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

Deliverable	**4.3 – Legal validation of the prototype tested during the Pilot**
Work package	WP4
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 Prof. Dr. Anton Vedder, ICRI/CIR KU Leuven (Internal reviewer) Peter Meyer, ECO (Reviewer) Rosa Hafezi, DE-CIX (Reviewer)
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	Modification
1.1	2014-11-28	First Draft – Karine e Silva (KUL)
1.2	2015-01-16	Second Draft – Karine e Silva (KUL)
1.3	2015-06-26	Finalised Draft for feedback – Valerie Verdoodt and Damian Clifford (KUL)
1.4	2015-07-23	Feedback reviewer (ECO)
1.5	2015-07-28	Review comments integrated (KUL)

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

Chapter 1 of this deliverable provides the basis for the legal validation of the prototype and is divided into three sections. Section 1 focuses on the process and methodology for defining the legal requirements and communicating them to partners, section 2 provides a brief overview of the requirements outlined in the previous deliverables and section 3 outlines the methodology for the legal validation and more in particular the process of gathering information to feed the analysis.

Chapter 2 of the deliverable focuses on the analysis of the findings and is divided into two sections. Section 1 focuses on the analysis of the legal requirements in relation to the ACDC prototype based on the inputs provided by the key partners. Section 2 will provide a more detailed assessment of the compliance of the CCH with the identified legal requirements based on the information stemming from the questionnaire and the Terms of Use.

It should be noted that the conclusions provided in this chapter are based upon the integrity of the inputs supplied by the partners and as such, KUL's assessment has been dependent on the correct delivery of the relevant data. Therefore, any inconsistencies with the information supplied fall within the responsibilities of the relevant partner as KUL is incapable of anticipating any deviations from the input provided by the partners.

Contents

INTRODUCTION

This deliverable aims at evaluating the compliance of the developed ACDC solution with the legal requirements as defined in D1.8.1 and D1.8.2. KUL's assessment of the ACDC prototype to be tested during the pilot is based on the information as provided by partners and as such is dependent on the correct delivery of the relevant data. The lessons learned from this analysis have supported the definition of potential barriers for an EU-wide deployment of the system as well as the policy recommendations as provided by D5.4.

ROADMAP

Chapter 1 of this deliverable provides the basis for the legal validation of the prototype and is divided into three sections. Section 1 focuses on the process and methodology for defining the legal requirements and communicating them to partners, section 2 provides a brief overview of the requirements outlined in the previous deliverables and section 3 outlines the methodology for the legal validation and more in particular the process of gathering information to feed the analysis. Chapter 2 of the deliverable will then focus on the analysis of the findings and is divided into two sections. Section 1 focuses on the analysis of the legal requirements in relation to the ACDC prototype based on the inputs provided by the key partners. Section 2 will provide a more detailed assessment of the compliance of the CCH with the identified legal requirements based on the information stemming from the questionnaire and the Terms of Use.

CHAPTER 1 - THE BASIS FOR THE LEGAL VALIDATION

Section 1 - Defining legal requirements - the process and methodology

In WP1, D1.8.1 [M12] outlined the legal requirements that partners need to take into account throughout the lifecycle of the project which are summarised in section 2 infra. Each of the partners are thus expected to have implemented the legal requirements in the architecture of the platform and at all levels where tools communicate and when data are shared among partners (e.g. from sensors to the CCH, from the CCH to the community platform, from subscribers to the community platform) and, evidently, at all levels of data processing input and output related to the mitigation tools operated by partners (e.g. sensors, website analysis tools, end-user tools).

Between the publication of D1.8.1 (WP1) and this D4.3 (WP4), 18 months have passed. Within this period, partners were expected to fully implement the requirements. This process was made possible by the strategy put in place by KUL with the support of the Project Leader, ECO, and the collaboration of DFN-CERT, FKIE, Inteco, EII, FCCN, and SignalSpam. Since it was not possible in terms of time and resource to evaluate the entire implementation of the requirements for each tool involved in the project, the evaluation was conducted by sampling. Indeed, this task focused on gathering evidence of implementation of the legal requirements by the key partners involved in the project that manage a specific tool. This allowed the verification of compliance at the core structure of the ACDC solution. To achieve this, the following process and methodology was chosen:

1. KUL (Karine e Silva) gave a presentation at the general ACDC Workshop in Frankfurt on May 28th, 2014. At this occasion, KUL presented an overview of the findings of D1.8.1 and presented the action plan for the successful attainment of D4.3 and D1.8.2. This included key partners' commitment to delivering a set of use cases related to their operations involving any kind of personal data (Use cases – due in the end of August – to feed D1.8.2) and to answer the 'ACDC – Legal validation of the prototype tested during the Pilot – D4.3' document (shared with partners on July 10th, 2014) by the end of September 2014. Partners have voluntarily agreed to this during the ACDC Workshop in Frankfurt, where only SignalSpam was not present, but was notified shortly after the event.

2. Between the formalised request by email and the delivery date for use cases and answers to the document, all key partners have been individually contacted and offered assistance by KUL (Karine e Silva) on what was expected from them. In the occasion, key partners were also informed that they would perform an important role in assisting and coordinating all other partners involved in their operations and tools to provide answers to 'ACDC – Legal validation of the prototype tested during the Pilot – D4.3' document'.

3. After receipt of the preparatory document, KUL started reviewing the answers to verify the need for any additional or missing information. If this was the case, partners were individually contacted and informed on what information was missing and how this could be resolved.

4. After the deadline for the additional or missing information, KUL started examining whether the implementation of the legal requirements as reported by partners was in compliance with the legal requirements as set out in D1.8.1. In this regard, the findings of the questionnaire were critically examined and used to feed this deliverable. The answers provided by partners can be found in Annex 2 of this deliverable.

