) in your jurisdiction?**

L.48/08 (Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalita' informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno)

http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2008;48

4) **Is there specific national legislation criminalising botnets?**
X No
☐ Yes - ____

5) **Has your country implemented the exceptions provided by article 13(1) of Directive 95/46?**[186]

[186] Article 13 - Exemptions and restrictions

☐ No
X Yes – it is addressed in D.Lgs. 196/03 various sections as section 47, 53, 58, 59 and so on

6) Has your country implemented the exceptions provided by article 15(1) of Directive 2002/58[187]?

☐ No
X Yes - it is addressed in D. Lgs.196/03 section 123, 125, 127, 132

7) Which actors are involved in the prevention and detection of cybercrime in your country? Please describe their roles and cooperation with law enforcement.

Polizia di Stato (Polizia Postale; CNAIPIC)

http://www.poliziadistato.it/articolo/10619-English/

Guardia di Finanza

http://www.gdf.gov.it/GdF/it/Home/index.html

TLC/ISP (Operators)

8) How does your law address the cooperation of ISPs in criminal investigation?

Law enforcement agencies collaborate through special departments with ISPs as well as with various certified forensic associations .

LEA can request the following services: Implementing procedures to capture log files, data traffic, mandatory services to the judicial authority, block of sites and/or removal of illegal contents. Cooperation with law enforcement on anti-pedophilia themes.

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

[187] Article 15 - Application of certain provisions of Directive 95/46/EC
1. Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union.

Section 2 - Monitoring Sensors and Malware Analysis Tools

9) ACDC sensors and detection tools will make 19 solutions available to partners. Are any of the following technologies or similar tools being used in your country (please check D.2.3 - Annex 1)? NO

1) ☐ Wildfire (LSEC)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

2) ☐ Spamtrap and low interaction honeypot(s) multipurpose appliance (CARNet)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

3) ☐ Passive DNS replication appliance (CARNet)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

4) ☐ Mediation server for sensors and Near real-time drive by download component (CARNet)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

5) ☐ HoneyNetRO (CERT-RO)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

6) ☐ Spam Analysis Tool (CERT-RO)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

7) ☐ Fortigate (CERT-RO)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

8) ☐ SPAM-BOT detection (TID)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

9) ☐ DNS-based BOT detection (TID)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

10) ☐ Smart BOT Detector (TID)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

11) ☐ SDN Malware Detector (TID)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

12) ☐ MonitoringHub and Accounting Manager (XLAB)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

13) ☐ Suricata Engine (XLAB)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

14) ☐ KB-IDS for Android (XLAB
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

15) ☐ AHPS (ATOS)

By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

16) ☐ Montimage Monitoring Tool (MI)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

17) ☐ Honeynet Network (TI)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

18) ☐ Operational Intelligence Centre (CASSIDIAN)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

19) ☐ Cyber threat detection (ECO)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

10) ACDC malware analysis tools will make 7 solutions available to partners. Are any of the following technologies or similar tools being used in your country (please check D.2.3 - Annex 1)? NO

22) ☐ WebCheck (CyDef)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

23) ☐ SiteVet (CyDef)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

24) ☐ HoneyUnit (FKIE)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

25) ☐ PDF Scrutinizer (FKIE)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

26) ☐ HoneyclientDispatcher (FKIE)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

27) ☐ Skanna (INTECO)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

28) ☐ Initiative-S (ECO)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

A – Internet Service Providers

11) Does your law enable ISPs to detect infections and identify infected users?

☐ No - (see question 11.1)
X Yes – D.Lgs. 69/12 and LG Garante Privacy
http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1915485
(see questions 11.2 to 11.3)

11.1) Do ISPs in practice do so?

☐ No
X Yes - (see questions 11.2 to 11.3)

11.2) What kind of data is processed by ISPs in these detections and identifications?

ISPs implement only general preventive server-side measures (ex. Anti-spam measures), while others worldwide are gearing to provide specific services directly to their customers). No personal data are managed.

12.4) Are ISPs required to mention the existence of such detection/ identification mechanisms in their contract?

☐ No
☐ Yes - ___________________________________(please provide a concrete example)

11.3) Do they deploy monitoring sensors?

☐ No
X Yes – **If so, which aspects of this monitoring sensors make it data privacy compliant?**

Monitoring sensors as *Probes,* with limitation and strict rules about processing of personal data and confidential access too

B – National Computer Emergency Response Teams

12) Is there a national or research CERT established in your country?

X No
☐ Yes - ______________(CERT name)____________________(see questions 12.1 to 12.2)

12.1) Do they deploy monitoring sensors?

X No
☐ Yes – **If so, which aspects of this monitoring sensors make it data privacy compliant?**

CERT

There is a national law not yet implemented.

https://www.sicurezzanazionale.gov.it/sisr.nsf/documentazione/riferimenti-giuridici/normativa-di-riferimento/dpcm-24-gennai-2013.html

12.2) What kind of data is processed by CERTs in these detections?

Section 3 - Centralised Clearing Data House and National Support Centre

13) Are there private or public-private partnerships established in your country where data concerning malware infections is exchanged?

X No

☐Yes – How is data collected and what kind of data is shared among partners?

14) Are there other private or public-private partnerships dealing with other aspects of cybersecurity (besides malware infections data sharing)? Please explain how they operate.

There are only large ICT Security vendors and other private associations or universities. They publish reports about security and malware, but no personal data analysis.

15) In which circumstances are IP-addresses, whether dynamic or static, considered as personal data in your country?

IP-addresses are considered as personal data

http://www.garanteprivacy.it/documents/10160/10704/1487717

16) **For how long are ISPs required to retain data in the terms of article 6 of Directive 2006/24/EC (Data Retention Directive)[188]?**

[188] Article 6 - Periods of retention

24 months (D.Lgs. 196/03 Section 132)
http://www.garanteprivacy.it/documents/10160/2012405/DataProtectionCode-2003.pdf

17) Are there circumstances in which the monitoring of communications by ISPs will not be considered an offence or a violation of privacy?

☐ No
X Yes - Compulsory for judicial authorities
http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1336877

18) Are ISPs allowed to share data of infections with other service providers?
X No
☐ Yes – if so, is this limited to a certain type of data? ____________________________

19) Are ISPs allowed to directly communicate to a customer identified as victim or author of an infection?

☐ No
X Yes, in some circumstances– LG Garante Privacy in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali
http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1915485

20) Are ISPs required to communicate detections/identifications to law enforcement agencies or other public authorities?

☐ No
X Yes – as above

21) Are CERTs allowed to share data of infections with actors others than law enforcement?

X No
☐ Yes – if so, is this limited to a certain type of data? ____________________________

22) Are CERTs allowed to directly communicate to an user identified as victim or author of an infection?

X No
☐ Yes - ____

Section 4 - End customer tools

Member States shall ensure that the categories of data specified in Article 5 are retained for periods of not less than six months and not more than two years from the date of the communication.

Concerning the practice of malware cleaning software in your country:

23) How do they assign liability for damages caused to customers and other users (non-customers)?

Decreto Legislativo 196/03 – Codice Trattamento Dati Personali http://www.garanteprivacy.it/documents/10160/2012405/DataProtectionCode-2003.pdf

L.48/08 (Ratifica Convenzione del Consiglio d'Europa - criminalita' informatica, Budapest 2001)

http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2008;48

24) How do they ask, record and store user's consent?

Not known or not clearly defined.

Section 5 – Additional information

25) Is there any additional information you would like to add that could help us with the analysis or any legal challenge that has not been addressed?

End of questionnaire

7.5 Portugal

Section 1 - Overview

This section calls for the major national instruments with regards to data privacy and cybercrime.

