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

Deliverable	1.8.2 – Legal Requirements (second iteration)
Work package	WP1
Due date	31-07-2015
Submission date	31-07-2015
Revision	
Status of revision	
Responsible partner	KU Leuven – B-CCENTRE
Contributors	Karine e Silva, B-CCENTRE, ICRI/CIR, KU Leuven
	Valerie Verdoodt, ICRI/CIR, KU Leuven
	Damian Clifford, ICRI/CIR, KU Leuven
	Uwe Rasmussen, Microsoft
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	2014-11-26	First internal draft Karine e Silva
1.2	2015-02-28	Final draft Karine e Silva shared with partners for feedback
1.3	2015-05-12	Amendments made by Valerie Verdoodt (KUL) and Damian Clifford (KUL) – affected chapters: all.
1.4	2015-07-31	Amendments from Uwe Rasmussen (Microsoft) included. Affected chapters: Annex 2.

Glossary

C&C Command-and-control centre

CCH Centralised Data Clearing House

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

Chapter 1 of this deliverable provides a brief overview of the requirements analysed in D1.8.1. This summary is divided in two sections including (1) the general data protection framework and (2) the main elements related to the cooperation with Law Enforcement Agencies ("LEAs").

Furthermore, Chapter 2 of the analysis aims at providing an overview of the recent developments which may have an effect on the operation of the ACDC solution. Similar to Chapter 1, the analysis is divided into two sections, the first focusing on the data protection and privacy developments and the second on the cooperation with Law Enforcement Agencies.

Chapter 3 of this deliverable is focused on the guidelines relevant for the ACDC project. However, it is significant to note that the legal barriers as experienced within the lifecycle of the ACDC project have been addressed in "D5.3 Policy Recommendations for Public Authorities Dealing with the Regulatory Aspects of the Fight against Botnets". Indeed, the current deliverable has focused entirely on the developments since its first iteration and as such does not have an analysis of gaps within its scope. Furthermore, this deliverable is not focused on the assessment of the ACDC solution vis-à-vis the requirements outlined supra and in D1.8.1. Instead, this is the focus of D4.3 and as such reference should be made to the analysis provided in this specified report.

The analysis is supplemented by two annexed documents which provide some more detailed analysis to aid the understanding of the elements discussed in the deliverable.

Table of Contents

Introduction

In D1.8.1 KUL conducted a thorough analysis of the scope of the applicable EU legislation and an overview of a corresponding selection of national implementations in relation to the ACDC Project. In this deliverable, D1.8.2, we build upon the legal requirements as set out in the previous deliverable. In particular, this deliverable offers an overview of the latest developments regarding the legal framework and the implications for the ACDC project. For further clarification of the concepts and standards described in this report, we refer the reader to D1.8.1. Moreover, in relation to the gaps and barriers found throughout the ACDC project, the reader should refer to D5.4 and for an assessment of the legality of the ACDC developed solution one should refer to D4.3.

ROADMAP

Chapter 1 of this deliverable provides a brief overview of the requirements analysed in D1.8.1. This summary is divided in two sections including (1) the general data protection framework and (2) the main elements related to the cooperation with Law Enforcement Agencies ("LEAs"). Furthermore, Chapter 2 of the analysis aims at providing an overview of the recent developments which may have an effect on the operation of the ACDC solution. Similar to Chapter 1, the analysis is divided into two sections, the first focusing on the data protection and privacy developments and the second on the cooperation with Law Enforcement Agencies. Chapter 3 of this deliverable is focused on the guidelines relevant for the ACDC project. The analysis is supplemented by two annexed documents which provide some more detailed analysis to aid the understanding of the elements discussed in the deliverable.

Chapter 1 - Summary of requirements established in D1.8.1

In D1.8.1 KUL conducted a thorough analysis of the scope of the applicable EU legislation and an overview of a corresponding selection of national implementations. For further clarification of the concepts and standards described in this report, we refer the reader to D1.8.1. The purpose of this section of the analysis is to provide a brief overview of the requirements analysed in D1.8.1. However, this does not represent a complete analysis of requirements and the reader should assess the legal obligations contained in this deliverable in conjunction with D1.8.1.

1. General data protection requirements

1.1 Applicable legislation

At an EU level two main instruments are particularly important for ACDC, namely Directive 95/46/EC (Data Protection Directive) and Directive 2002/58/EC (e-Privacy Directive). The first of these provides the lex generalis framework whereas the latter stipulates the lex specialis rules relevant for public communications networks and services. Accordingly, both of these Directives have applicability in the context of the ACDC project.

1.2 Data quality principles

It is significant to note that Article 6 Directive 96/46/EC provides several key principles which must be complied with when processing personal data. These have been outlined in detail in D1.8.1, however in summary, it should be noted that the key principle is that personal data must be processed fairly and lawfully (Art. 6 (1) (a)). Additionally, other key principles as contained in Article 6 include purpose specification limitation, data minimisation and limited retention.

1.3 Legitimate ground

The issue of legitimate grounds is rather complex and fundamental to the legal viability of the ACDC project. As such, it is explored in a separate section in this document (see infra, section 5).

1.4 Data subject rights

Articles 12 and 14 Directive 95/46/EC stipulate the data subject rights which must be respected by the data controller. In summary, these rights relate to the right of access to the personal data being processed in relation to them and the right to object the further personal data processing under specified conditions. Furthermore, one should also note the overlap with Article 15 Directive 95/46/EC, which provides that data subjects have the right not to be subject to automated individual decisions. This right is supplemented by Article 12 (a), which specifies that data subjects have the right to obtain information relating to any logic involved in the automatic processing of their personal data. Accordingly, this adds to the data subject rights outlined. To this end, KUL recommends each controller to establish a data protection officer inside the institution to oversee the processing and guarantee individuals are given the opportunity and means to exercise their rights.

1.5 Confidentiality and security of processing

Data controllers shall prevent unauthorised access to the data being processed and put in place technical and organisational measures that guarantee an optimal level of security to protect personal data (Article 17 Directive 95/46/EC). Thus, controllers hold the duty to safeguard the confidentiality, integrity and authenticity of the data. Such security measures are required to be appropriate regarding the risks associated with the particular data processing at hand. In addition, the nature of the data collected is also significant in the assessment of the appropriateness of the security measures. Accordingly, Article 17 (2) further indicates that the appropriate level of security is determined by

- the state of the art
- the costs
- the sensitivity of the data.

In the assessment of the state of the art, one must consider ENISA opinions.

1.6 The principle of proportionality

Any processing of personal data must be proportionate vis-à-vis the aims of the processing and the potential for the infringement of fundamental rights and freedoms of citizens. This is

of particular importance to anyone involved in ACDC. In simple terms, the impact on the fundamental rights of individuals cannot exceed that which is necessary in order to mitigate the impact of botnet attacks. This balancing exercise is not an easy one. For example, one should refer to the CJEU ruling that invalidated Directive 2006/24/EC (Data Retention Directive) (see infra).

1.7 Notification to the DPA

Finally, Directive 95/46/EC allows broad discretion in the implementation of the provisions related to notification contained in Articles 18 and 19. Article 18 provides for the functioning of a notification procedure for data controllers or their representatives in a wholly or partly automatic manner. Article 19 stipulates a list of the minimum information to be included in such a notification. However, Article 18 (2) provides room for discretion by stating that Member States have the capacity to indicate a simplification or exemption of the procedure if certain specified conditions are met. Therefore, in order for a complete understanding of the particular requirements in a Member State, one must refer to the national implementing measures.