Section 2 - Background and requirements from previous deliverables

The legal requirements relevant for the ACDC project have been analysed in depth in D1.8.1 and updated in D1.8.2. For a comprehensive analysis of these obligations one should refer to the specific deliverables. However, in order for this deliverable to analyse the legality of the ACDC prototype tested during the Pilot, it is necessary to first provide a brief overview of the requirements outlined in the previous deliverables. In particular, Annex 1 to this report, offers a detailed overview of the legal requirements as expressed in a tabular format in order to facilitate reader understanding.

The requirements extrapolated from the data protection and privacy framework are of key importance for the implementation of a legally compliant ACDC prototype. Indeed, it should be noted that cooperation with law enforcement agencies ("LEAs") is more of a reactionary legal requirement and as such does not affect the implementation of an architecture.

The privacy and data protection requirements on the other hand have a defined effect on the processes and operations to be performed by an engineered solution. As a result, the data quality principles and in particular data minimisation, purpose specification and limitation and data retention must be respected in the very design of an architecture. Therefore, these requirements as provided for in Article 6 Directive 95/46/EC[1] form the basis of our analysis. Moreover, Article 7 Directive 95/46/EC indicates the specific grounds upon which the personal data processing operations can be legitimised. As described in D1.8.1 and D1.8.2, several of these grounds have relevance in the context of the ACDC project. In particular, consent (Article 7 (a)), contractual obligation (Article 7 (b)), public interest (Article 7 (e)) and the legitimate interest of the data controller (Article 7 (f)). For the specifics regarding the scope and application of each of these grounds, one should refer to the detailed analysis provided previously. In addition, the data subject rights must be respected (Articles 12 and 14 Directive 95/46/EC). Article 15 Directive 95/46/EC is of particular significance as it relates to the data subject's right not to be subject to automated individual decisions. Furthermore, Article 17 Directive 95/46/EC stipulates the specific requirements vis-à-vis the confidentiality and security of the personal data being processed.

Also, the specific requirements as found in the e-Privacy Directive[2] should be respected. Significant in this regard are the requirements in relation to traffic data and the specific obligations regarding breach notification.

Finally, it should be noted that the fundamental EU principle of proportionality must be taken into account throughout the data processing operations. Indeed, this principle plays a key role in legitimising security operations versus the potential for the infringement of fundamental human rights. Therefore, the proceeding analysis relies on the key legal requirements as described supra.

[1] 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.

[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.

Section 3 - Methodology for the legal validation of the prototype

Having outlined the legal requirements as summarised above, partners were required to implement them during the development of the ACDC solution. In order to assess this implementation, KUL (Karine e Silva) decided that the most appropriate method for gathering information was to disseminate a questionnaire requesting input from the key partners. Chapter 2 of this deliverable will assess this input vis-à-vis the questions posed and the underlying associated legal requirements. The questionnaire was divided into five sections namely:

1. Preliminary questions
2. Purpose specification, legitimate grounds and data quality principles
3. Proportionality of processing
4. Data subjects rights
5. Security of processing

These divisions were made in order to simplify the questionnaire for the partners and to facilitate the comparison outlined in Chapter 2. Accordingly, the analysis in Chapter 2 focuses on a comparative examination of the inputs received based on the desk research conducted in D1.8.1 and D1.8.2 which concentrated on the deciphering of the relevant legal requirements.

The following table is a representation of the questionnaire that was disseminated to the key partners.

A. Preliminary questions

A.1. Are you processing personal data? If so, what types of personal data are you processing?

A.2. Are you planning to anonymise these personal data at any stage of the processing (e.g. after collection; before analysis; before sharing with the CCH)?

A.3. Are you sure it is not possible for your tool to achieve the same planned result/impact by anonymising these data after collection or before sharing it with the CCH?

A.4. Is it possible to pseudonymise these data at any stage?

A.5. After reading section 2.4.6 of D1.8.1 (pp. 28-30), do you consider yourself a controller or a processor[3]?

A.6. If you consider yourself a processor, who would be the controller of the processing you are involved in?

B. Purpose specification, legitimate grounds and data quality principles

B.1. What is the purpose of your tool?

B.2. How do you technically ensure the data are only used for that limited purpose?

B.3. After reading section 2.4.9 and Chapter 4 of D1.8.1 (pp. 36-40, pp. 53-63), are any of the legitimation grounds of Article 7 of Data Protection Directive applicable to your tool[4]? How do you justify this?

B.4. How can you prove you are collecting only the data which are necessary to achieve the purpose of the processing and that you cannot reach the same purpose with less or anonymised data?

B.5. How do you define how long the data should be stored?

B.6. How will you ensure the data are deleted after storage period is finished?

B.7. How do you ensure the processed data (e.g. stored by your tool) is accurate and up to date?

B.8. Is there an entity or agent responsible for overseeing your processing, inside your institution?

[3] Data controller is a person or organisation who/which determines the purposes and means of data processing. 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. The legal distinction between 'controller' and 'processor' is not dependent on whether 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.

[4] Unambiguous consent (Article 7(a))
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;
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, for the performance of the contract;
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;
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)
This provision is often used by companies seeking for a legitimate excuse in the processing of personal data. 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.

C. Proportionality of processing

C.1. If you answered Art. 7(f) in B.3, what is the nature of the legitimate interest pursued by your tool (private or public)?

C.2. Who directly benefits from your tool (e.g. end users, ISPs, customers, etc.)? Are there any indirect beneficiaries (e.g. the organisation, ISPs, law enforcement)?