1) **Which law(s) has/have implemented Directive 95/46 (Data Protection Directive) in your jurisdiction?**

Law 67/98, of the 26th October
(http://dre.pt/pdf1sdip/1998/10/247A00/55365546.pdf)

2) **Which law(s) has/have implemented Directive 2002/58 (e-Privacy Directive) in your jurisdiction?**

- Law 41/2004, of the 18th August
(http://dre.pt/pdf1sdip/2004/08/194A00/52415245.pdf)

-Law 46/2012, of the 29th August (modifies articles 1, 2, 3, 5, 6, 7, 8, 14 and 15 of the Law 41/2004
(https://dre.pt/pdf1sdip/2012/08/16700/0481304826.pdf)

3) **Which law(s) has/have implemented the Council of Europe Convention – 185 on Cybercrime (Budapest Convention) in your jurisdiction?**

Law 109/2009, of the 15th June
(http://www.cnpd.pt/bin/legis/nacional/LEI109_2009_CIBERCRIME.pdf)

4) **Is there specific national legislation criminalising botnets?**

☐ No
☒ Yes – Article 6,par. 2 of the Law 109/2009

5) **Has your country implemented the exceptions provided by article 13(1) of Directive 95/46?**[189]

[189] Article 13 - Exemptions and restrictions
1. Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6 (1), 10, 11 (1), 12 and 21 when such a restriction constitutes a necessary measures to safeguard:
(a) national security;
(b) defence;

☐ No
☒ Yes – it is addressed in paragraph 7 or the article 4 of the Law 67/98 that admits the possibility of exceptions in data treatment motivated by public security, national defence and the State's security, as long as these exceptions are provided for in specific legislation or in international treaties of which Portugal is part.

6) **Has your country implemented the exceptions provided by article 15(1) of Directive 2002/58[190]?**

☐ No
☒ Yes - it is addressed in paragraph 4 of the Law 41/2004 that admits exceptions to the application of the law that are deemed necessary to the protection of public security, defence, the State's security and the prevention, investigation and repression of penal infractions and that are provided for in specific legislation.

7) **Which actors are involved in the prevention and detection of cybercrime in your country? Please describe their roles and cooperation with law enforcement.**

ISP or whoever has control of the data may be forced by the judicial authority or by the criminal police to preserve that data. ISP or whoever has control of the data must notify the judicial authority or the criminal police of the identity of other ISP involved in the communication through which the communication.

Whoever has control over the data necessary to provide evidence may be forced by the judicial authority to communicate it in the judicial procedure or to allow access to the computer system in which that data is stored.

8) **How does your law address the cooperation of ISPs in criminal investigation?**

See answer to question 7)

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

[190] Article 15 - Application of certain provisions of Directive 95/46/EC
1. Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union.

Section 2 - Monitoring Sensors and Malware Analysis Tools

9) ACDC sensors and detection tools will make 19 solutions available to partners. Are any of the following technologies or similar tools being used in your country (please check D.2.3 - Annex 1)?

1) ☒ Wildfire (LSEC) (similar)
By ☒ ISPS, ☐ webmasters, ☐ hosts, ☒ CERTs, ☐ Law enforcement, ☐ end-users

2) ☐ Spamtrap and low interaction honeypot(s) multipurpose appliance (CARNet)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

3) ☐ Passive DNS replication appliance (CARNet)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

4) ☒ Mediation server for sensors and Near real-time drive by download component (CARNet) (similar)
By ☒ ISPS, ☐ webmasters, ☐ hosts, ☒ CERTs, ☐ Law enforcement, ☐ end-users

5) ☐ HoneyNetRO (CERT-RO)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

6) ☒ Spam Analysis Tool (CERT-RO) (similar)
By ☒ ISPS, ☐ webmasters, ☐ hosts, ☒ CERTs, ☐ Law enforcement, ☐ end-users

7) ☐ Fortigate (CERT-RO)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

8) ☐ SPAM-BOT detection (TID)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

9) ☐ DNS-based BOT detection (TID)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

10) ☐ Smart BOT Detector (TID)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

11) ☐ SDN Malware Detector (TID)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

12) ☐ MonitoringHub and Accounting Manager (XLAB)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

13) ☐ Suricata Engine (XLAB)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

14) ☐ KB-IDS for Android (XLAB
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

15) ☐ AHPS (ATOS)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

16) ☐ Montimage Monitoring Tool (MI)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

17) ☐ Honeynet Network (TI)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

18) ☐ Operational Intelligence Centre (CASSIDIAN)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

19) ☐ Cyber threat detection (ECO)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

10) ACDC malware analysis tools will make 7 solutions available to partners. Are any of the following technologies or similar tools being used in your country (please check D.2.3 - Annex 1)?

20) ☒ WebCheck (CyDef) (similar)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☒ CERTs, ☐ Law enforcement, ☐ end-users

21) ☐ SiteVet (CyDef)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

22) ☐ HoneyUnit (FKIE)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

23) ☒ PDF Scrutinizer (FKIE) (similar)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☒ CERTs, ☐ Law enforcement, ☐ end-users

24) ☐ HoneyclientDispatcher (FKIE)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

25) ☐ Skanna (INTECO)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

26) ☐ Initiative-S (ECO)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

A – Internet Service Providers

11) Does your law enable ISPs to detect infections and identify infected users?

☐ No - (see question 11.1)
☐ Yes –_________________________________(see questions 11.2 to 11.3)
We are not sure of this information, nor is our Telecom Regulator.

11.1) Do ISPs in practice do so?

☐ No
☐ Yes - (see questions 11.2 to 11.3)
We don’t have access to this information, nor does our Telecom Regulator.

11.2) What kind of data is processed by ISPs in these detections and identifications?

We don't have access to this information, nor does our Telecom Regulator.

12.4) Are ISPs required to mention the existence of such detection/ identification mechanisms in their contract?

☐ No
☐ Yes - ____(please provide a concrete example)

11.3) Do they deploy monitoring sensors?

☐ No
☐ Yes – **If so, which aspects of this monitoring sensors make it data privacy compliant?**

We don't have access to this information, nor does our Telecom Regulator.

B – National Computer Emergency Response Teams

12) Is there a national or research CERT established in your country?

☐ No
☒ Yes – CERT.PT ____________________(see questions 12.1 to 12.2)

12.1) Do they deploy monitoring sensors?

☐ No
☒ Yes – **If so, which aspects of this monitoring sensors make it data privacy compliant?**

Monitor only their own networks (Research and Academic Network), which is a private network regulated by an AUP (Acceptable Use Policy) and a contract with the connected institutions.

12.2) What kind of data is processed by CERTs in these detections?

IP addresses, Port numbers, timestamps and in some cases URLs

Section 3 - Centralised Clearing Data House and National Support Centre

13) Are there private or public-private partnerships established in your country where data concerning malware infections is exchanged?

☐ No
☒ Yes – How is data collected and what kind of data is shared among partners?

There is implemented a network of CSIRTs (coordinated by CERT.PT), where information about compromised systems is shared with the CSIRTs responsible for those systems. This information is part public, part provided by security partners to CERT.PT

Data is shared on a need to now basis (an CSIRT only receives information of systems within their constituency), on a weekly basis, using privileged contacts and a specific data exchange format.

14) Are there other private or public-private partnerships dealing with other aspects of cybersecurity (besides malware infections data sharing)? Please explain how they operate.

Yes. The same network also works on Incident Handling and other minor and operational projects. It is also starting to work on the implementation of a sensor network in Portuguese Cyberspace.

15) In which circumstances are IP-addresses, whether dynamic or static, considered as personal data in your country?

If it is possible to identify the person(s) using that IP address, than it is considered personal data.

16) **For how long are ISPs required to retain data in the terms of article 6 of Directive 2006/24/EC (Data Retention Directive)[191]?**

Data must be preserved for one year, starting on the date of the conclusion of the communication.____

17) Are there circumstances in which the monitoring of communications by ISPs will not be considered an offence or a violation of privacy?

☒ No
☐ Yes - ____

[191] Article 6 - Periods of retention
Member States shall ensure that the categories of data specified in Article 5 are retained for periods of not less than six months and not more than two years from the date of the communication.

18) **Are ISPs allowed to share data of infections with other service providers?**

☐ No
☐ Yes – if so, is this limited to a certain type of data? ____________________________
We are not sure of this information, nor is our Telecom Regulator.

19) **Are ISPs allowed to directly communicate to a customer identified as victim or author of an infection?**

☐ No
☐ Yes - _ ____
We are not sure of this information, nor is our Telecom Regulator.

20) **Are ISPs required to communicate detections/identifications to law enforcement agencies or other public authorities?**

☒ No
☐ Yes -_

21) **Are CERTs allowed to share data of infections with actors others than law enforcement?**

☐ No
☒ Yes – if so, is this limited to a certain type of data? _Non private data ____________________________

22) **Are CERTs allowed to directly communicate to an user identified as victim or author of an infection?**

☐ No
☐ Yes____
We are not sure of this information.