2. Cooperation with law enforcement authorities

As mentioned in D1.8.1, cooperation with law enforcement authorities ("LEAs") is an important aspect of the fight against botnets. Having LEAs engaged in the ACDC project is significant for the sustainability of the project. In particular, for mitigation efforts to be effective, cybercriminals should be prevented from regaining access to information systems. With this in mind, this section will discuss the main elements related to cooperation with LEAs.

2.1 No compulsory network monitoring

Article 15(1) of Directive 2000/31 on Electronic Commerce[1] does not provide a systematic obligation of surveillance and collaboration on ISPs to monitor the entire traffic undergoing their network. Accordingly, in the context of ACDC, the contribution and participation of ISPs happens on a voluntary basis. The monitoring activities must be legitimised and comply with the Directive 95/46/EC and the e-Privacy Directive, based on the legitimate ground as defined in D1.8.1.

2.2 Breach notification obligations

According to Article 4(3) of the e-Privacy Directive[2], ISPs have an obligation to notify national authorities of any personal data breach.[3] Moreover, service providers are required to inform end-users of any personal data breaches which are likely to adversely affect its personal data or privacy without undue delay. In other words, 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. In addition, as discussed in D1.8.1, ISPs are allowed to redirect users to the National Support Centre of their home country.

3. Table of requirements

The table below provides a clear overview of the relevant requirements extracted from the data protection framework as set out in D1.8.1 and summarised above. This representation

[1] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), *OJ L* 178, 17.7.2000, 1–16.

[2] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), *OJ L* 201, 31.7.2002, 37–47.

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

of requirements aims at indicating a general insight into the partners' obligations vis-à-vis the data protection and privacy framework. It does not however provide an entire analysis of all requirements as specified by Directive 95/46/EC and Directive 2002/58/EC and the national implementations, but rather an extrapolated indicative list of applicable provisions.

Req. Number	Requirement	Description	Comment	Legal basis
Req. 1	Prior authorisation and notification	The data controller MUST meet all notification and authorisation requirements that may be stipulated by the national law of the competent Member State.	National implementations must be consulted as due to disparity between the adoptions of the data protection framework, divergences in these requirements may exist.	Articles 18, 19 and 20 Directive 95/46/EC and their national MS equivalents as stipulated by the national law of the competent Member State.
Req. 2	Restrictions on the processing of sensitive data	If sensitive data is processed the specific restrictions MUST be complied with.	The more stringent national laws applicable for the processing of sensitive data and the requirements of Art. 8 Directive 95/46/EC (including export restrictions) must be complied with if these special categories of data are being processed.	Article 8 Directive 95/46/EC
Req. 3	Legal ground for processing	The data controller MUST have a legal ground for processing (as specified further in req. 3.1-3.4 In addition, regard should be had to any potential exemption in national law to the application of the legal requirements.	Within ACDC, the potential legal grounds for processing personal data are the following: ➢ Obtaining the consent of the data subject ➢ Contractual obligation ➢ Public interest ➢ Legitimate interest of the data controller See Req. 3.1-3.4	Article 7a Article 7b Article 7e Article 7f Directive 95/46/EC Exemption – Article 13 Directive 95/46/EC
Req. 3.1	Consent	IF the data controller wants to rely on the data subject's consent as a legal ground for processing, the consent MUST be valid.	For consent for the processing of sensitive data (see Article 8 95/46/EC) to be valid, it must be given explicitly.	Article 7(a) Directive 95/46/EC
Req. 3.2	Performance of a contract	IF the data controller wants to rely on a performance of a contract as a legal ground for processing, the data controller MUST only act within the boundaries of this contract. Furthermore, the extent of the data processing MUST be necessary to fulfil this contract.	For instance, if ACDC uses an external entity to process personal data, however, this does not apply to entities that ***define the purpose of the processing***. Accordingly, ECO is a data controller as distinct from a data processor, but their processing may be justified under a contractual obligation.	Article 7(b) Directive 95/46/EC
Req. 3.3	Performance of a task in the public interest	IF the data controller wants to rely on the performance of a task in the public interest or in the	In the context of ACDC, the protection of a public network could be deemed a task in the	Article 7(e) Directive 95/46/EC

		exercise of official authority, the data controller must only act in the furtherance of this task.	public interest. However, national DPA's should be consulted.	
Req. 3.4	Legitimate interest of the data controller	IF the data controller wants to rely on its legitimate interest as a legal ground for processing, the data controller MUST have a legitimate interest in the data processing.	In the context of ACDC, the protection of a public network could be deemed a task within the legitimate interest of the data controller, if such an attack could have a major impact on their business model. However, national DPA's should be consulted.	Article 7(f) Directive 95/46/EC
Req. 3.4.1	Credible evidence	IF the data controller wants to rely on its legitimate interest as a legal ground for processing, the data controller MUST be able to provide credible evidence to prove the existence of its legitimate interest.	This exercise involves a weighing of the data subjects' and data controller's legitimate interests, as well as taking into account the principle of proportionality (see D4.3).	
Req. 4	Data quality	The personal data and processing MUST adhere to the legal standards of data quality.	To fulfil this requirement, ACDC data controllers should ensure compliance with sub-requirements 4.1-4.6.	Article 6 Directive 95/46/EC
Req. 4.1	Fairness	All processing operations involving personal data within ACDC MUST be completed processed fairly and lawfully.		Article 6(a) Directive 95/46/EC
Req. 4.2	Purpose limitation	The personal data MUST only be collected for specified, explicit and legitimate purposes. Furthermore, the data MUST NOT be further processed in a way which is incompatible with those purposes.	Thus any personal data collected for purposes as specified by ACDC (i.e., botnet mitigation) cannot be later re-used for a different and incompatible purpose.	Article 6(b) Directive 95/46/EC
Req. 4.3	Necessary and adequate for the purpose	The personal data MUST be relevant, adequate and not excessive regarding the purposes for which it is collected and/or further processed. In ACDC, this purpose would be the mitigation of botnets.	Partners that process personal data must ensure that all reasonable steps are taken in order to ensure that inaccurate and/or incomplete data are deleted or updated while remaining aware of the purposes of the processing. (See also Req.4.4 and 4.5)	Article 6(c) Directive 95/46/EC
Req. 4.4	Accuracy	The data controller responsible for the processing MUST take every reasonable step to ensure that the personal data is accurate and up to date.	Therefore, the accuracy of any personal data stored within ACDC should be constantly assessed and inaccurate data should be deleted (see also Req. 4.5).	Article 6(d) Directive 95/46/EC
Req. 4.5	Deletion	When the personal data is no longer necessary for the specified purposes, it MUST be deleted or anonymised.	Therefore ACDC should implement a mechanism that arranges deletion or anonymisation of the personal data which has become unnecessary.	Article 6(d) Directive 95/46/EC
Req.	Secure	The deleted personal data MUST		