C.3. Have you identified the impact this tool has on fundamental rights such as privacy or confidentiality of communications (e.g. in case of mistakes, false positives, etc.)?

C.4. Which measures have you taken to mitigate the impact of the tool on fundamental rights of citizens?

C.5. Do you process sensitive data (personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life)?

C.6. Are you accountable for any damage caused by your tool? If not, who would be?

C.7. What additional safeguards have you put in place to prevent undue impact on the lives of citizens?

D. Data Subjects' rights

D.1. Has your organization appointed someone to answer data subjects' requests?

D.2. How will you inform users about your processing, types of data involved and the identity of the third parties that may have access to their data?

D.3. How do you empower data subjects to exercise their rights (objection, erasure and blocking) and enable mechanisms for them to access, modify, delete, transfer, or otherwise further process (or let third parties further process) their own data?

E. Security of processing

E.1. How do you ensure the security (integrity, availability and confidentiality) of the data processed by your tool?

E.2. Have you taken into account the sensitivity of the data processed and the impact on the lives of citizens in the case of a security breach before choosing for these mechanisms?

E.3. Do they correspond to the state-of-the-art?

CHAPTER 2 - ANALYSIS OF THE FINDINGS

This Chapter of the deliverable is divided into two sections. Section 1 focuses on the analysis of the legal requirements in relation to the ACDC prototype based on the inputs provided by the key partners. This section will be further subdivided as per the sections contained in the questionnaire. Section 2 will provide a more detailed assessment of the compliance of the CCH with the identified legal requirements based on the information stemming from the questionnaire and the Terms of Use.

It should be noted that the conclusions provided in this chapter are based upon the integrity of the inputs supplied by the partners and as such, KUL's assessment has been dependent on the correct delivery of the relevant data. Therefore, any inconsistencies with the information supplied fall within the responsibilities of the relevant partner as KUL is incapable of anticipating any deviations from the input provided by the partners.

Section 1 - Analysis of the legal requirements in relation to the ACDC prototype

1.1 Preliminary questions

As is clear from the title, the first subsection of the questionnaire dealt with the relevant preliminary questions necessary to determine the applicability of the data protection and privacy framework. In order to establish applicability, partners were asked if they were processing personal data (and if so the types), if any personal data being used during the course of the project would be anonymised (as anonymised data does not fall under the scope of the Directive 95/46/EC), whether the partners consider themselves to be the data controller or data processor (based on the definitions provided in D1.8.1).

In assessing the responses, it is important to note that several partners have indicated that they process personal data (IP, emails, spam reports, names, e-mailaddresses, attached documents, URL, device serial number, (full name, working position – for the ACDC Community Portal)). The use and sharing of IP addresses has been highlighted by several of the partners who provided input. As per the analysis provided in D1.8.2, the current status of dynamic IP addresses and their classification as personal data is unclear. However, as this uncertainty relates to an inability to identify natural persons with a dynamic IP, this debate has questionable relevance in the context of the ACDC project. Indeed, as the ACDC solution aims at identifying the affected machines of citizens, questions in relation to linkability are somewhat redundant. As such, personal data is being processed in the context of the ACDC project and therefore, the data protection and privacy framework is applicable.

Having identified that the material scope of Directive 95/46/EC is satisfied, our attention now turns to the personal scope and the classification of partners as data controllers and processors. This is an important distinction given the disparity in responsibilities and liabilities under Directive 95/46/EC. Nevertheless, it should be noted that the proposed General Data Protection Regulation foresees in the implementation of changes in this regard. More specifically, data processors will have increased responsibilities and liabilities, bringing them somewhat in line with those of data controllers. These changes are reflected in KULs observations as expressed in D5.4 Policy Recommendations for Public Authorities Dealing with the Regulatory Aspects of the Fight against Botnets. Indeed, recommendation 8 stipulates that:

Reforms that are currently on the negotiating table at an EU level should be adopted expeditiously in order to ensure greater harmonisation.

Such clarification regarding the increase in responsibilities and liabilities of data processors would allow for legal certainty and also, better protection of data subject interests.

As there are several partners who deem themselves data controllers or data processors, the above analysis is relevant and the second requirement for the application of the data protection framework is satisfied.

As the final requirement on the scope of application relates to geographical location (i.e., partners have to be processing personal data in the EU for Directive 95/46/EC to be applicable), one can conclude that the requirements as expressed in Directive 95/46/EC must be complied with.

1.2 Purpose specification, legitimate grounds and data quality principles

Subsection 2 of the questionnaire dealt with Article 6 and 7 Directive 95/46/EC. As illustrated above, key to this analysis are the purpose specification, data minimisation and limited retention principles. Moreover, the legal grounds legitimising the processing operations conducted in ACDC were assessed on the basis of partner input.

In analysing the partner inputs relevant for the data quality principles, it is clear that the partners have aimed to protect the integrity of the requirements specified in Article 6 Directive 95/46/EC. More specifically, partners report that they refine raw data so that only the personal data which is necessary for the purposes of the processing is processed (Reqs. 4.2 and 4.3). Moreover, partners have indicated that they will delete personal data that is unnecessary for the purposes of the processing (Reqs. 4.2, 4.3 and 4.5).

Furthermore, all partners have reported the use of either Articles 7 (a), (e) and (f) Directive 95/46/EC. Given ACDC’s purposes and the measures implemented by the partners as described in their input to the questionnaire, it appears that the personal data processing in the context of ACDC is legitimised by one or more of these specified grounds. Accordingly, Articles 6 and 7 Directive 95/46/EC appear to be satisfied and in this regard the ACDC solution appears to be a legally compliant one (Reqs. 3, 3.1, 3.3, 3.4 and 3.4.1).