Section 4 - End customer tools

Concerning the practice of malware cleaning software in your country:

23) **How do they assign liability for damages caused to customers and other users (non-customers)?**

We don't have specific legislation for this purpose. The client accepts the risk of damage by the tool (usually defined in the EULA – End-user license agreement) and the provider is not liable for the damages caused.

24) How do they ask, record and store user's consent?

Generally through the software EULA. The client has to accept the EULA before he can install (or run) the software.

Section 5 – Additional information

25) Is there any additional information you would like to add that could help us with the analysis or any legal challenge that has not been addressed?

Most of the questions that we were not able to answer were because we could not get the input on those issues with the Data Protection Commission in Portugal.

We feel that this might be an issue that might affect this whole project viability and should be formally and transversally assessed throughout all the member countries. We think we should have formal input on the Data Privacy Legislation interferences with the whole framework - sensors, clearing house, information sharing and tools dissemination.

End of questionnaire

7.6 Romania

Section 1 - Overview

This section calls for the major national instruments with regards to data privacy and cybercrime.

1) **Which law(s) has/have implemented Directive 95/46 (Data Protection Directive) in your jurisdiction?**

Law no.677/2001

http://www.dataprotection.ro/index.jsp?page=legislatie_primara&lang=en

http://ec.europa.eu/justice/policies/privacy/docs/implementation/ro_law_677_2001_en_unofficial.pdf

2) **Which law(s) has/have implemented Directive 2002/58 (e-Privacy Directive) in your jurisdiction?**

LAW no.506/2004
http://www.dataprotection.ro/servlet/ViewDocument?id=173

Law no.140/2012 for approval with amendments of the Government Emergency Ordinance no. 111/2011 regarding electronic communications
http://www.ancom.org.ro/en/uploads/links_files/OUG_2011_111_en.pdf
Art. 8,(2), g); Art. 51, (6); Art.60, (11), b); Art.69, alin.(6);
Final dispositions, list of EU Directives implemented - Directive (2009)136.

3) **Which law(s) has/have implemented the Council of Europe Convention – 185 on Cybercrime (Budapest Convention) in your jurisdiction?**

Law no.161/2003

http://diicot.ro/index.php/legislatie

4) **Is there specific national legislation criminalising botnets?**

☒ No
☐ Yes - ____

5) **Has your country implemented the exceptions provided by article 13(1) of Directive 95/46?**[192]

☐ No
☒ Yes – it is addressed in

Law no.677/2001, art.2, (5), (7), (8)
http://www.dataprotection.ro/index.jsp?page=legislatie_primara&lang=en
Law no.682/2001, art.2
http://www.dataprotection.ro/index.jsp?page=legislatie_primara&lang=en
Law no.506/2004, art.1 (4)
http://www.dataprotection.ro/servlet/ViewDocument?id=173

6) **Has your country implemented the exceptions provided by article 15(1) of Directive 2002/58[193]?**

☐ No
☒ Yes - it is addressed in
Law no.238/2009
Law no. 82/2012 (DATA RETENTION)

7) **Which actors are involved in the prevention and detection of cybercrime in your country? Please describe their roles and cooperation with law enforcement.**

Art. 36, Law no.161/2003, Title III on preventing and fighting cyber-crime
In order to ensure the security of the computer systems and the protection of the personal data, the authorities and public institutions with competence in the domain, the service providers, the non-governmental organisations and other representatives of the civil society carry out common activities and programmes for the prevention of cyber-crime.
Authorities and public institutions with competence: Ministry of Justice, Ministry of Domestic Affairs, Ministry of Communications and Information Technology, Romanian Intelligence Service, Romanian Foreign Intelligence Service. Government Decision 494/2011 establishes CERT-RO, along the above mentioned structures, as an institution with competence involved in the prevention and detection of cybercrime.

[192] Article 13 - Exemptions and restrictions
1. Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6 (1), 10, 11 (1), 12 and 21 when such a restriction constitutes a necessary measures to safeguard:
(a) national security;
(b) defence;
(c) public security;
(d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;
(e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;
(f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);
(g) the protection of the data subject or of the rights and freedoms of others.

[193] Article 15 - Application of certain provisions of Directive 95/46/EC
1. Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union.

8) How does your law address the cooperation of ISPs in criminal investigation?

Law no. 82/2012 (DATA RETENTION)
Art. 3, (2); Art. 18, (1)
According to art. 3 (2) from Law no. 82/2012 (Data Retention), ISPs are required to preserve the retained data for 6 months from the date of the communication. Moreover, judicial police investigation bodies have the right to request the data retained under this law, but only with the consent of the prosecutor who supervises or conducts prosecution or competent prosecutor in accordance with the procedure of commissioning tracking of persons and with the consent of the competent judge.

Criminal Procedure Code of Romania
Art. 97
http://www.anp.gov.ro/documents/10180/57727/Codul+de+Procedur%C4%83%20Penal%C4%83.pdf
According to art. 97 from Criminal Procedure Code of Romania, ISPs are required to provide to the criminal prosecution body or the court, at their request, any object, document or information which can serve as a proof (means of sample).

Section 2 - Monitoring Sensors and Malware Analysis Tools

9) ACDC sensors and detection tools will make 19 solutions available to partners. Are any of the following technologies or similar tools being used in your country (please check D.2.3 - Annex 1)?

1) ☐ Wildfire (LSEC)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

2) ☐ Spamtrap and low interaction honeypot(s) multipurpose appliance (CARNet)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

3) ☐ Passive DNS replication appliance (CARNet)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

4) ☐ Mediation server for sensors and Near real-time drive by download component (CARNet)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

5) ☒ HoneyNetRO (CERT-RO)
By ☒ ISPS, ☐ webmasters, ☐ hosts, ☒ CERTs, ☐ Law enforcement, ☐ end-users

6) ☒ Spam Analysis Tool (CERT-RO)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☒ CERTs, ☒ Law enforcement, ☐ end-users

7) ☒ Fortigate (CERT-RO)
By ☒ ISPS, ☒ webmasters, ☐ hosts, ☒ CERTs, ☒ Law enforcement, ☐ end-users

8) ☐ SPAM-BOT detection (TID)

By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

9) ☐ DNS-based BOT detection (TID)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

10) ☐ Smart BOT Detector (TID)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

11) ☐ SDN Malware Detector (TID)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

12) ☐ MonitoringHub and Accounting Manager (XLAB)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

13) ☐ Suricata Engine (XLAB)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

14) ☐ KB-IDS for Android (XLAB
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

15) ☐ AHPS (ATOS)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

16) ☐ Montimage Monitoring Tool (MI)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

17) ☐ Honeynet Network (TI)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

18) ☐ Operational Intelligence Centre (CASSIDIAN)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

19) ☐ Cyber threat detection (ECO)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

10) ACDC malware analysis tools will make 7 solutions available to partners. Are any of the following technologies or similar tools being used in your country (please check D.2.3 - Annex 1)?

20) ☐ WebCheck (CyDef)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

21) ☐ SiteVet (CyDef)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

22) ☐ HoneyUnit (FKIE)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

23) ☐ PDF Scrutinizer (FKIE)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

24) ☐ HoneyclientDispatcher (FKIE)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

25) ☐ Skanna (INTECO)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

26) ☐ Initiative-S (ECO)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

A – Internet Service Providers

11) Does your law enable ISPs to detect infections and identify infected users?

☐ No - (see question 11.1)
☒ Yes - According to Decision no.512/2013 of the President of Romanian National Regulatory Authority (ANCOM), applicable from 1 October 2013, the ISPs are empowered, but not forced, to establish adequate measures to protect its network against malicious codes infections and DDOS.(see questions 11.2 to 11.3)

11.1) Do ISPs in practice do so?

☒ No
☐ Yes - (see questions 11.2 to 11.3)

11.2) What kind of data is processed by ISPs in these detections and identifications?

12.4) Are ISPs required to mention the existence of such detection/ identification mechanisms in their contract?

☒ No
☐ Yes - ________________________________(please provide a concrete example)

11.3) Do they deploy monitoring sensors?

☐ No
☒ Yes – **If so, which aspects of these monitoring sensors make it data privacy compliant?**

Honeypots; icmp (ping/tracert); event handlers: snmp-get; graphs: rrd-tool, mrtg.

B – National Computer Emergency Response Teams

12) Is there a national or research CERT established in your country?

☐ No
☒ Yes – Romanian National Computer Security Incident Response Team – CERT-RO (see questions 12.1 to 12.2). In Romania there is also an governmental CERT team (CORIS-STS) and an academic CERT team (ROCSIRT).