4.5.1	deletion	NOT be retrievable.		
Req. 4.6	Automated individual decisions	Within the ACDC context, automated individual decisions relating to the data subject MUST NOT be made or supported, unless authorised by law.		Article 15 Directive 95/46/EC
Req. 5	Data subject's rights	Data controllers MUST respect the data subject's rights.	ACDC should allow an easy operation of data subject's rights.	Article 14 (a) and (b) Directive 95/46/EC
Req. 5.1	Right to information	The data controller MUST provide data subjects with sufficient information on at least the following aspects: the identity of the controller, the categories of data that will be processed, whether the information is voluntary of obligatory, the purpose for processing, &the recipients of the personal data, the further rights to access and to rectify.		Article 10 and 11 Directive 95/46/EC
Req. 5.2	Right to access	Data subjects MUST be capable of obtaining intelligible information from the data controller without expense or excessive delay.	If deemed necessary, the ACDC consortium could integrate a system capable of processing requests from data subject.	Article 12 Directive 95/46/EC
Req. 5.3	Right to rectify	Within ACDC, the data subject's rights to legitimately rectify, reply, revoke, erase or block his or her personal data MUST be supported.		Article 12(b) Directive 95/46/EC
Req. 6	Technical and organisational measures	Both data controllers and processors MUST guarantee that appropriate and state-of-the-art technical and organisational measures to ensure security and confidentiality are implemented.	In this regard, the ENISA opinions on state-of the art in a given industry need to be taken into account. Also, regard must be had for the level of sensitivity of the data and the cost of implementation of the measures.	Article 17 Directive 95/46/EC and Article 4 e-Privacy Directive
Req. 7	Location and traffic data	ISPs MUST abide by the requirements related to traffic and location data.		Articles 5 and 9 e-Privacy Directive
Req. 8	Breach notification	Providers of publicly available electronic communications services MUST notify national authorities without undue delay of any personal data breach. When the personal data breach is likely to adversely affect the personal data or privacy of a subscriber or individual, the provider SHALL also notify the subscriber or individual of the breach without undue delay.	This is significant for the ISPs involved in ACDC.	Article 4(3) e-Privacy Directive

Table 1 – Data protection requirements.

Chapter 2 - Recent developments

This section of the deliverable aims at providing an overview of the recent developments which may have an effect on the operation of the ACDC solution. Similar to Chapter 1, the analysis is divided into two section, the first focusing on the data protection and privacy developments and the second on the cooperation with Law Enforcement Agencies ("LEAs").

1. Data protection and privacy - developments

1.1 Data protection reform package

As noted in D1.8.1, the data protection framework [Directive 95/46/EC] is currently under reform. The proposed General Data Protection Regulation has been in the pipeline since 2012 and has recently entered trilogue phase.[4] It should be noted that this is the final stage before the potential adoption of the Regulation and it is therefore important to consider the key legislative changes that this draft proposes. For example, although the proposed Regulation maintains the key data quality principles as expressed in Article 6 Directive 95/46/EC, it expressly provides for the principles of transparency, data minimisation and controller liability which thus far have only been implicitly recognised. Specifically in relation to the data minimisation principle, although the CJEU has previously recognised the existence of this principle, the draft proposal provides a legislative acknowledgement of its existence.[5]

Moreover, one of the main objectives of the proposed General Data Protection Regulation is to establish a clear attribution of the responsibilities of both controllers and processors. More in particular, Recital 62 determines that:

> "The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processor, also in relation to the monitoring by and measures of supervisory authorities, requires a clear

[4] See press release of 15.6.2015 http://www.europarl.europa.eu/news/en/news-room/content/20150615IPR66464/html/Data-protection-Parliament%E2%80%99s-negotiators-welcome-Council-negotiating-brief.

[5] CJEU Case274/99 *P. Connolly v Commission*, [2001] OJ C173/13 see also more recently in CJEU Case C-131/12 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014] OJ C 212/4.

attribution of the responsibilities under this Regulation, including where a controller determines the purposes, conditions and means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller."

As such, the Regulation introduces certain new elements resulting in increased accountability for both controllers and processors. For instance, if processors decide to process data beyond the controller's instructions, they should be regarded as joint controllers.[6] According to Article 24, Joint controllers will have to determine their respective responsibilities for compliance with the data protection requirements in a transparent way (i.e., in a contract). Thus, it seems that the Regulation will force processors to take their share of responsibility for the implementation of accountability and the compliance with the data protection requirements. However new difficulties may arise regarding the definition of "joint controllers" and what constitutes "processing data beyond the controller's instructions". It will depend on the interpretation of this article by the data protection authorities and the courts.

Aside from the Regulation, it should be noted that the data protection reform also encompasses the proposed Police and Criminal Justice Data Protection Directive.[7] This Directive aims at replacing the existing Framework Decision covering personal data processing in the area of law enforcement and criminal justice thereby simplifying the current framework. The impact of this element of the reform package for ACDC is perhaps relevant for partners with law enforcement capacity as established under national law. Accordingly, relevant partners should also be aware of this element and the potential changes if adopted.

---

[6] European Commission, "Explanatory Memorandum to the proposal for a General Data Protection Regulation", 20 January 2012, 10, accessible at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0011&from=en; The responsibilities of joint controllers are clarified in Article 24 of the Regulation.

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

1.2 Data Retention Directive

It is significant to note the seminal decision of the Court of Justice European Union ("CJEU") which found the Data Retention Directive invalid.[8] Indeed, the Court of Justice found that:

> "Directive 2006/24 does not lay down clear and precise rules governing the extent of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter. It must therefore be held that Directive 2006/24 entails a wide-ranging and particularly serious interference with those fundamental rights in the legal order of the EU, without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary."

The Court continued by specifying that the Directive failed to provide objective criteria to ensure that only competent authorities have access to the data and that this access is only used for the purposes of prevention, detection or prosecutions in order to ensure that the interference is justified based on the seriousness of the offences. The Court also found that in relation to the retention, the imposition of a 6 month period without a distinction between the categories of data or its usefulness vis-a-vis the objective pursued was excessive. Finally, the Court decided that the Directive:

> "does not provide for sufficient safeguards, as required by Article 8 of the Charter, to ensure effective protection of the data retained against the risk of abuse and against any unlawful access and use of that data."

In summary, the court found that the powers provided for by the Directive were not proportionate and thus that they were contrary to the fundamental rights provided for in the Charter. Due to this judgement the national implementations of this Directive have unclear foundations. Member States such as Austria, Bulgaria, Slovenia, Belgium and the Netherlands have annulled the national implementing measures whereas the UK has implemented emergency measures providing for their continued legitimacy and application.

---

[8] CJEU, Joined cases C-C293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and others,* 8 April 2014.

The issue is currently pending in countries such as Ireland and Hungary. Therefore, there is a large degree of disparity amongst the Member States.

1.3 Article 29 Working Party Opinion 06/2014[9] on Article 7(f) Directive 95/46/EC

Since the first deliverable (D1.8.1), the Article 29 Working Party has issued an opinion on the application of Article 7(f) of the Directive. As previously explained in D1.8.1, Article 7(f) stipulates that

> "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)."

Accordingly, this ground for processing requires a balancing of the legitimate interests of the controller or beneficiary third party and the fundamental rights of citizens. The Article 29 Working Party decided to issue an opinion clarifying several aspects related to the application of the provision. The content of this opinion is relevant for ACDC as private sector companies may rely on this ground for processing.

Legitimate Interest. The Article 29 WP makes a distinction between "interest" and "purpose". An interest must be real and present, directly linked to the activities related to the processing, while the purpose may be more abstract and broader. For example, an ISP sharing data through the CCH has the purpose of supporting intelligence gathering of botnets, but its interest is mainly receiving data that points to infections affecting its own network and customers. Therefore, while the purpose relates to threat mitigation and security, the interest is targeted at a direct activity performed by the ISP.