1.3 Proportionality of processing

Subsection 3 of the questionnaire related to the proportionality of the processing operations performed by the partners. This subsection is clearly impacted by the results of all other sections. As such, given that KUL has concluded that partners have aimed to respect and comply with Articles 6 and 7 Directive 95/46/EC, this provides a degree of reassurance and clarity in relation to the proportionality of the processing. Of particular significance are those operations relying on Article 7 (e) and (f) Directive 95/46/EC given the associated balancing test necessary for their applicability (see in particular D1.8.1 and D1.8.2). Given that the focus of ACDC is the prevention, detection and mitigation of botnet attacks and threats, this purpose is adequate and specific and therefore provides significant weight in the balancing of the scales. However, the proportionality of actions is still key but it appears that the partners are very much aware of this, given their detailed replies to this subsection of the questionnaire.

1.4 Data subject rights

It must be understood that data subjects would have extremely limited interaction with the tools developed within the ACDC project. Indeed, as these tools are designed for industry partners and LEAs, citizens facing elements are limited. The supply of personal data is dependent on the sharing of information on behalf of the relevant partners. As such, data subject rights and specifically information relating to the types of information being gathered and the purposes to which it is put should be respected by the entity gathering and sharing the information in the first instance (i.e., the data controller). These data controllers are required to specify their data gathering operations and the security purposes for which this gathering takes place. Accordingly, the obligations contained in Articles 12 and 14 Directive 95/46/EC (see reqs. 5.1, 5.2 and 5.3) need to be monitored by each data controller. In their inputs, partners have referred to their respective privacy policies and the protections that they implement. For instance, partners specified the designation of a particular individual within the organisation in charge of data subjects' requests. Therefore, it appears that these requirements have also been met.

1.5 Security of processing

The final subsection related to the security and confidentiality of the personal data processing operations conducted during the project. As described above, this relates in particular to Article 17 Directive 95/46/EC and Article 4 e-Privacy Directive and therefore requirement 6 as represented in the table in Annex 1. In response to this requirement, partners noted in their inputs that they comply with the state of the art and as such the obligations as specified in the relevant Articles outlined above. For a more detailed description of the implemented measures, one should refer to the relevant deliverables, partners and the questionnaire responses in Annex 2.

Section 2 – The CCH

This section focuses specifically on the CCH as it is the key component of the ACDC project. The analysis is divided into two subsections. The first focusing on the CCH's compliance with the legal requirements as expressed supra. The second subsection analyses the terms of use as commented upon by KUL.

1.1 Compliance with legal requirements

In order to adequately assess the legal compliance of the CCH, this analysis will focus on the responses given by ECO (as the partner responsible for its implementation) in relation to the questionnaire. First and foremost, ECO notes that it processes personal data, more specifically IP Addresses. These IP addresses are used for statistical purposes and are also subject to an anonymisation process. These statistical and anonymisation procedures are defined and conducted by ECO and as such, ECO satisfies the definition of a data controller under Directive 95/46/EC. Accordingly, it is important to note how ECO has satisfied the legal requirements as contained in Directive 95/46/EC and in particular in relation to the data quality principles (Article 6 Directive 95/46/EC), the grounds for processing (Article 7 Directive 95/46/EC) and the security obligations (Article 17 Directive 95/46/EC). ECO has noted compliance with each of these requirements in the responses to the questionnaire. Indeed, to illustrate, ECO notes that it deletes personal data (storage in real-time) within 15 minutes and any data that was kept on a long-term basis is anonymised. This in compliance with the data minimisation, purpose limitation and secure deletion principles as contained in Article 6 Directive 95/46/EC. Moreover, ECO notes a specific ground for the personal data processing operations conducted in the CCH and that the state-of-the-art of security mechanisms have been implemented (in respect of Articles 7and 17 Directive 95/46/EC). Therefore, from the information provided, it can be concluded that the CCH is operating in a legally compliant manner. Indeed, the key balancing act between the protection of data subject and security interests has been acknowledged and the principle of proportionality has been taken into account.

1.2 Terms of Use

KUL provided ECO with feedback on the Terms of Use for the CCH. At first, the Terms of Use did not include a specific section dealing with the data protection requirements. Therefore, KUL stressed that more emphasis on the data protection requirements was crucial. As a result, ECO introduced a specific section titled ‘Data Protection’ in its Terms of Use. Furthermore, other partners were invited to reflect upon the matter and provide any comments or concerns. Partners that took advantage of this opportunity were INCIBE, EII and DFN-Cert. Finally ECO consolidated the comments and the current Terms of Use of the CCH state the following regarding data protection:

> *“The CCH distributes the data based on the defined Sharing-Policies, managed by the ECO. Besides of this the submitted data are distributed to signed-up network owners and CERTs for which they are responsible. Data will be stored 24 hours in plaintext. After this period the data are stored encrypted in a not re-producible way. To respect data privacy the most identifying fields within a data record are replaced by one or more artificial identifiers, or pseudonyms. The purpose is to render the data records less identifying and to keep the data in a form which is suitable for extensive analytics and processing.*
>
> *Every tool exchanging data with the CCH is connected via SSL. This ensures that all data are transferred securely by using encryption. The number of persons having direct access to the CCH is strictly limited to a very small number of defined persons. The security architecture is defined in D.1.2.2.”*

With regard to compliance with the data protection framework, the following can be said. First of all, the Terms of Use state that data will only be stored in plaintext for a 24h period. After this, ECO commits to storing the data in a non-reproducible way. To achieve this, ECO will implement encryption techniques as well as pseudonymisation. As such, ECO has taken efforts to comply with the limited retention principle, which states that data can only be stored for a limited period (i.e., for as long as is necessary to achieve the purpose for which the data were initially collected).[5] Since Directive 95/46/EC does not foresee in a fixed duration for legitimate data storage, it should be determined based on the specificities of the case. Furthermore, in order to comply with the limited retention principle, ECO will have to delete or anonymise the data once they are no longer necessary. As mentioned supra ECO has informed KUL that anonymisation in the long-term storage part of the CCH will be available, however, this component at the time of writing has not been finalised and no further details on the progress of the implementations was available.