12.1) Do they deploy monitoring sensors?

☐ No

☒ Yes – **If so, which aspects of this monitoring sensors make it data privacy compliant?**

CERTs deploy honeypot type sensors. This type of sensors does not interact with the internal network (no privacy issues here) and only collects source (IPs) and type of attack. The data transmitted by the computers in the network the honeypot sensor resides, and their IP addresses, are unknown to the sensor and do not interact at all.

12.2) What kind of data is processed by CERTs in these detections?

The honeypot sensors collect information about the source of the attack (IPs) and type of attack (the port it aims, type of scanning and other technical details that could describe the type of attack).

Section 3 - Centralised Clearing Data House and National Support Centre

13) Are there private or public-private partnerships established in your country where data concerning malware infections is exchanged?

☐ No

☒ Yes – How is data collected and what kind of data is shared among partners?

In CERT-RO case, malware samples are collected from the affected parties only with their consent. Also any kind of details regarding malware infections is collected with the consent of the affected entity.

So if the affected entity agrees, malware samples can be collected and sent to third parties for further analysis.

14) Are there other private or public-private partnerships dealing with other

Yes. CERT-RO, along with other public structures in RO, has different kind of public-private partnerships, related to cyber-security, with third parties:

- With security companies – related to technology promotion and awareness rising among population.
- With companies that have detection mechanisms (Shadowserver, Team Cymru, Google etc.) – for receiving periodic feeds about IPs in RO detected with malicious in Internet (botnets).
- With financial institutions – regarding the mutual exchange of information in case of cyber-security incidents.
- With other national CERT structures.

15) In which circumstances are IP-addresses, whether dynamic or static, considered as personal data in your country?

According to Law 677/2001, art.3, a)*," personal data: - any information referring to an identified or identifiable person; an identifiable person is a person that can be identified, directly or indirectly, particularly with reference to an identification number or to one or more specific factors of his physical, physiological, psychological, economic, cultural or social identity;* The strict case regarding the status of IP addresses is not specifically referred in our legislation. In this case, we can say that dynamically allocated IPs, without any other information (like timestamp for ex.), cannot be considered personal data as long as they cannot identify a real person. When it comes to static IPs, they can be considered personal data, according to a specific situation.

16) **For how long are ISPs required to retain data in the terms of article 6 of Directive 2006/24/EC (Data Retention Directive)[194]?**

Law no.82/2012, Chapter II Data retention - art. 3 point 2 "The retention period is of six months from the date of communication".

17) Are there circumstances in which the monitoring of communications by ISPs will not be considered an offence or a violation of privacy?

☐ No
☒ Yes – According to data retention related law, ISPs are enforced to monitor the metadata of the communication (source, destination, timestamp etc.) without the actual

[194] Article 6 - Periods of retention
Member States shall ensure that the categories of data specified in Article 5 are retained for periods of not less than six months and not more than two years from the date of the communication.

content of the communication. The content can only be monitored with a mandate from a prosecutor.

18) Are ISPs allowed to share data of infections with other service providers?

☐ No
☒ Yes – if so, is this limited to a certain type of data? As long as the data shared does not concern personal data of the clients of the ISP, the sharing can be done and is also encouraged in order to limit the effects of some cyber-security incidents.

19) Are ISPs allowed to directly communicate to a customer identified as victim or author of an infection?

☐ No

☒ Yes – The national law specifically asks them to notify clients or other affected parties. According to Decision no.512/2013 of the President of Romanian National Regulatory Authority (ANCOM), applicable from 1 October 2013, the ISPs must establish incidents communications plans for notifying clients or other affected parties.

20) Are ISPs required to communicate detections/identifications to law enforcement agencies or other public authorities?

☒ No – ISP are not required to communicate infections detected, but other types of incidents.
☐ Yes

21) Are CERTs allowed to share data of infections with actors others than law enforcement?

☐ No
☒ Yes – if so, is this limited to a certain type of data? Data can be exchanged with parties that are responsible for incident handling or remediation. Statistics upon infections can be shared with a broader audience.

22) Are CERTs allowed to directly communicate to an user identified as victim or author of an infection?

☐ No
☒ Yes – It is not prohibited by any law but CERTs rarely get to the real victim or to the author of an infection.

Section 4 - End customer tools

Concerning the practice of malware cleaning software in your country:

23) How do they assign liability for damages caused to customers and other users (non-customers)?

The software producers explicitly reject liability for any sort of damages (incidental or otherwise) caused by the use or functioning of the products. Also see the new Romanian civil code, articles 1350 and following, regarding exoneration clauses in contracts.

24) How do they ask, record and store user's consent?

Product installation is conditioned upon acceptance of the EULA. Consent to collect, transmit and store information relating to product functionality (such as samples of suspicious executable) is always asked explicitly and the choice made is stored locally. Upon uninstall, any locally-stored data is deleted.

Section 5 – Additional information

25) Is there any additional information you would like to add that could help us with the analysis or any legal challenge that has not been addressed?

End of questionnaire

7.7 Slovenia

Section 1 - Overview

This section calls for the major national instruments with regards to data privacy and cybercrime.

1) Which law(s) has/have implemented Directive 95/46 (Data Protection Directive) in your jurisdiction?

Information Commissioner Act*
https://www.ip-rs.si/index.php?id=325
regarding the establishment of the Office of the Commissioner (Article 1)
*This translation was prepared by the office of the Commissioner for access to public information. Only the official publication of the Act in Slovene language, as published and promulgated in the Official Gazette of the Republic of Slovenia, is authentic.

Personal Data Protection Act
http://www.mp.gov.si/fileadmin/mp.gov.si/pageuploads/mp.gov.si/zakonodaja/angleski_prevodi_zakonov/071029_personal_data_protection_act_RS.pdf
regarding the processing of personal data (Chapter 1/II), protection of individuals (Chapter 2/II), security of personal data (Chapter 3/II), notification of filing systems (Chapter 4/II), rights of the individual (Part III), inspection supervision (Chapter 3/IV), transfer of personal data (Part V), sectoral arrangements (Part VI) and penal provisions (Part VII)

Minor Offences Act
https://www.ip-rs.si/zakonodaja/zakon-o-prekrskih/
regarding the obligation of the data controller to supply data to institutions (Article 45) and the minor offence authority's filing system (Article 203)

Patient Rights Act
https://www.ip-rs.si/zakonodaja/zakon-o-pacientovih-pravicah/
regarding data protection (Article 44)

Electronic Communications Act
https://www.ip-rs.si/zakonodaja/zakon-o-elektronskih-komunikacijah-zekom-1/
regarding the Agency's filing system (Article 200), the collection and giving of data and information (Article 201), the cooperation with the Information Commissioner (Article 215) also regarding control (Articles in XVI) and penal provisions (Article 233 – Article 236). https://www.ip-rs.si/fileadmin/user_upload/Pdf/zakoni/ZEKom_ANG.pdf

2) Which law(s) has/have implemented Directive 2002/58 (e-Privacy Directive) in your jurisdiction?

Electronic Communications Act
https://www.ip-rs.si/zakonodaja/zakon-o-elektronskih-komunikacijah-zekom-1/
regarding the processing of personal data and the security of electronic communications (Chapter XII)

3) **Which law(s) has/have implemented the Council of Europe Convention – 185 on Cybercrime (Budapest Convention) in your jurisdiction?**

Criminal Code
http://www.dz-rs.si/wps/portal/Home/deloDZ/zakonodaja/izbranZakonAkt?uid=C12563A400338836C1257435005A1F1C&db=spr_zak&mandat=VIregarding regarding the mishandling of personal information (Article 143 p.2), violation of author's rights (Article 147-149), offences related to child pornography (Article 176), attack on the information system (Article 221) and invasion of a business information system (Article 237)

Criminal Procedure Act
http://www.uradni-list.si/1/objava.jsp?urlid=20068&stevilka=296
regarding secret surveillance (Article 149.a), obtaining of data on traffic in the electronic communications networks (Article 149.b), control of communications or computer system (Article 150), cooperation with other countries (Article 160.b), search of premises and seizure of objects (Article 214-224), international assistance (Article 514-520) and extradition (Article 521-537)

Electronic Communications Act
https://www.ip-rs.si/zakonodaja/zakon-o-elektronskih-komunikacijah-zekom-1/
regarding the lawful interception of the communications (Article 160), storage of personal data (Chapter XIII) and penal provisions (Chapter XVIII)

4) **Is there specific national legislation criminalising botnets?**

☒ No
☐ Yes - ____

5) **Has your country implemented the exceptions provided by article 13(1) of Directive 95/46?**[195]

☐ No
☒ Yes – it is addressed in Article 36 of the Personal Data Protection Act

6) **Has your country implemented the exceptions provided by article 15(1) of Directive 2002/58**[196]**?**

[195] Article 13 - Exemptions and restrictions
1. Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6 (1), 10, 11 (1), 12 and 21 when such a restriction constitutes a necessary measures to safeguard:
(a) national security;
(b) defence;
(c) public security;
(d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;
(e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;
(f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);
(g) the protection of the data subject or of the rights and freedoms of others.