Having an interest alone is not sufficient, as this interest must be legitimate for the application of Article 7 (f). For an interest to be legitimate, it must be sufficiently specific

[9] Article 29 Working Party Opinion 06/2014 on the "Notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC".

and clearly articulate, and should represent a real and present interest.[10] In its opinion, the Article 29 Working Party expressly listed **physical security, IT and network security; processing for historical, scientific or statistical purposes; and processing for research purposes** (including marketing research) as examples of legitimate interests. In ACDC the use of Article 7(f) could be applied in situations where the processing of data is deemed necessary for achieving a general public interest or private actor's interest.

Proportionality and the Balancing test. The interest of the controller or third party needs to be compelling. Minor and less compelling interests can only be justified under Article 7(f) when the impact on the lives of data subjects is minimal or insignificant. In this regard, the Article 29 Working highlights the importance of **adequate safeguards** for reducing the impact of processing on data subjects. Furthermore, the Working Party recommends the use of privacy risk assessments to evaluate the potential impact of a processing activity. Therefore, **any controllers making use of Article 7(f) as a legal ground for processing in ACDC are recommended to run a privacy risk assessment**.

In evaluating the balance between the interests of the controller/third party and the rights of the individuals, the Article 29 Working Party outlines a list of **important elements to be taken into account when assessing the overall impact of the processing**. Specifically:

1) The controller's/third party legitimate interest:
    1.1 Is it the exercise of a fundamental right?
    1.2 Is there a public interest or a wider societal interest involved?
2) The impact of the processing:
    2.1 Did a competent body assess the impact?
    2.2 What is the nature of the data involved in the processing?
    2.3 What are the risks involved in the way the data are being processed?
    2.4 What are the reasonable expectations of the data subjects in this context?
    2.5 What are the capabilities and size of the controller and processor?

[10] Article 29 Working Party Opinion 06/2014 on the "Notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC", 25.

These elements are significant and have a clear impact on the safeguards necessary for Article 7 (f) to be applicable. Indeed, as mentioned above, data controllers are required to ensure the confidentiality and security of the personal data. However, in the context of the application of Article 7 (f), the Article 29 Working Party highlights that in order to "tip the balance" in favour of the legitimacy of the use of Article 7 (f) additional safeguards may need to be satisfied. These safeguards may not be explicitly expressed as requirements under the Directive, but the Working Party provides the following indicative examples:

- Technical and organisational measures to ensure that the data cannot be used to take decisions or other actions with respect to individuals ('functional separation' as is often the case in a research context)
- Extensive use of anonymisation techniques
- Aggregation of data
- Privacy-enhancing technologies, privacy by design, privacy and data protection impact assessments
- Increased transparency
- General and unconditional right to opt-out
- Data portability & related measures to empower data subjects

As it is the responsibility of each partner in ACDC to comply with the applicable legal framework, **it is for each partner to verify whether they fulfil the balance test of Article 7(f), as implemented by their national law**, and have their legal department or counsel decide on this matter.

1.4 Dynamic IP addresses

Another significant development relates to the classification of IP addresses as personal data. Currently there is a pending case before the CJEU which may clarify the status of dynamic IPs and thus their classification as personal data. The German Federal Court

(Bundesgerichtshof) referred this question to the CJEU on the 28th of October 2014.[11] Specifically the German Court is seeking to clarify whether dynamic IPs constitute personal data when the IP address itself is stored by an ISP while the information capable of identifying a natural person is held by a third party.[12] The Article 29 Working Party has previously stated in its opinion on the concept of personal data that as in practice it is practically difficult to distinguish between static and dynamic IPs both should be treated as personal data. [13] As such, it can be concluded that in essence although this opinion fails to classify dynamic IPs as personal data but instead recommends giving dynamic IPs a *de facto* personal data status due to the inability of service providers to make a distinction.[14] This will be an issue that will be hotly debated in the Court and it may allow the CJEU the opportunity to provide some degree of clarity.

Finally, reference should be made to Annex 1 to this Deliverable, which provides a more detailed analysis of the country-specific requirements in relation to IP addresses from a Bulgarian perspective. This input was provided by BG-Post and gives an indication of the complexity of the area.

2. Cooperation with LEA – developments

There have been a few developments worth noting in relation to cooperation between law enforcement agencies (LEA) and other actors in the context of botnet threat mitigation. Significant in this regard are Directives 2013/40/EU, Directive 2014/41/EU and the notification obligations in the proposed NIS-Directive and the General Data Protection

[11] Bundersgerichtshof, « Vorlage and den EuGH in Sachen Speicherung von dynamischen IP Adressen », Pressemitteilung Nr. 152/14, 28 October 2014, accessible at http://www.google.com/url?q=http%3A%2F%2Fjuris.bundesgerichtshof.de%2Fcgi-bin%2Frechtsprechung%2Fdocument.py%3FGericht%3Dbgh%26Art%3Dpm%26Datum%3D2014%26Sort%3D3%26nr%3D69184%26pos%3D0%26anz%3D152&sa=D&sntz=1&usg=AFQjCNE7JKxXgMXIS5N5nzkUXWothT7LPQ

[12] D.Clifford and J. Schroers, "Personal data and dynamic IPs – time for clarity?", LSE Media Policy Blog, 2015, accessible at http://blogs.lse.ac.uk/mediapolicyproject/2015/01/23/personal-data-and-dynamic-ips-time-for-clarity/.

[13] Article 29 Working Party Opinion on Search Engines, 4 April 2008, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp148_en.pdf.

[14] D.Clifford and J. Schroers, "Personal data and dynamic IPs – time for clarity?", LSE Media Policy Blog, 2015, accessible at http://blogs.lse.ac.uk/mediapolicyproject/2015/01/23/personal-data-and-dynamic-ips-time-for-clarity/.

Regulation. This section of the analysis will provide a concise overview of the requirements contained in these legislative developments and their potential impact on ACDC.

2.1 Directive 2013/40/EU on attacks against information systems

Directive 2013/40/EU aims to establish minimum rules in relation to the definition of criminal offences and sanctions in the context of attacks against information systems (see Article 1).[15] This Directive will replace the Council Framework Decision 2005/222/JHA of 24 February 2005[16] and requires adoption before the 4th of September 2015. More specifically, the Directive aims towards the harmonisation of minimum standards in order to ensure that such crimes are punishable by effective, proportionate and dissuasive criminal penalties. Although these provisions require transposition, thereby raising concerns vis-à-vis potential implementation disparities, such harmonisation will allow for some degree of clarity regarding the transboundary substantive and procedural legal standards for the specified offences. Given that this section of the deliverable focuses on the legislative developments relating to cooperation with LEAs, it is important to consider the specific provisions relevant for procedural harmonisation. As noted in the questionnaire attached to D1.8.1, the Convention on Cybercrime does contain some harmonising measures in relation to procedural aspects. However, the Convention allows for broad discretion and in addition countries such as Ireland are yet the legislative text into national law. It is with this in mind that the EU has aimed to strengthen cooperation in the form of Directive 2013/40/EU. Indeed, this Directive focuses on increasing cooperation in the area of criminal justice via:

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

[15] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.

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

- introducing an obligation to collect basic statistical data on cybercrimes.[17]

As the Directive specifically targets botnet attacks, its relevance for ACDC is clear. For a clear understanding of the obligations derived from the Directive, close attention should be given to the national implementations in order to understand the future application of the requirements.