Secondly, in relation to the requirement for secure personal data processing under Article 17 of Directive 95/46/EC (i.e., data controllers have to put in place technical and organisational measures that guarantee an optimal level of security to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access), a few commitments have been made by ECO. First, ECO commits to the secure transfer of information through the CCH. More in particular, ECO refers to the use of SSL connections whenever a tool exchanges data with the CCH. In essence, according to ECO, the secure exchange of information is ensured by using encryption techniques (as mentioned by the Terms of Use). Aside from this, according to the Terms of Use, ECO will strictly limit access to the CCH to a very small number of defined persons. In other words, ECO commits to implementing strict access controls within the CCH. This prevents unauthorised access to the data that are transferred or stored within the CCH.

[5] Article 6 (1) (e) Directive 95/46/EC.

CONCLUSION

Therefore, from the analysis conducted throughout this deliverable, it appears from the information provided by the partners that the ACDC prototype to be tested during the pilot is in compliance with the legal requirements that have been determined as being relevant. In conclusion, KUL envisages no major legal concern provided the inputs are indicative of the implemented ACDC solution.

Finally, reference should be made to D5.3 which focuses on the gaps that have been identified in the current legal framework. This deliverable provides detailed insights into the modifications necessary in order to facilitate the deployment of anti-botnet systems.

ANNEX 1 – TABLE OF REQUIREMENTS

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 exercise of official authority, the data controller must only act in the furtherance of this task.	In the context of ACDC, the protection of a public network could be deemed a task in the public interest. However, national DPA's should be consulted.	Article 7(e) Directive 95/46/EC
Req. 3.4	Legitimate	IF the data controller wants to	In the context of ACDC, the	Article 7(f)

	interest of the data controller	rely on its legitimate interest as a legal ground for processing, the data controller MUST have a legitimate interest in the data processing.	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.	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. 4.5.1	Secure deletion	The deleted personal data MUST NOT be retrievable.		
Req. 4.6	Automated individual decisions	Within the ACDC context, automated individual decisions relating to the data subject MUST		Article 15 Directive 95/46/EC

		NOT be made or supported, unless authorised by law.		
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

ANNEX 2 – RESPONSES TO THE QUESTIONNAIRE

1. ECO (DE)

Questionnaire on the CCH itself

A. Preliminary questions

A.7. Are you processing personal data? If so, what types of personal data are you processing? Yes / IP-Addresses

A.8. Are you planning to anonymise these personal data at any stage of the processing (e.g. after collection; before analysis; before sharing with the CCH)? YES, after sharing, but only for the long term storage. It has been implemented.

A.9. Are you sure it is not possible for your tool to achieve the same planned result/impact by anonymising these data after collection or before sharing it with the CCH? YES, if we anonymize the data, it is useless for about 90% of the project goals.

A.10. Is it possible to pseudonymise these data at any stage? YES

A.11. After reading section 2.4.6 of D1.8.1 (pp. 28-30), do you consider yourself a controller or a processor[6]? Data controller

A.12. If you consider yourself a processor, who would be the controller of the processing you are involved in? /

B. Purpose specification, legitimate grounds and data quality principles

B.9. What is the purpose of your tool? The central database for the entire project

B.10. How do you technically ensure the data are only used for that limited purpose? Storage in real-time, data gets deleted after 15 minutes

B.11. After reading section 2.4.9 and Chapter 4 of D1.8.1 (pp. 36-40, pp. 53-63), are any of the legitimation grounds of Article 7 of Data Protection Directive applicable to your tool[7]? How do you justify this? Article 7 (f) applies here. Purposes of the legitimate interests are fighting of cyber crime and misuse of data. The data subjects are interested in information regarding the misuse of their data

B.12. How can you prove you are collecting only the data which are necessary to achieve the purpose of the processing and that you cannot reach the same purpose with less or

[6] Data controller is a person or organisation who/which determines the purposes and means of data processing. 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. The legal distinction between 'controller' and 'processor' is not dependent on whether 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.

[7] Unambiguous consent (Article 7(a))
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;
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, for the performance of the contract;
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;
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)
This provision is often used by companies seeking for a legitimate excuse in the processing of personal data. 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.

anonymised data? We do no collect data, we only process the data provided by the users of the data base

B.13. How do you define how long the data should be stored? 15 minutes real-time

B.14. How will you ensure the data are deleted after storage period is finished? With a cron-job that deletes the data

B.15. How do you ensure the processed data (e.g. stored by your tool) is accurate and up to date? We only store data long-term if it has been anonymised.

B.16. Is there an entity or agent responsible for overseeing your processing, inside your institution? YES

C. Proportionality of processing

C.8. If you answered Art. 7(f) in B.3, what is the nature of the legitimate interest pursued by your tool (private or public)? Public interests: informing data subjects of misuse of their data, give options to take further actions for investigation, protections mechanism etc.