☐ No
☒ Yes - it is addressed in Article 36 of the Personal Data Protection Act

7) Which actors are involved in the prevention and detection of cybercrime in your country? Please describe their roles and cooperation with law enforcement.

Police/ National investigation office/ Criminal investigation police office

ISPs - They inform law enforcement about detected threats.

CERT - They inform law enforcement about detected threats.

8) How does your law address the cooperation of ISPs in criminal investigation?

There is nothing specifically written regarding this subject.

[196] Article 15 - Application of certain provisions of Directive 95/46/EC
1. Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union.

Section 2 - Monitoring Sensors and Malware Analysis Tools

9) **ACDC sensors and detection tools will make 19 solutions available to partners. Are any of the following technologies or similar tools being used in your country (please check D.2.3 - Annex 1)?**
Some are definitely used by ISPs, but they do not wish to classify which ones. By machine they have classical fw, dpi and specialised engines and sw packages.

1) ☐ Wildfire (LSEC)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

2) ☐ Spamtrap and low interaction honeypot(s) multipurpose appliance (CARNet)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

3) ☐ Passive DNS replication appliance (CARNet)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

4) ☐ Mediation server for sensors and Near real-time drive by download component (CARNet)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

5) ☐ HoneyNetRO (CERT-RO)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

6) ☐ Spam Analysis Tool (CERT-RO)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

7) ☐ Fortigate (CERT-RO)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

8) ☐ SPAM-BOT detection (TID)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

9) ☐ DNS-based BOT detection (TID)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

10) ☐ Smart BOT Detector (TID)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

11) ☐ SDN Malware Detector (TID)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

12) ☐ MonitoringHub and Accounting Manager (XLAB)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

13) ☐ Suricata Engine (XLAB)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

14) ☐ KB-IDS for Android (XLAB)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

15) ☐ AHPS (ATOS)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

16) ☐ Montimage Monitoring Tool (MI)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

17) ☐ Honeynet Network (TI)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

18) ☐ Operational Intelligence Centre (CASSIDIAN)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

19) ☐ Cyber threat detection (ECO)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

10) ACDC malware analysis tools will make 7 solutions available to partners. Are any of the following technologies or similar tools being used in your country (please check D.2.3 - Annex 1)?

20) ☐ WebCheck (CyDef)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

21) ☐ SiteVet (CyDef)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

22) ☐ HoneyUnit (FKIE)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

23) ☐ PDF Scrutinizer (FKIE)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

24) ☐ HoneyclientDispatcher (FKIE)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

25) ☐ Skanna (INTECO)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

26) ☐ Initiative-S (ECO)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

A – Internet Service Providers

11) Does your law enable ISPs to detect infections and identify infected users?

☒ No
☐ Yes - ____(see questions 11.2 to 11.3)

11.1) Do ISPs in practice do so?

☐ No
☒ Yes – ISPs also do remote disinfect on site or true remote when requested. Special procedures are applied to business users, with multilayer security approach.

11.2) What kind of data is processed by ISPs in these detections and identifications?

Usually IP addressing scheme and protocol stack used during infection. Identification is dependent on the types of devices used and internal algorithms for detection

12.4) Are ISPs required to mention the existence of such detection/ identification mechanisms in their contract?

☐ No
☐ Yes - ___________________________________(please provide a concrete example)

11.3) Do they deploy monitoring sensors?

☐ No
☒ Yes – **If so, which aspects of this monitoring sensors make it data privacy compliant?**

Monitoring is deployed only at certain network parts, not at each user or groups of them. Price would be prohibitive. Data privacy is preserved strictly by prior announcement of data types gathered and providing this to Information Commissioner. It has full authority to monitor internal process activity procedures and make unannounced inspections to verify that / what is gathered is by the pre determined / announced book.

B – National Computer Emergency Response Teams

12) Is there a national or research CERT established in your country?

☐ No
☒ Yes – SI-CERT https://www.cert.si/en/

12.1) Do they deploy monitoring sensors?

☐ No
☐ Yes – **If so, which aspects of this monitoring sensors make it data privacy compliant?**

12.2) What kind of data is processed by CERTs in these detections?

Section 3 - Centralised Clearing Data House and National Support Centre

13) Are there private or public-private partnerships established in your country where data concerning malware infections is exchanged?

☐ No
☒ Yes – How is data collected and what kind of data is shared among partners?

14) Are there other private or public-private partnerships dealing with other aspects of cybersecurity (besides malware infections data sharing)? Please explain how they operate.

15) In which circumstances are IP-addresses, whether dynamic or static, considered as personal data in your country?

16) **For how long are ISPs required to retain data in the terms of article 6 of Directive 2006/24/EC (Data Retention Directive)[197]?**

Around 3 months, but may be up to 2 years. Depends also on the capabilities. Call records are retained only for 3 months.

17) Are there circumstances in which the monitoring of communications by ISPs will not be considered an offence or a violation of privacy?

☒ No
☐ Yes - ____

18) Are ISPs allowed to share data of infections with other service providers?
☒ No
☐ Yes – if so, is this limited to a certain type of data? ____________________________
Have no information of this. Yes conferences are held and articles posted, but there are no official procedures. Top IT guys do communicate and inform each other in cases of grave security risks and infection spreads.

19) Are ISPs allowed to directly communicate to a customer identified as victim or author of an infection?

☐ No
☒ Yes – This is done mainly in relations to the customer, no record of it when it comes to authors. Procedures involve the Criminal investigation police.

20) Are ISPs required to communicate detections/identifications to law enforcement agencies or other public authorities?

☐ No
☒ Yes - ____

[197] Article 6 - Periods of retention
Member States shall ensure that the categories of data specified in Article 5 are retained for periods of not less than six months and not more than two years from the date of the communication.

21) **Are CERTs allowed to share data of infections with actors others than law enforcement?**

☐ No
☐ Yes – if so, is this limited to a certain type of data? ___________________________

22) **Are CERTs allowed to directly communicate to a user identified as a victim or author of an infection?**

☐ No
☐ Yes - ____

Section 4 - End customer tools

Concerning the practice of malware cleaning software in your country:

23) **How do they assign liability for damages caused to customers and other users (non-customers)?**

24) **How do they ask, record and store user's consent?**

By a business contract.

Section 5 – Additional information

25) **Is there any additional information you would like to add that could help us with the analysis or any legal challenge that has not been addressed?**

End of questionnaire

7.8 Spain

Section 1 - Overview

This section calls for the major national instruments with regards to data privacy and cybercrime.

1) **Which law(s) has/have implemented Directive 95/46 (Data Protection Directive) in your jurisdiction?**

http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/estatal/common/pdfs/LOPD_consolidada.pdf
ORGANIC LAW 15/1999 of 13 December on the Protection of Personal Data.
http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/estatal/common/pdfs/RD_1720_2007.pdf
RD approving the regulation of development of the law organic 15/1999 of 13 december data protection personal.

2) **Which law(s) has/have implemented Directive 2002/58 (e-Privacy Directive) in your jurisdiction?**

http://www.minetur.gob.es/telecomunicaciones/lssi/normativa/DocNormativa/1.%20Leyes/Ley32_2003.pdf
Law 32/2003 General Telecommunications.
http://www.minetur.gob.es/telecomunicaciones/lssi/normativa/DocNormativa/1.%20Leyes/Ley25_2007.pdf
Law 25/2007 of October 18 of conservation of data relating to commnunications electronic and public communications networks.
http://www.minetur.gob.es/telecomunicaciones/lssi/normativa/DocNormativa/1.%20Leyes/Ley34_2002.pdf

Law 34/2002 of July 11. Services Information Society and Electronic Commerce **Art 12 bis** Security Aspects

3) **Which law(s) has/have implemented the Council of Europe Convention – 185 on Cybercrime (Budapest Convention) in your jurisdiction?**

The substantive and procedural criminal content of the Budapest Convention was already contained in our legal system (Law 10/1995 of November 23 of Penal Code and Criminal Procedure Act)

Some adaptation on types of cybercrime and the criminal liability of legal persons is conducted by law 5/2010 of june 22 amending some articles of the Penal Code.