2.2 Directive 2014/41/EU on the European investigation order in criminal matters

In addition to the above, it is also important to consider Directive 2014/41/EC on the European investigation order in criminal matters.[18] This Directive requires adoption before the 22nd of May 2017 and provides harmonising measures relating to the transfer of evidence between Member States.[19] This reform will provide for increased harmonisation. According to Article 1(1):

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

---

[17] ENISA, "The Directive on attacks against information systems A Good Practice Collection for CERTs on the Directive on attacks against information systems", 24 October 2013, 4, accessible at https://www.enisa.europa.eu/activities/cert/support/fight-against-cybercrime/the-directive-on-attacks-against-information-systems/at_download/fullReport.

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

[19] Currently the legislative framework consists of: (1) European Convention on Mutual Assistance in Criminal Matters Strasbourg, 20.IV.1959 accessed on 24/03/2015 at www.conventions.coe.int/Treaty/en/Treaties/Html/030.htm; (2) Schengen Agreement of 1985; (3) Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union (2000/C 197/01); (4) Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union (2000/C 197/01); (5) Council Framework Decision 2003/577/JHA of 22 July 2003 on the execution in the European Union of orders freezing property or evidence OJ L 196 45–55.

In summary this mechanism will allow for more effective cross-border investigations. This is significant in order to identify and prosecute the perpetrators of transboundary crimes, such as botnet attacks.[20] Given the timeframe for adoption, attention must be had for its implementation in the Member States.

2.3 Update on the breach notification obligations

Finally, there have been certain developments related to the obligations to notify security or personal data breaches. First, the proposed Network and Information Security Directive foresees in such an obligation in Article 14.[21] This Directive is currently being debated at the Council level, but is indicative of a general move towards increased cooperation in relation to this issue at an EU level. Although the first iteration of this proposal coming from the European Commission included obligations for private actors generally, its scope has since been restricted to the domain of critical infrastructures (e.g. sectors energy, transport, etc.). Accordingly, only actors falling into such a classification will be required to respect the requirements contained in the proposal if it is adopted in its current version. Therefore, the developments in this area should be watched closely.

Second, the draft General Data Protection Regulation should be considered. Articles 31 and 32 provide an obligation for every data controller to notify personal data breaches to the relevant parties "without undue delay". Moreover, the proposed Police and Criminal Justice Data Protection Directive[22] further reflects the requirement.

3. Implications of the developments for ACDC

[20] E. De Capitani and S. Peers, "The European Investigation Order: A new approach to mutual recognition in criminal matters", accessible at eulawanalysis.blogspot.com/2014/05/the-european-investigation-order-new.html.

[21] Proposal of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union' COM (2013) 48 final.

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

From the analysis provided in sections 1 and 2 of this Chapter, certain key developments have been identified and examined. The purpose of this section is to assess the potential impact of these developments for the ACDC project.

First, regarding the developments in the area of data protection and privacy, it is important to observe that in the context of ACDC, the proposed General Data Protection Regulation foresees increased responsibilities for data processors. This will bring data processors' obligations more in line with those specified for data controllers. Such a change may have a clear impact on the operation of the ACDC solution. From D4.3 it should be noted that the CCH may fall into the category of a data processor. Although there are limited legal obligations for data processors under Directive 95/46/EC (as described in D1.8.1) the proposed Regulation would result in increased legal obligations and liabilities. However, for a complete analysis of this, one should refer to the specific section of D4.3. Furthermore, it should be noted that although the analysis provided supra in relation to the status of dynamic IP addresses may provide clarity in this area, given that the focus of the ACDC project is on the identification of infected hardware (and the participation of partners with the capacity to do this) the impact of the case may be restricted. Finally, the data retention developments and the finding by the CJEU of the invalidity of the Data Retention Directive may have an effect on the operation of the ACDC solution. However, given the unclear status of the national implementing measures in many of the 28 Member States, obtaining a clear overview of requirements is a challenge. As such, partners should take into account the status of data retention in their respective jurisdictions.

Second, in relation to the developments in the field of cooperation with LEAs, the changes discussed in section 2 of this Chapter are significant. First and foremost, it should be noted that Directives 2013/40/EU and 2014/41/EU have been adopted and are simply awaiting transposition into national law. Importantly, as per the fundamental principles of EU law, although these Directives are yet to enter into force Member States are prevented from acting in a manner contradictory to the aims and objectives of the legislation. Moreover, Directive 2013/40/EU has an implementation deadline in September of this year and as such many requirements may already be found in national law as this Directive provides minimum harmonising standards. Finally, the proposed NIS-Directive may have a potential impact on the ACDC project (e.g., security breach notification obligations) if it is adopted in its original

form. However, developments regarding this proposal should be watched closely and it is unlikely that the more recently watered down proposal will be given renewed strength.

Chapter 3 – Guidelines

Chapter 3 of this deliverable is focused on the guidelines relevant for the ACDC project. However, it is significant to note that the legal barriers as experienced within the lifecycle of the ACDC project have been addressed in "D5.3 Policy Recommendations for Public Authorities Dealing with the Regulatory Aspects of the Fight against Botnets". Indeed, the current deliverable has focused entirely on the developments since its first iteration and as such does not have an analysis of gaps within its scope. Furthermore, this deliverable is not focused on the assessment of the ACDC solution vis-à-vis the requirements outlined supra and in D1.8.1. Instead, this is the focus of D4.3 and as such reference should be made to the analysis provided in this specified report.

In order to foster compliance with the requirements provided above, the following table provides a set of guidelines on how to implement the requirements mentioned in Table 1 within the ACDC solution. These implementation guidelines have been deciphered from the analysis provided. It should be noted that these guidelines are a representation of the privacy by design and by default methodology, which is gaining increasing traction in European data protection law. Indeed, the proposed General Data Protection Regulation explicitly recognises privacy by design as a key principle in the future of data protection law. Given that the proposed Regulation is to be regarded as a significant development, and also, its entry into the trilogue phase it is important to consider the potential impact of this potential addition to the ACDC project. However, it is noteworthy that a successful implementation of the legal requirements listed in the deliverables should in itself cater for any potential changes brought about by the adoption of the Regulation.

Guide. No.	Description	Associated Req.	Comment
Guid. 1	Only the minimum amount of data should be collected/received/stored within the CCH.	Req. 4.3	To restrict the remaining amount of personal data, it is recommended to use the highest level of aggregation including the least amount of data.
Guid. 2	The interrelationships between personal data should be hidden from plain view. This is particularly relevant for the long-term storage of the data within the CCH	Req. 6	To implement this strategy, a variety of means exist, such as encrypting the data; using a mix networks to hide traffic patterns; using anonymisation techniques which

			allow to unlink the relationship between related events.
Guid. 3	It is recommended to complete personal data processing in a distributed fashion. This would prevent the completion of full profiles of individuals.	Req. 6	At the moment, no design patterns for this strategy are known.[23]
Guid. 4	It is recommended that authentication protocols with privacy features are implemented.	Req. 6	
Guid. 5	The security of the personal data should be ensured throughout the entire lifecycle of the data.	Req. 6	For this, encryption should be employed throughout, and the default state of data should be unreadable in case there is data leak.
Guid. 6	It is recommended that at the end of its lifecycle, personal data is securely disposed or anonymised, in order to be in compliance with the principles of limited retention and data minimisation.	Req. 4.4, Req. 4.5	
Guid. 7	It is recommended that all communications within the ACDC Platform solutions are encrypted.	Req. 6	
Guid.8	It is recommended that systems are designed to ensure that when personal data are exchanged, any data elements that are not necessary to fulfil the purpose of the transmission are filtered out or removed.	Req. 4.3, Req. 6	
Guid. 9	It is recommended that systems are designed to restrict access to the personal data transferred to the extent necessary for the role that is performed.	Req. 6	Appropriate access controls should be in place, in order to prevent unauthorised disclosures of personal data.
Guid.10	Integrate a system whereby data subject requests can be processed within the ACDC infrastructure.	Req. 5	This ensures the possibility for the enforcement of data subjects rights and is crucial for compliance with the data protection requirements.