C.9. Who directly benefits from your tool (e.g. end users, ISPs, customers, etc.)? Are there any indirect beneficiaries (e.g. the organisation, ISPs, law enforcement)? As it is the central database, everybody participating in the project benefits from it

C.10. Have you identified the impact this tool has on fundamental rights such as privacy or confidentiality of communications (e.g. in case of mistakes, false positives, etc.)? Yes

C.11. Which measures have you taken to mitigate the impact of the tool on fundamental rights of citizens? We just implemented what we were allowed to, based on the legal analysis.

C.12. Do you process sensitive data (personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life)? No

C.13. Are you accountable for any damage caused by your tool? If not, who would be? No, each data provider is responsible for his own data

C.14. What additional safeguards have you put in place to prevent undue impact on the lives of citizens? None

D. Data Subjects' rights

D.4. Has your organization appointed someone to answer data subjects' requests? No, but we can if necessary.

D.5. How will you inform users about your processing, types of data involved and the identity of the third parties that may have access to their data? This should have been covered within the terms of use.

D.6. How do you empower data subjects to exercise their rights (objection, erasure and blocking) and enable mechanisms for them to access, modify, delete, transfer, or otherwise further process (or let third parties further process) their own data? We have no insight on what partners deliver, share, modify, delete, transfer or process

E. Security of processing

E.4. How do you ensure the security (integrity, availability and confidentiality) of the data processed by your tool? A penetration test will be done before the end of the project

E.5. Have you taken into account the sensitivity of the data processed and the impact on the lives of citizens in the case of a security breach before choosing for these mechanisms? Yes

E.6. Do they correspond to the state-of-the-art? Yes. The overall security architecture is described in deliverable D1.1.2 (Overall Software Architecture Description); the security architecture of the Centralized Clearing House has been included in deliverable D.1.2.2 (Specification of Tool Group 'Centralized Data Clearing House')

Tool INITIATIVE-S

A. Preliminary questions

A.1. Are you processing personal data? If so, what types of personal data are you processing?
- Within the initiative-s we collect Domain names and the E-Mail Addresses of the technical contact of the domain.

While the domain name is not a "private" data, the necessary E-Mail Address of the technical contact might be considered as a "private" Data.

A.2. Are you planning to anonymise these personal data at any stage of the processing (e.g. after collection; before analysis; before sharing with the CCH)?
- E-Mail Address won´t be shared with the CCH.
- Only domain name and Name of the malicious code (or code snipped) will be shared with the CCH.

A.3. Are you sure it is not possible for your tool to achieve the same planned result/impact by anonymising these data after collection or before sharing it with the CCH?
- See above: The only data we share is public data and nothing private

A.4. Is it possible to pseudonymise these data at any stage?
- No personal data is stored -> no anonymisation is needed.

A.5. After reading section 2.4.6 of D1.8.1 (pp. 28-30), do you consider yourself a controller or a processor?
Controller

A.6. If you consider yourself a processor, who would be the controller of the processing you are involved in?

B. Purpose specification, legitimate grounds and data quality principles

B.1. What is the purpose of your tool?
Purpose of Initiative-S is to check a website for malicious software and other malicious changes made to the website

B.2. How do you technically ensure the data are only used for that limited purpose?
Only communication of this tool goes from the INITIATIVE-S Servers to the OTRS Ticket System on the eco National Support Centre. Only Dataset transferred consists of a Ticket number (generated by the OTRS) , Domain-name, contact E-mail, Timestamp and Malware description which was found by the tool.

B.3. After reading section 2.4.9 and Chapter 4 of D1.8.1 (pp. 36-40, pp. 53-63), are any of the legitimation grounds of Article 7 of Data Protection Directive applicable to your tool? How do you justify this?
Owner / technical contact of the website must actively request, that his domain is scanned by Initiative-S. Before the registration it is clearly stated what we are doing and which data we are processing.
The Owner/Technical contact must perform a double opt in:
a) opt in at the website and choose on Contact E-Mail address for his website
b) answer to the registration email which is sent to this e-Mail address after opting in.
So all data that we collect falls under:

§7a) Member States shall provide that personal data may be processed only if:
(a) the data subject has unambiguously given his consent,
and ... Necessity in a contractual or pre-contractual context (Article 7(b))

B.4. How can you prove you are collecting only the data which are necessary to achieve the purpose of the processing and that you cannot reach the same purpose with less or anonymised data?

- We are only collecting a HTML snapshot of a given Website

This snapshot is automatically analysed and deleted in case our scanners find nothing. If we find malware or suspicious Code, only the suspicious Code-Snipped is copied with a timestamp of the finding.

B.5. How do you define how long the data should be stored?

Data is stored on the tool itself just to the next reporting period / Scan run.

B.6. How will you ensure the data are deleted after storage period is finished?

Database deletes all scan results automatically.

B.7. How do you ensure the processed data (e.g. stored by your tool) is accurate and up to date?

Technically

B.8. Is there an entity or agent responsible for overseeing your processing, inside your institution?

The owner/developer of the tool.

C. Proportionality of processing

C.1. If you answered Art. 7(f) in B.3, what is the nature of the legitimate interest pursued by your tool (private or public)?

C.2. Who directly benefits from your tool (e.g. end users, ISPs, customers, etc.)? Are there any indirect beneficiaries (e.g. the organisation, ISPs, law enforcement)?

End-customers -> owner of the domain

ISP / hosting companies which can be informed on Malware on their hosting service.

C.3. Have you identified the impact this tool has on fundamental rights such as privacy or confidentiality of communications (e.g. in case of mistakes, false positives, etc.)?

no impact

C.4. Which measures have you taken to mitigate the impact of the tool on fundamental rights of citizens?

C.5. Do you process sensitive data (personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life)?

No

C.6. Are you accountable for any damage caused by your tool? If not, who would be?