4) **Is there specific national legislation criminalising botnets?**

☒ No
☐ Yes - ____

5) **Has your country implemented the exceptions provided by article 13(1) of Directive 95/46?**[198]

☐ No
☒ Yes – it is addressed in ____________________________________

http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/estatal/common/pdfs/LOPD_consolidada.pdf

Organic Law 15/1999, **Arts. 22 , 23 y 24**

http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/estatal/common/pdfs/RD_1720_2007.pdf

RD 15/1999 , **Art. 4.c) y art. 10.2**

6) **Has your country implemented the exceptions provided by article 15(1) of Directive 2002/58**[199]**?**

☐ No
☒ Yes - it is addressed in question 2 (Law 32/2003 General Telecommunications and Law 25/2007 of October 18) and Circular 1/2013 of january of State Attorney General in http://www.fiscal.es/cs/Satellite?blobcol=urldata&blobheader=application%2Fpdf&blobheadername1=Content-disposition&blobheadervalue1=attachment%3B+filename%3D%27CIRCULAR+1-2013+INTERVENCIONES+TELEFONICAS.pdf%27&blobkey=id&blobtable=MungoBlobs&blobwhere=1246969707016&ssbinary=true

7) **Which actors are involved in the prevention and detection of cybercrime in your country? Please describe their roles and cooperation with law enforcement.**

- Authorities and public institutions with competence: Ministry of Justice, Ministry of Industry, Energy and Tourism and Ministry of Interior
- State Security Forces (Computer Crimes Unit of the Police and Crime Squad telematics Civil Guard)
- Law enforcement bodies
- Customs Surveillance officials
- CERTS (included INTECO-CERT)
- CNI (Intelligence Agency) and its CCN CERT

[198] Article
1. Membe
for in Articles 6 (1), 10, 11 (1), 12 and 21 when such a restriction constitutes a necessary measures to safeguard:
(a) national security;
(b) defence;
(c) public security;
(d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;
(e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;
(f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);
(g) the protection of the data subject or of the rights and freedoms of others.

[199] Article 15 - Application of certain provisions of Directive 95/46/EC
1. Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union.

8) **How does your law address the cooperation of ISPs in criminal investigation?**

Interception of comunications prior judicial authorization with the limits contained in the law:

Law 32/2003 General Telecommunications: arts **33, 34 y 35**

Circular 1/2013 of january of State Attorney General

Data retention:

Law 25/2007 of October 18 of conservation of data relating to commnunications electronic and public communications networks.

Capítulo II (arts 4 a 9)

Duty of cooperation of service providers with the competent bodies to **suspend the transmission, data hosting, access to telecommunications networks or the provision of any other equivalent service intermediation**. Law 34/2002 of July 11. Services Information Society and Electronic Commerce **Art 11.**

Section 2 - Monitoring Sensors and Malware Analysis Tools

9) **ACDC sensors and detection tools will make 19 solutions available to partners. Are any of the following technologies or similar tools being used in your country (please check D.2.3 - Annex 1)?**

1) ☐ Wildfire (LSEC)
By x ISPS, ☐ webmasters, ☐ hosts, x CERTs, ☐ Law enforcement, ☐ end-users

2) ☐ Spamtrap and low interaction honeypot(s) multipurpose appliance (CARNet)
By ☐ ISPS, ☐ webmasters, ☐ hosts, x CERTs, ☐ Law enforcement, ☐ end-users

3) ☐ Passive DNS replication appliance (CARNet)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

4) ☐ Mediation server for sensors and Near real-time drive by download component (CARNet)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

5) ☐ HoneyNetRO (CERT-RO)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

6) ☐ Spam Analysis Tool (CERT-RO)
By ☐ ISPS, ☐ webmasters, ☐ hosts, x CERTs, ☐ Law enforcement, ☐ end-users

7) ☐ Fortigate (CERT-RO)
By x ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

8) ☐ SPAM-BOT detection (TID)
By x ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

9) ☐ DNS-based BOT detection (TID)
By x ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

10) ☐ Smart BOT Detector (TID)

By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

11) ☐ SDN Malware Detector (TID)
By x ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

12) ☐ MonitoringHub and Accounting Manager (XLAB)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

13) ☐ Suricata Engine (XLAB)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

14) ☐ KB-IDS for Android (XLAB
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

15) ☐ AHPS (ATOS)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

16) ☐ Montimage Monitoring Tool (MI)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

17) ☐ Honeynet Network (TI)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

18) ☐ Operational Intelligence Centre (CASSIDIAN)
By ☐ ISPS, ☐ webmasters, ☐ hosts, x CERTs, ☐ Law enforcement, ☐ end-users

19) ☐ Cyber threat detection (ECO)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

10) ACDC malware analysis tools will make 7 solutions available to partners. Are any of the following technologies or similar tools being used in your country (please check D.2.3 - Annex 1)?

20) ☐ WebCheck (CyDef)
By ☐ ISPS, x webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

21) ☐ SiteVet (CyDef)
By x ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

22) ☐ HoneyUnit (FKIE)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

23) ☐ PDF Scrutinizer (FKIE)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

24) ☐ HoneyclientDispatcher (FKIE)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

25) ☐ Skanna (INTECO)
By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

26) ☐ Initiative-S (ECO)
By ☐ ISPS, ☐ webmasters, ☐ hosts, x CERTs, ☐ Law enforcement, ☐ end-users

A – Internet Service Providers

11) Does your law enable ISPs to detect infections and identify infected users?

☐ No - (see question 11.1)
X Yes -

Although not specifically stated in the legislation, in accordance with the Article 36 bis of the General Law of Telecommunications about its obligations to the integrity and security of networks and electronic communications services, operators usually provide such actions in their private contracts with users.

11.1) Do ISPs in practice do so?

☐ No
X Yes - When it affects the security of their networks and services and on the terms contained in a private contract with its customers.

11.2) What kind of data is processed by ISPs in these detections and identifications?

ISPs must provide this information.

12.4) Are ISPs required to mention the existence of such detection/ identification mechanisms in their contract?

☐ No
☐ Yes - __________________________________(please provide a concrete example)

11.3) Do they deploy monitoring sensors?

☐ No
☐ Yes – **If so, which aspects of this monitoring sensors make it data privacy compliant?**

Yes. ISPs must provide this information.

B – National Computer Emergency Response Teams

12) Is there a national or research CERT established in your country?

☐ No
X **Yes** - INTECO-CERT (see questions 12.1 to 12.2)

12.1) Do they deploy monitoring sensors?

☐ No
X Yes – If so, which aspects of this monitoring sensors make it data privacy compliant?

In compliance with Spanish legislation on data protection, data files are notified to the Spanish Agency for Data Protection for which INTECO applies security measures required by law.

12.2) What kind of data is processed by CERTs in these detections?

IP addresses (applying measures explained in question before).

Domain names, Malware information, type of attacks information, Spam information captured by spamtraps, and other information with no privacy issues.

Section 3 - Centralised Clearing Data House and National Support Centre

13) Are there private or public-private partnerships established in your country where data concerning malware infections is exchanged?

☐ No
X **Yes** – How is data collected and what kind of data is shared among partners?

CERTs exchange information with other CERTs and security teams (public and private) through collaborative working groups.

14) Are there other private or public-private partnerships dealing with other aspects of cybersecurity (besides malware infections data sharing)? Please explain how they operate.

Yes, for example:

- Madrid chapter of ISMS forum (https://www.ismsforum.es/)

15) In which circumstances are IP-addresses, whether dynamic or static, considered as personal data in your country?

IP-addresses are considered as personal data under any circumstance (dynamic or static) .

Report of the Spanish Agency for Data Protection No. 327/2003

16) **For how long are ISPs required to retain data in the terms of article 6 of Directive 2006/24/EC (Data Retention Directive)[200]?**

12 months since the communication is done (art 5 Law 25/2007 of October 18 of conservation of data relating to commnunications electronic and public communications networks)

17) Are there circumstances in which the monitoring of communications by ISPs will not be considered an offence or a violation of privacy?