Table 3 Implementation guidelines

[23] G. Danezis, J. Domingo-Ferrer J., M. Hansen, J-H. Hoepman, D. Le Métayer, R. Tirtea and S. Schiffner, 'The implementation of the Privacy and Data Protection by Design – from policy to engineering' (ENISA 2014), accessed at https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-and-data-protection-by-design.

Conclusion

From the analysis provided above, it can be concluded that there have been certain developments in relation to the legal framework as outlined in D1.8.1. Despite these changes it should be noted that the impact on ACDC is limited. We have assessed the modifications under the data protection and privacy and cooperation with LEAs frameworks. However, significantly, much of what has been discussed is still in draft format and thus is yet to be adopted. With this in mind, partners should closely follow the developments in this regard.

Annex 1 - Regulations Concerning the Exchange of Personal Data and the Status of the IP Address in Bulgarian Legislation

Authors: Lilyana Goranova, Antoaneta Nikolaeva, Nadezhda Aleksieva

The Regulatory Framework in Bulgaria

The regulatory framework in Bulgaria concerning personal data protection can be divided into general and sectoral legislation. The Law on Personal Data Protection, the Rules of Procedure of the Commission for Personal Data Protection and its Administration, Ordinance №1 of January 30th, 2013 for the Minimal Level of Technical and Organizational Measures and the Admissible Type of Personal Data Protection can be defined as **general legislation**. The following acts can be defined as **sectoral legislation**: Law on Civil Registration, Law on Copyright and Related Rights, Law on E-commerce, Law on Electronic Communications, Law on the Electronic Document and the Electronic Signature, Law on E-governance, Law on Protection of Classified Information, Law on Consumer Protection, Law on the Commercial Register, Law on Obligations and Contracts, the Commercial Law.

In fact, technological development and the accompanying social-economic relations, including business on the Internet, often outstrip the regulation of the new areas, so that when a new law or amendment is already in force, the market and technology have already put forward a host of new issues to be solved.

International Legislation

The main legal acts regulating the topic being discussed are as follows:

Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

Directive 97/66/EC of the European Parliament and of the Council on the processing of personal data and the protection of privacy in the telecommunications sector;

Directive 2000/43/EC implementing the principle of equal treatment between persons irrespective of racial or ethnic origin;

Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications);

Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.

Personal Data Protection

The Law on Personal Data Protection (LPDP) in effect as of January 1st, 2002 provides a definition of the term "personal data" and establishes obligations with regards to its collection and processing. According to the legal definition of Art. 2, paragraph 1 of the LPDP, "**personal data** is any information, relating to a natural person, who is identified or can be identified directly or indirectly by an identification number or by one or more specific signs".

The Law also introduces the concept of "data controller", which according to Art. 3, paragraph 1 of the LPDP is a natural person or a legal entity as well as a public authority or local government, which alone or together with another person determines the aims and the means of processing personal data.

Art. 4, paragraph 1 of the LPDP comprehensively enumerates the cases when the processing of personal data is admissible:

1. processing is necessary to fulfill a legal obligation of the data controller;

2. the natural person, to whom the data relates, have given explicitly their consent;

3. processing is necessary to fulfill obligations under a contract, to which the natural person, to whom the data relates, is a party as well as for actions that precede the conclusion of a contract and taken at their request;

4. processing is necessary to protect the life and health of the natural person, to whom the data relates;

5. processing is necessary to perform a task carried out in the public interest;

6. processing is necessary for the exercise of powers conferred by law to the controller or a third party to whom the data is disclosed;

7. processing is necessary for the realization of the legitimate interests of the data controller or a third party to whom the data is disclosed, except where such interests are overridden by the interests of the natural person to whom the data relates.

The processing of personal data according to the legal definition of § 1, point 1 of the Additional Provisions of the LPDP is any action or a combination of actions which can be performed with regards to personal data with automatic or other means, such as collection, recoding, organization, storage, adaptation or modification, retrieval, consultation, use, disclosure through transmission, dissemination, provision, updating or combination, blocking, erasure or destruction. According to position №11-3333/23.04.2015 of the Commission for Personal Data Protection, for there to be lawful processing of personal data, it should be performed if at least one of the optional criteria for eligibility of processing, given and listed in Art. 4, paragraph 1 of the LPDP, is present as well as in strict compliance with the principles for their processing, pointed out in Art. 2, paragraph 2 of the LPDP.

The statutory right of data controllers to process personal data is related to certain obligations, such as those listed in Art. 19, paragraph 1 of the LPDP: to inform the persons, from whom the data was collected, about the aims of data processing, the recipients, to whom they may be disclosed, information about the right of access to and correction of the data, etc. The inclusion of a provision, to this effect, in the contract between the website's owner, for example, and its users could help to prove compliance with the obligations under Art. 19 of the LPDP.

Any data controller should check whether the data, which they collect from their users and clients and process, falls within the scope of the law, and should take respective measures. And each person, whose personal data shall be collected and processed, should explicitly give their consent.

It is prohibited to process personal data that relates to health, sexual life and human genome, i.e. the publication of information, where a disease of a particular person is discussed, shall be deemed violation of the law.

Data controllers have to comply with the following rules established in Section 3 of the LPDP:

-to collect personal data only with the knowledge and consent of the persons to whom it relates;

-to collect only as much data as they need to perform the service or activity, for which the data is collected;

-to store the data reliably and not to provide other data controllers with the data without the knowledge and consent of the persons;

-to provide the persons with access to the data whenever requested by them;

-after the performance of the activity, for which it is collected, to destroy the data or to make it anonymous.

Any natural person has the right to access to the personal data relating to them. When exercising this right, anyone can at any time request the following from the data controllers:

- Confirmation as to whether the data relating to them is processed, information about the aims of this processing, the categories of data and the recipients or the categories of recipients, to whom the data is disclosed;

- Communication to them in a comprehensible form, containing their personal data which is processed as well as any available information about its source;

- Information about the logic involved in any automated processing of personal data relating to them.

In position № 1659/ 07.04.2014, Sofia, 02.05.2011, the Commission for Personal Data Protection draws the following conclusion regarding the treatment of the IP address as personal data:

1. The IP address should be regarded as information, constituting personal data, in all cases when it allows or helps for the direct or indirect identification of a user.

2. With the aim of protecting the fundamental rights and freedoms of persons when processing data related to them, the IP address in all cases should be treated as personal information.

3. Any data controller should process an IP address only if at least one of the eligibility conditions in Art. 4 of the LPDP is present, and if the principles of conformity with the law, expedience and proportionality are observed.

The Status of the IP-address in International Law

Regarding the issue of processing personal data, one should bear in mind the text of p.6 of the Commission Recommendation of 9 March 2012 on preparations for the roll-out of smart metering systems. Promulgated L OB, issue 73 of March 13th, 2012, 2012/148/EU under which it should be taken into consideration that according to Art. 8 of the Charter of Fundemental Rights of the European Union and Art. 8, paragraph 2 of the European

Convention on Human Rights justification is required in case of interference with the right to protection of personal data. The grounds of the interference should be assessed separately for each and every case in accordance with the cumulative criteria for lawfulness, necessity, legitimacy and proportionality. Therefore, any processing of personal data, where interference in the fundamental right to personal data protection is present, within the smart energy grid and the smart metering system, has to be necessary and proportional so that it could be deemed fully compliant with the Charter.