No. Tool is not considered to change anything- just grabs a website and informs per mail

C.7. What additional safeguards have you put in place to prevent undue impact on the lives of citizens?

None

D. Data Subjects' rights

D.1. Has your organization appointed someone to answer data subjects' requests?

we can be reached within the National Support Centre and we can answer all questions on the given Tools there,

furthermore see also : http://international.eco.de/legal-notice/privacy-policy.html

-> data protection officer, at the email address datenschutz@eco.de, the postal address: eco Verband der deutschen Internetwirtschaft e.V., Lichtstrasse 43h, 50825 Cologne, Keyword: "Data protection" or via fax under the number +49221 - 70 00 48-111.

D.2. How will you inform users about your processing, types of data involved and the identity of the third parties that may have access to their data?

a) per Mail
b) per phone if user calls the national Support Centre
https://www.initiative-s.de/de/datenschutz.html english : https://www.initiative-s.de/en/datenschutz.html

D.3. How do you empower data subjects to exercise their rights (objection, erasure and blocking) and enable mechanisms for them to access, modify, delete, transfer, or otherwise further process (or let third parties further process) their own data?

if someone wishes his data to be deleted, he can unsubscribe from the service, no data will ne stored then and no scans performed.
a data subject can also ask the national Support Centre to delete his ticket data.
a data subject can reach out for our data privacy officer.

E. Security of processing

E.1. How do you ensure the security (integrity, availability and confidentiality) of the data processed by your tool?

tool runs only on our own servers
communication with the tool only by ssl and by keybased authentification.

E.2. Have you taken into account the sensitivity of the data processed and the impact on the lives of citizens in the case of a security breach before choosing for these mechanisms?

no

E.3. Do they correspond to the state-of-the-art?

yes

National Support Centre

A. Preliminary questions

A.1 Are you processing personal data? If so, what types of personal data are you processing?

partly.
a) ISP can send us incidents -> no personal data is processed, just Incident number and a error description. No customer data is transmitted or stored at all.
b) enduser writes a Mail or creates a account on the NSC Forum – only Mail and username are stored

A.2 Are you planning to anonymise these personal data at any stage of the processing (e.g. after collection; before analysis; before sharing with the CCH)?

we are not processing or sharing personal data with the cch or anyone

A.3 Are you sure it is not possible for your tool to achieve the same planned result/impact by anonymising these data after collection or before sharing it with the CCH?

A.4 Is it possible to pseudonymise these data at any stage?

user is encouraged to register a pseudonym / user name in the Forum.

A.5 After reading section 2.4.6 of D1.8.1 (pp. 28-30), do you consider yourself a controller or a processor?

processor

A.6 If you consider yourself a processor, who would be the controller of the processing you are involved in?
in Case A1 a) ISP which is submitting a report
in Case A1 b) the user, who asks for help

B. Purpose specification, legitimate grounds and data quality principles

B.1. What is the purpose of your tool?
End User Help

B.2. How do you technically ensure the data are only used for that limited purpose?
no connection to outside
Ticket System is keeping logs of every access to a ticket

B.3. After reading section 2.4.9 and Chapter 4 of D1.8.1 (pp. 36-40, pp. 53-63), are any of the legitimation grounds of Article 7 of Data Protection Directive applicable to your tool? How do you justify this?
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)

B.4. How can you prove you are collecting only the data which are necessary to achieve the purpose of the processing and that you cannot reach the same purpose with less or anonymised data?
Data logs and Ticket examples from the national support Centre

B.5. How do you define how long the data should be stored?
by practical experience

B.6. How will you ensure the data are deleted after storage period is finished?
by technical measures – backup jobs which are automated

B.7. How do you ensure the processed data (e.g. stored by your tool) is accurate and up to date?
only data which is actively given to us can be stored. We cant make sure, the data our users are offering to us is correct

B.8. Is there an entity or agent responsible for overseeing your processing, inside your institution?
the support agents on the national support centre

C. Proportionality of processing

C.1. If you answered Art. 7(f) in B.3, what is the nature of the legitimate interest pursued by your tool (private or public)?
Legitimate interest is to provide help for affected customers- storing the data about incidents, so we can build up a incident history without having personal data stored.
example: Customer calls, Ticket is opened containing Ticket number – Malware findings, actions to solve the problem -→ no personal data at all is stored, Customer gets the Ticket number from the Support agent. Ticket closed.

C.2. Who directly benefits from your tool (e.g. end users, ISPs, customers, etc.)? Are there any indirect beneficiaries (e.g. the organisation, ISPs, law enforcement)?
ISP -> help in mitigation of malware
End User – gets help in cleaning his PC / website

C.3. Have you identified the impact this tool has on fundamental rights such as privacy or confidentiality of communications (e.g. in case of mistakes, false positives, etc.)?
no

C.4. Which measures have you taken to mitigate the impact of the tool on fundamental rights of citizens?

none necessary

C.5. Do you process sensitive data (personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life)?

no

C.6. Are you accountable for any damage caused by your tool? If not, who would be?

no user gets help on request. We are just providing manuals and software. The use of the manuals and tools is at the end user´s risk.

C.7. What additional safeguards have you put in place to prevent undue impact on the lives of citizens?

none

D. Data Subjects' rights

D.7. Has your organization appointed someone to answer data subjects' requests?

customer care agent (NSC)

and see also : http://international.eco.de/legal-notice/privacy-policy.html

-> data protection officer, at the email address datenschutz@eco.de, the postal address: eco Verband der deutschen Internetwirtschaft e.V., Lichtstrasse 43h, 50825 Cologne, Keyword: "Data protection" or via fax under the number +49221 - 70 00 48-111.