☐ No
X Yes – See answer to question no 8.

18) Are ISPs allowed to share data of infections with other service providers?
X No
☐ Yes – if so, is this limited to a certain type of data? ____________________________

No, whether it is personal or private. They have to preserve the right of privacy of communications.

19) Are ISPs allowed to directly communicate to a customer identified as victim or author of an infection?

☐ No
x **Yes -** ____

See answer to question 11.

20) Are ISPs required to communicate detections/identifications to law enforcement agencies or other public authorities?

X No. There is a soft law developed but not fully effective

[200] Article 6 - Periods of retention
Member States shall ensure that the categories of data specified in Article 5 are retained for periods of not less than six months and not more than two years from the date of the communication.

☐ Yes -

21) Are CERTs allowed to share data of infections with actors others than law enforcement?

☐ No
☐ Yes – if so, is this limited to a certain type of data? ____________________________

The law does not cover this aspect explicitly, but CERTs share information with affected entities always complying with the Data Protection Act.

22) Are CERTs allowed to directly communicate to an user identified as victim or author of an infection?

☐ No
☐ Yes - ____

CERTs cannot identify end users infected, only the ISP responsible/owner of the IP address.

Section 4 - End customer tools

Concerning the practice of malware cleaning software in your country:

23) How do they assign liability for damages caused to customers and other users (non-customers)?

Under the terms of the cleaning software license.

24) How do they ask, record and store user's consent?

Under the terms of the cleaning software license. Requesting acceptance of that license, normally before executing the software.

Section 5 – Additional information

25) Is there any additional information you would like to add that could help us with the analysis or any legal challenge that has not been addressed?

End of questionnaire

7.9 The Netherlands

Section 1 - Overview

This section calls for the major national instruments with regards to data privacy and cybercrime.

1) **Which law(s) has/have implemented Directive 95/46 (Data Protection Directive) in your jurisdiction?**

Wet bescherming persoonsgegevens [Personal Data Protection Act], *Staatsblad* 2000, 302 [hereafter: Wbp]

(All Dutch laws are available at http://wetten.overheid.nl, both the current and the original version. The official publication in the Staatsblad (Official Journal) can also be found at http://zoek.officielebekendmakingen.nl.)

2) **Which law(s) has/have implemented Directive 2002/58 (e-Privacy Directive) in your jurisdiction?**

Wet van 22 april 2004 tot wijziging van de Telecommunicatiewet en enkele andere wetten in verband met de implementatie van een nieuw Europees geharmoniseerd regelgevingskader voor elektronische communicatienetwerken en -diensten en de nieuwe dienstenrichtlijn van de Commissie van de Europese Gemeenschappen [Law of 22 April 2004 changing the Telecommunications Act and some other Acts to implement a new European harmonised regulatory framework for electronic communications services and the new services Directive of the Commission of the European Communities], *Staatsblad* 2004, 189

NB The Directive has thus been implemented in the Telecommunications Act (particularly in Ch. 11 of the Act).

3) **Which law(s) has/have implemented the Council of Europe Convention – 185 on Cybercrime (Budapest Convention) in your jurisdiction?**

Ratification: Rijkswet van 1 juni 2006 tot goedkeuring van het op 23 november 2001 te Boedapest totstandgekomen Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken (Trb. 2002, 18) [Kingdom Law of 1 June 2006 approving the Convention on Cybercrime, *Staatsblad* 2006, 299.

Implementation: Wet computercriminaliteit II [Computer Crime II Act], *Staatsblad* 2006, 300.

NB Many provisions of the Convention were already implemented by earlier legislation, notably the Wet computercriminaliteit [Computercrime Act], *Staatsblad* 1993, 33.

4) Is there specific national legislation criminalising botnets?

☐ No
☐ Yes -
It depends on what you mean with "specific" and which aspects of botnets you mean. Criminal law does not criminalise things (such as botnets) but it criminalises acts (e.g., hacking or blocking access to a computer, or misuse of devices).
Many activities related to botnets are criminalised, e.g.

Creating a botnet:

- disseminating malware (art. 350a(3) Wetboek van Strafrecht [Sr, Criminal Code])
- hacking (art. 138ab Sr)
- data interference (art. 350a(1) Sr)

Using a botnet:

- hacking (art. 138ab Sr)
- denial of service attacks (art. 138b Sr)
- computer sabotage (art. 161sexies(1) Sr)
- misuse of devices (in the sense of art. 6 Cybercrime Convention) (art. 139d(2) and art. 161sexies(2) Sr)
- NB sending spam is not criminalised, but (under certain conditions) an administrative offence

5) Has your country implemented the exceptions provided by article 13(1) of Directive 95/46?[201]

☐ No
☒ Yes – most of these exceptions are mentioned in art. 2(2) and 2(3) Wbp. For criminal justice, data protection is regulated in the Wet politiegegevens [Police Data Act], Staatsblad 2007, 300, changed by Law of 6 October 2011, Staatsblad 2011, 490. For national security, there are some data protection provisions in the Wet op de inlichtingen- en veiligheidsdiensten 2002 [Intelligence and security services Act 2002], Staatsblad 2002, 148.

6) Has your country implemented the exceptions provided by article 15(1) of Directive 2002/58[202]?

[201] Article 13 - Exemptions and restrictions
1. Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6 (1), 10, 11 (1), 12 and 21 when such a restriction constitutes a necessary measures to safeguard:
(a) national security;
(b) defence;
(c) public security;
(d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;
(e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;
(f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);
(g) the protection of the data subject or of the rights and freedoms of others.

[202] Article 15 - Application of certain provisions of Directive 95/46/EC
1. Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this

☐ No

☒ Yes - it is addressed in

* art. 5 on confidentiality: inter alia art. 126m, 126t, 126zg Wetboek van Strafvordering [hereafter: Sv] [Code of Criminal Procedure], art. 25 Intelligence and security services Act 2002 (allowing wiretapping)

* art. 6 on traffic data: inter alia art. 126n, 126u, 126zh Code of Criminal Procedure, art. 28 Intelligence and security services Act 2002 (allowing production orders or requests for traffic data)

* data retention: art. 13.2a Telecommunicatiewet [Telecommunications Act] (requiring data retention)

7) **Which actors are involved in the prevention and detection of cybercrime in your country? Please describe their roles and cooperation with law enforcement.**

Law enforcement: police, Public Prosecutor

National CyberSecurity Center (NCSC): monitoring of security threats, provide information to law enforcement if they encounter something that is relevant for criminal investigation or prosecution.

National Forensics Institute (NFI) and private forensic companies (e.g. Fox-IT for digital investigations): forensic investigations at request of police or judiciary.

Private actors: companies (e.g. banks) taking preventative measures; Fox-IT conducting investigations for both government and private actors.

Public-Private Partnerships: Samen tegen Cybercrime [Together against Cybercrime], an initiative to share security-threat-related information between a wide range of actors; Electronic Commerce Platform (ECP.nl), which does awareness-raising campaigns.

8) **How does your law address the cooperation of ISPs in criminal investigation?**

ISPs have to cooperate with orders from law enforcement, on the basis of investigation powers (e.g. art. 126m, 126n, and 126ng Sv) and of cooperation obligations laid down in art. 13.2 and 13.2b of the Telecommunications Act. According to art. 13.1 Telecommunications Act, ISPs offering public electronic communication services have to ensure that their services are interceptable.

Although there may be some scope for ISPs to cooperate voluntarily with requests (not orders) from the police, the general understanding of the law is that if law enforcement wants information from ISPs (or any other party), they have to order this officially through a production order.

Section 2 - Monitoring Sensors and Malware Analysis Tools

9) **ACDC sensors and detection tools will make 19 solutions available to partners. Are any of the following technologies or similar tools being used in your country (please check D.2.3 - Annex 1)?**

paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union.