The German Commissioner for Data Protection, Mr. Peter Schaar, leading the group for the preparation of a report on how well search engines comply with European laws on personal data protection, thinks that since someone is identified by an IP address or another protocol, then this is storage of personal data.

His opinion differs from that of Google, for example; in their opinion the IP address simply identifies the location of the computer, not who the individual user is. Schaar admits that the IP addresses of computers are not always personal as in many cases the same computers are used by many users.

The treatment of IP addresses as personal data would affect the way companies store these addresses. Google is the first company to take steps to reduce the time for storing information to up to 18 months. It also manages to reduce the time for storing "biscuits" that collect information about how users look for data on the Internet to up to two years. By default this period is 30 years for Google.

A considerable number of applications on the Internet show the addresses of people who are using a service of a website at the moment or who used such a service. For example, many forums show the name of the user and their IP address simultaneously. Thus everyone can identify easily the location of this user. Another example are websites that provide statistics about the number of visits – often the IP addresses from which the site was visited, or the IP addresses of users who are currently online are shown.

In line with the position of the European Supervisory Authority of June 5th, 2010 regarding the project of the Anti-Counterfeiting Trade Agreement (ACTA), citing the definition of personal data in Art. 2 of Directive 95/46/EC: *"any information related to an identified or a person, subject to identification ("respectively natural person"); a person, subject to identification, is a person that can be identified, directly or indirectly, most specifically by an*

identification number", we can only draw the conclusion that IP addresses and information about the actions related to these addresses are personal data in all cases regarding the topic. In fact the IP address serves as an identification number, which allows finding the name of the user, to whom this IP address was provided.

Regarding the obligation of providers to store information:

According to Directive 2002/58/EC, and in particular Art. 6 thereof, collection and storage of traffic data such as IP addresses is only allowed on grounds directly related to the communication service, including for the purpose of issuing an invoice for the service, management of traffic and fraud prevention. With the removal of these grounds, data should be destroyed. This obligation does not affect the obligations under the Directive on retention of data, which as pointed out above contains the requirements as to the storage of traffic data and making it available to police and prosecutors to aid the investigation of serious crimes only.

This means that when the holders of copyright address Internet service providers after the expiry of a limited period, the latter should not have files with data regarding the activity of the users, connecting the IP addresses with the respective users. The storage of data files after the expiry of this period should be allowed only when the grounds, related to the aims set out in the law, are present.

In this respect, the Bulgarian Constitutional Court was approached when in April, 2014 the European Court of Justice (ECJ) declared Directive 2006/24/EC of the European Parliament on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks null and void. The case was opened at the request of the Ombudsman of the Republic of Bulgaria – Konstantin Penchev, with the aim of establishing the unconstitutionality of the provisions of Art. 250a – 250e, Art. 251 and Art. 251a of the Law on electronic communications (promulgated, State Gazette, issue 41 of 2007, last alteration and amendment, State Gazette, issue 11 of 2014).

With the contestation of the legal texts, the access of the Ministry of Internal Affairs and the security authorities to traffic data regarding the Internet and telephone communications of citizens was facilitated. The amendments provide that this data can be provided to the Ministry of Internal Affairs and the Prosecutor's Office when this is necessary for the

detection and investigation of serious crimes (i.e. punishable by more than 5 years of imprisonment), computer crime as well as for the tracing down of persons (Art. 250a, paragraph 2 of the Law on electronic communications). According to the Ombudsman, the collection and storage of traffic data about all users of electronic communications services for a period of more than 12 months, with the aim of the possible use of some of this data with regards to a limited number of persons for the possible detection of crimes, is disproportionate and unjustified interference in citizens' rights.

According to Art. 4 (1) of the Law on The State Agency for National Security (amended, State Gazette, issue 35 of 2009, issue 93 of 2009, issue 52 of 2013), the State Agency for National Security performs activities to protect national security from attacks directed to the independence and sovereignty of the Republic of Bulgaria, its territorial integrity, national interests, the established constitutional order in the country and the fundamental rights and freedoms of citizens, related to: …

10. disruptive impact on communication and information systems; ….

17. computer crimes or crimes committed in or via computer networks and systems;

Art. 29 (2) stipulates that for the performance of the tasks and activities under this law, **the structural units of the Agency can collect personal data as well**.

In view of the above-mentioned, we should wait for the position of the Constitutional Court, given the existence of special laws in the country, which could prove to be in contradiction.

The thesis of IP addresses as personal data is known to the European Supervisory Authority. There is judicial practice in this sense in Poland, Sweden and others. For exhaustiveness of the discussion, it should be mentioned that there is a counter thesis – IP addresses are not personal data according to courts in Germany, Ireland and others. And in Great Britain the concept is that they could be or they could not be personal data, depending on the particular case.

On January 25th, 2012 the European Commission proposed a comprehensive reform of the EU rules for data protection of 1995 with the aim to strengthen privacy rights in the online environment, and to boost the development of the European digital economy. The aim of the amendments is to have one law that will end the current fragmentation and costly administrative burden, and that will create economies for businesses. With the Commission's proposals the principles established in the Directive for personal data protection of 1995 are updated and modernized in order to guarantee privacy rights in the

future. The proposals consists of a communication on policy, where the Commission's aims are presented, and two legislative proposals: regulation for establishment of a common EU framework for data protection and a directive for protection of personal data processed for the purposes of prevention, detection, investigation or prosecution of crimes and related judicial activities.

The main changes introduced by the reform are:

- **One set of rules** for data protection, valid across the EU, which will eliminate the unnecessary **administrative requirements** such as requirements for notification by companies. This will save businesses around € 2.3 billion annually.
- Instead of the current obligation for all companies to notify supervisory authorities for data protection about all data protection activities – requirement that led to unnecessary administrative formalities and costs for businesses to the amount of more than € 130 million annually, the regulation provides for greater **responsibility and accountability** for those processing personal data.
- Thus, for example, companies and organizations have to notify the national supervisory authority about all serious **violations of the security of data** as soon as possible (if possible, within 24 hours).
- Organizations will be able to work with only **one national data protection authority** in the EU Member State, where they have their principle place of establishment. Similarly, people will be able to address the **data protection authority** in their country even when their personal data is processed by a company established outside of the EU. When **consent** for data processing is required, it should be explained that the consent has to be given explicitly, rather than being assumed.
- People will have an easier **access to their own data** and will be able to **transfer personal data** more easily from one provider to another (right to data portability). This will improve competition in the service sector.
- "**The right to be forgotten**" will help people to manage better the risks related to data protection in the online environment: people will be able to delete their data unless there are legal grounds for their retention.

- The EU rules have to be applied when personal data **is processed abroad** by companies that perform their activity on the EU market and offer their services to the EU citizens.
- **The independent national data protection authorities** will be strengthened so they can better implement EU rules in their countries. They will be empowered to impose fines on companies, which violate EU rules for data protection. This may lead to fines to the amount of up to €1 million or up to 2% of the annual turnover of the company.
- Based on the new **directive,** the common principles and rules for data protection will be applied to the **police and judicial cooperation regarding criminal matters**. The rules will be applicable to both internal and cross-border transmission of data.