1) ☐ Wildfire (LSEC)

By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

2) ☐ Spamtrap and low interaction honeypot(s) multipurpose appliance (CARNet)

By ☒ ISPS, ☐ webmasters, ☐ hosts, ☒ CERTs, ☐ Law enforcement, ☐ end-users

3) ☐ Passive DNS replication appliance (CARNet)

By ☒ ISPS, ☐ webmasters, ☐ hosts,☒ CERTs, ☐ Law enforcement, ☐ end-users

4) ☐ Mediation server for sensors and Near real-time drive by download component (CARNet)

By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

5) ☐ HoneyNetRO (CERT-RO)

By ☒ ISPS, ☐ webmasters, ☐ hosts, ☒ CERTs, ☒ Law enforcement, ☐ end-users

6) ☐ Spam Analysis Tool (CERT-RO)

By ☒ ISPS, ☐ webmasters, ☐ hosts, ☒ CERTs, ☐ Law enforcement, ☐ end-users

7) ☐ Fortigate (CERT-RO)

By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

8) ☐ SPAM-BOT detection (TID)

By ☒ ISPS, ☐ webmasters, ☐ hosts, ☒ CERTs, ☐ Law enforcement, ☐ end-users

9) ☐ DNS-based BOT detection (TID)

By ☒ ISPS, ☐ webmasters, ☐ hosts, ☒ CERTs, ☐ Law enforcement, ☐ end-users

10) ☐ Smart BOT Detector (TID)

By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

11) ☐ SDN Malware Detector (TID)

By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

12) ☐ MonitoringHub and Accounting Manager (XLAB)

By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

13) ☐ Suricata Engine (XLAB)

By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

14) ☐ KB-IDS for Android (XLAB

By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

15) ☐ AHPS (ATOS)

By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

16) ☐ Montimage Monitoring Tool (MI)

By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

17) ☐ Honeynet Network (TI)

By ☒ ISPS, ☐ webmasters, ☐ hosts, ☒ CERTs, ☐ Law enforcement, ☐ end-users

18) ☐ Operational Intelligence Centre (CASSIDIAN)

By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

19) ☐ Cyber threat detection (ECO)

By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

10) ACDC malware analysis tools will make 7 solutions available to partners. Are any of the following technologies or similar tools being used in your country (please check D.2.3 - Annex 1)?

20) ☐ WebCheck (CyDef)

By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

21) ☐ SiteVet (CyDef)

By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

22) ☐ HoneyUnit (FKIE)

By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

23) ☐ PDF Scrutinizer (FKIE)

By ☒ ISPS, ☐ webmasters, ☐ hosts, ☒ CERTs, ☐ Law enforcement, ☐ end-users

24) ☐ HoneyclientDispatcher (FKIE)

By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

25) ☐ Skanna (INTECO)

By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

26) ☐ Initiative-S (ECO)

By ☐ ISPS, ☐ webmasters, ☐ hosts, ☐ CERTs, ☐ Law enforcement, ☐ end-users

A – Internet Service Providers

11) Does your law enable ISPs to detect infections and identify infected users?

☐ No - (see question 11.1)
☒ Yes

This is not a yes-or-no issue. The law does not specifically allow ISPs to detect infections, but neither does it explicitly prohibit ISPs from detecting infections of their customers. If detection of infections is possible by scanning traffic data without accessing content of communications, I think this would be allowed. If detection requires more infringing measures, it will depend on the context.

ISPs are forbidden to access computers without right (art. 138ab Wetboek van Strafrecht [Sr, Criminal Code], prohibiting hacking), and they are prohibited to take knowledge, without right, of data processed through their networks which are not addressed to them (i.e. traffic to and from customers) (art. 273d Sr). But since these provisions include the clause 'without right', it depends on the contractual terms whether ISPs can detect infections by accessing computers or monitoring (content of) communications of their customers. If the General Terms and Conditions of an ISP contain a provision allowing the ISP to scan for infections, then this will generally be lawful under Dutch law.

- ____(see questions 11.2 to 11.3)

11.1) Do ISPs in practice do so?

☐ No
☒ Yes - (see questions 11.2 to 11.3)

11.2) What kind of data is processed by ISPs in these detections and identifications?

I am not positive about what kind of data.

12.4) Are ISPs required to mention the existence of such detection/ identification mechanisms in their contract?

☐ No
☐ Yes - ________________________________(please provide a concrete example)

11.3) Do they deploy monitoring sensors?

☐ No
☐ Yes – **If so, which aspects of this monitoring sensors make it data privacy compliant?**

I am not sure

B – National Computer Emergency Response Teams

11) Is there a national or research CERT established in your country?

☐ No
☒ Yes – National Cyber Security Center
______________(CERT name)____________________(see questions 12.1 to 12.2)

12.1) Do they deploy monitoring sensors?

☐ No
☐ Yes – **If so, which aspects of this monitoring sensors make it data privacy compliant?**

I am not sure , probably.

12.2) What kind of data is processed by CERTs in these detections?

Section 3 - Centralised Clearing Data House and National Support Centre

12) **Are there private or public-private partnerships established in your country where data concerning malware infections is exchanged?**

☐ No

☒ Yes – How is data collected and what kind of data is shared among partners?

http://www.abuseinformationexchange.nl/

It is still being build, but typically buying from 3rd parties

13) **Are there other private or public-private partnerships dealing with other aspects of cybersecurity (besides malware infections data sharing)? Please explain how they operate.**

I am not positive

14) **In which circumstances are IP-addresses, whether dynamic or static, considered as personal data in your country?**

The CBP (the Data Protection Authority) considers a static IP address always to be personal data, and dynamic IP addresses to be personal data in combination with date and time, since the address can always be traced back to a natural person. It does not matter whether the data controller itself can trace it back, what matters is that there is someone (usually the ISP) who can make the link. (The fact that sometimes it traces back to a legal person does not alter this general rule.) Also relevant is the fact that IP addresses can be used to take decisions (without having combining them with (other) personal data) whether or not to allow someone to access information (e.g. geolocation) is relevant to treat IP addresses as personal data.

Source: College Bescherming Persoonsgegevens (2007), *CBP Richtsnoeren Publicatie van persoonsgegevens op internet*, http://www.cbpweb.nl/downloads_rs/rs_20071211_persoonsgegevens_op_internet_definitief.pdf, p. 10.

15) **For how long are ISPs required to retain data in the terms of article 6 of Directive 2006/24/EC (Data Retention Directive)[203]?**

6 months

16) **Are there circumstances in which the monitoring of communications by ISPs will not be considered an offence or a violation of privacy?**

☐ No
☒ Yes – see answer to question 11

17) **Are ISPs allowed to share data of infections with other service providers?**

☐ No
☐ Yes – if so, is this limited to a certain type of data? ___________________________

Again, this depends on the circumstances – which data, which other providers, which reasons, and, particularly, which provisions are included in the General Terms and Conditions. The sharing of data is generally regulated under the same conditions as those of Directive 95/46/EC.

18) **Are ISPs allowed to directly communicate to a customer identified as victim or author of an infection?**

☐ No
☒ Yes – why wouldn't they be allowed? In the Netherlands, people are allowed to communicate directly with other people.

Art. 11.3 Telecommunications Act requires ISPs to take care to inform their customers of "special risks for violating the safety or security of the offered network or offered service" as well as of the possible means that can be used to counter these risks (other than measures that the ISP can or should take itself). Although this provision is probably targeted at informing customers of more general threats (such as a particularly high-risk virus), it may perhaps also be interpreted as a duty of care to inform users that they are infected, in cases the ISP has acquired knowledge about such infection.

19) **Are ISPs required to communicate detections/identifications to law enforcement agencies or other public authorities?**

☒ No
☐ Yes - ____

20) **Are CERTs allowed to share data of infections with actors others than law enforcement?**

☐ No
☐ Yes – if so, is this limited to a certain type of data? ___________________________

I think they are allowed to share data with others, but again it depends on the context. I'm not sure whether the NCSC qualifies as an administrative agency

[203] Article 6 - Periods of retention
Member States shall ensure that the categories of data specified in Article 5 are retained for periods of not less than six months and not more than two years from the date of the communication.

(bestuursorgaan), in which case the sharing of data would be regulated under the Algemene wet bestuursrecht [General Administration Law Act], or as a private or law-enforcement or intelligence agency – since it is a hybrid organisation with tasks also in the field of crime detection and national security, sharing of data may fall under different legal regimes depending on the type of data and context.

21) **Are CERTs allowed to directly communicate to an user identified as victim or author of an infection?**

☐ No
☒ Yes – Why not?

Section 4 - End customer tools

Concerning the practice of malware cleaning software in your country:

22) **How do they assign liability for damages caused to customers and other users (non-customers)?**

Not sure

23) **How do they ask, record and store user’s consent?**

Can't determine it.

Section 5 – Additional information

24) **Is there any additional information you would like to add that could help us with the analysis or any legal challenge that has not been addressed?**

No

End of questionnaire