In conclusion, emphasis should be put on the position of the Commission for Personal Data Protection on the issue of the provision and exchange of personal data, namely: *„According to § 1, p.5 of the Additional Provisions of the LPDP, "provision of personal data" refers to actions for complete or partial transmission of personal data from one data controller to another or to a third party on the territory of the country or outside of it, and constitutes processing of personal data within the meaning of the law. Any action with regards to the processing of personal data, including the provision and/or exchange for the purposes of the ACDC project, should be done within the established regulations."*

Annex 2 - Final Iterations

The case of Microsoft: transfer of data between non-EU private sector partner through the CCH

Microsoft has a large database containing external IP addresses of botnet infected computers concerning 250 different botnet virus strains from 15 different virus families. The infection data has been distributed by Microsoft to partners for some years with the purpose of having partners notify the IP address users so that the infected machines can be cleaned up. Microsoft's expertise in the legal framework for the distribution of infection data was to benefit the ACDC project as it can be read from ACDC DOW, in Taskgroup 2 "provide its expertise in contracts elaborated to enable information sharing between the Microsoft Cybercrime Center (based on US law) and third parties (CERTs, national cybersecurity centers or ISPs)" and "bring its expertise in EU policy matters, with participation from its Brussels based policy team".

However, the legal constraints that the ACDC is under has made it impossible for ACDC to make use Microsoft's distribution model. Instead most of the discussions under the 1.8 task have revolved around the challenges of distributing the infection data. In particular, un-harmonized EU privacy legislation has made been challenging to have ACDC become a data controller but instead the CCH operates as a data processor for the data it receives so as to not have to meet the data subjects' rights and not to have to notify DPAs in all jurisdictions where the data is to be used.

Microsoft's model is based on that the data collection is governed by US law as it is carried out in the United States pursuant to a US Court Order. The data is made available to partners from a secure platform located in the United States. If a partner, the data consumer, wants to use the data within the EU, it is the partner who imports the data in the EU who is data controller and thus their responsibility to ensure that the intended usage of the data meets the requirements in the Data Protection Directive and in particular:

- That a legitimate reason is justifiable, article 7(f),
- That data subjects receive complete information about the processing (article 11) and have a right of access (article 12),
- The data processing must be publicized through notification with the national Data Protection Authority, article 21.

Microsoft's US model is not transposable to the EU. Indeed, it would be impossible for a data controller to meet the above legal requirements as the identity of the user of the infected IP address is not known and only privy to the Internet Access Provider. Moreover, the keeping

of the identity of the user of the IP address is viewed as illegal in a recent decision by the Belgian Supreme Court[24].

Although the Directive includes an exemption for the above points in article 13(d): "*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: … (d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions*;" these derogations for the data processor are not mandatory under EU law and indeed most Member States have not been implemented the exemption making it all but impossible to operate on a EU level.

While Microsoft has not been able to replicate its distribution model to the CCH of ACDC, Microsoft is extremely satisfied with the project. It has allowed for the creation of National Anti-Botnet Support Centres in Europe which Microsoft's partners such as Telefonica and Deutsche Telecom can refer their infected customers to as they receive the botnet infection data from Microsoft.

It is noteworthy that many EU DPA's have indicated that enforcement of EU data transfer rules "*will not be their priority*" in relation to transfers of personal data of non-EU residents collected outside the EU and transferred back again. An example would be that a US based company transfers data to an EU based processor. In this situation, the US data are processed and stored on servers in the EU. Following Article 4(1)(c) of Directive 95/46/EC, EU data protection legislation will be applicable.[25] In this regard, the DPA's state that even though EU data protection legislation is applicable, they will not enforce it as it "*may have undesirable consequences in terms of economic impact and enforceability*".[26]

---

[24] The link between an IP address and the natural person is information that only the owner of the IP address has and even he may not be able to collect it as the Belgian Constitutional Court ruled on decision 84/2015 of June 11th, 2015.

[2525] See also Article 29 Working Party Opinion 8/2010 on applicable law, 16 December 2010, 9, accessible at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_en.pdf.

[26] See CNIL "CNIL facilitates the use of outsourcing services performed in France on behalf of non-European companies", 15 March 2011, accessible at http://www.cnil.fr/english/news-and-events/news/article/cnil-facilitates-the-use-ofoutsourcing-services-performed-in-france-on-behalf-of-non-european-compa/ as cited by L. Moerel, "Binding corporate rules: Fixing the regulatory patchwork of data protection", 2011, 108-110, accessible at https://pure.uvt.nl/portal/files/1346784/Moerel_binding_19-09-2011.pdf. For instance, according to the UK Information Commissioner's Office: "*it would be a disincentive for businesses to locate their processing operations in the EU*."

Bibliography

6.1 Primary Sources

Legislative documents

Directive 95/46/EC of the European Parliament and Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31.

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), *OJ L* 178, 17.7.2000, 1–16.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), *OJ L* 201, 31.7.2002, 37–47.

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

Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) COM (2012) 11 final.

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

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

Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.

European Commission, "Explanatory Memorandum to the proposal for a General Data Protection Regulation", 20 January 2012, 10, accessible at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0011&from=en.

'Proposal of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union' COM (2013) 48 final.

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

Case law

CJEU Case274/99 *P. Connolly v Commission*, [2001] OJ C173/13 see also more recently in CJEU Case C-131/12 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014] OJ C 212/4.

CJEU, Joined cases C-C293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and others,* 8 April 2014.

6.2 Secondary Sources

Article 29 Working Party Opinion 8/2010 on applicable law, 16 December 2010, 9.

Article 29 Working Party Opinion on Search Engines, 4 April 2008.

Article 29 Working Party Opinion 05/2014 on Anonymisation Techniques, adopted on 10 April 2014.

Article 29 Working Party Opinion 06/2014 on the "Notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC".

Clifford D. and Schroers J., "Personal data and dynamic IPs – time for clarity?", LSE Media Policy Blog, 2015, accessible at http://blogs.lse.ac.uk/mediapolicyproject/2015/01/23/personal-data-and-dynamic-ips-time-for-clarity/.

CNIL "CNIL facilitates the use of outsourcing services performed in France on behalf of non-European companies", 15 March 2011, accessible at http://www.cnil.fr/english/news-and-events/news/article/cnil-facilitates-the-use-ofoutsourcing-services-performed-in-france-on-behalf-of-non-european-compa/ as cited by L. Moerel, "Binding corporate rules: Fixing the regulatory patchwork of data protection", 2011, 108-110, accessible at https://pure.uvt.nl/portal/files/1346784/Moerel_binding_19-09-2011.pdf.

Danezis G., Domingo-Ferrer J., Hansen M., Hoepman J-H., Le Métayer D., Tirtea R. and Schiffner S., 'The implementation of the Privacy and Data Protection by Design – from policy to engineering' (ENISA 2014) https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-and-data-protection-by-design accessed on 02//022015.

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

ENISA, “The Directive on attacks against information systems A Good Practice Collection for CERTs on the Directive on attacks against information systems”, 24 October 2013, 4, accessible at https://www.enisa.europa.eu/activities/cert/support/fight-against-cybercrime/the-directive-on-attacks-against-information-systems/at_download/fullReport.

Hoepman J-H, ‘Privacy design strategies – (extended abstract) In ICT Systems Security and Privacy Protection’ (29th IFIP TC 11 International Conference SEC Morocco, June 2014).