D.8. How will you inform users about your processing, types of data involved and the identity of the third parties that may have access to their data?

on the website: http://international.eco.de/legal-notice/privacy-policy.html

https://www.botfrei.de/datenschutz.html

no 3rd party tool has access to any data of the NSC

D.9. How do you empower data subjects to exercise their rights (objection, erasure and blocking) and enable mechanisms for them to access, modify, delete, transfer, or otherwise further process (or let third parties further process) their own data?

per contactiong our data protection officer, see above

E. Security of processing

E.1. How do you ensure the security (integrity, availability and confidentiality) of the data processed by your tool?

Own Server hardware by eco. Data is not shared in our organisation.

E.2. Have you taken into account the sensitivity of the data processed and the impact on the lives of citizens in the case of a security breach before choosing for these mechanisms?

yes

E.3. Do they correspond to the state-of-the-art?

yes. Website, Forum and Blog are secured with state of the art measures, administrative access from inside and outside eco´s network is only possible for selected persons.

2. Fraunhofer (FKIE)

HoneyUnit

A. Preliminary questions

A.1. Are you processing personal data?

No.

A.2. Are you processing any non-personal data?

Yes.

A.3. Have you tried to collect anonymised data?

No.

A.4. Are you sure it is not possible to achieve the same result by anonymising this data after collection?

Does not apply.

A.5. Is it possible to pseudonymise these data at any stage?

Does not apply.

A.6. Are you a controller or a processor?

As a tool provider, neither operating the tool nor receiving any data from it, we are neither.

A.7. If you consider yourself a processor, who is the controller of the processing you are involved in?

Does not apply.

A.8. Are the data Protection Directive and/or the e-Privacy Directive applicable to your case? Have you identified the national laws that have implemented these directives in your country?

The Data Protection Directive does not apply since we are not processing any personal data.

B. Purpose specification, legitimate grounds and data quality principles

B.1. What is the purpose of your tool?

To determine whether a given website tries to attack the client's web browser with a set of known attacks or whether there are indicators for attempts to attack the client with an unknown attack.

B.2. How do you technically ensure the data are only used for that limited purpose?

The result of the analysis is provided as a structured document that does not contain any personal data, hence there is no data that could be used for other purposes.

B.3. Are any of the legitimation grounds of Article 7 of data Protection Directive applicable to your tool? How do you justify this?

The HoneyUnit does not process any personal data, so the Data Protection Directive does not apply.

B.4. If not, are you aware this means you cannot process personal data lawfully?

Does not apply.

B.5. How can you prove you are keeping the data to a minimum and that you cannot reach the same purpose with less or anonymised data?

Does not apply.

B.6. How do you justify the storage period of these data?

The HoneyUnit does not store any data.

B.7. How will you ensure the data are deleted after the purpose is achieved? Can you define in concrete terms when this is going to take place?

The HoneyUnit does not store any data.

B.8. How do you ensure the data collected and analysed is absolutely accurate and up to date?

The HoneyUnit retrieves a web page for analysis directly or through a proxy server from the server that provides that page. Thus, it will always analyse the most recently published version of that page.

B.9. Is there an entity or agent responsible for overseeing your processing, inside your institution?

Since there is no processing inside our institution: No.

C. Proportionality of processing

C.1. Who is the legitimate interested party in your processing?

End users, staff acting on their behalf or their equipment provider (e.g. a company) as well as law enforcement who want do determine whether a given website attempts to attack the client's web browser.

C.2. What is the nature of the legitimate interest pursued by your tool?

The HoneyUnit serves to prevent infections, i.e. criminal attacks against IT systems.

C.3. Which fundamental rights does your tool act upon?

It supports users protecting their personal data, which would be compromised if their IT systems would be successfully attacked.

C.4. How do you inform users about the reasons you believe the purpose interests are not overridden by the data subject's interests or fundamental rights and freedoms?

The HoneyUnit does not interfere with any data subject's rights since it does not process any personal data.

C.5. Did you evaluate the actual impact of your tool in the lives of citizens?

We evaluated the effectiveness of the HoneyUnit in respect to whether it was able to distinguish malicious from non-malicious websites.

C.6. Did you evaluate the possible damages that could be caused to data subject in the case of false positives or any other mistake happens?

No.

C.7. How invasive is your tool and how do you respond to this?

The HoneyUnit does not process any personal data and is thus not invasive at all.

C.8. How sensitive the data being processed by your tool?

The HoneyUnit only processes data retrieved from a public web server. Thus, the data is considered not sensitive at all.

C.9. How do you empower data subjects to exercise their rights?

Data subject's rights are not influenced by the use of the HoneyUnit.

C.10. Will you enable mechanisms for the data subject to access, modify, delete, transfer, or otherwise further process (or let third parties further process) their own data?

Since there is no such data, there is no impetus for such a mechanism.

C.11. What additional safeguards have you put in place to prevent undue impact on the lives of citizens?

Does not apply.

C.12. Who is accountable for any damage caused by your tool?

The HoneyUnit is provided under an open source license that requires the person or entity using it to assume full accountability.

C.13. How do you plan to repair any damages caused by your tool?

Does not apply.

D. Data Subjects' rights

D.1. Who will be responsible for ensuring data subjects' rights in your processing?

Does not apply, the HoneyUnit does not process any personal data.

D.2. How transparent is your tool in terms of informing users about what you are doing?

Does not apply.

D.3. How will you inform users about the operation of your tool?

Does not apply.

D.4. How will you inform users about what types of data will be collecting and analysing?

Does not apply.

D.5. How will you inform users about the identity of the third parties that may have access to their data?

Does not apply.

D.6. How do you ensure users have the right to object to the processing?

Does not apply.

D.7. How do you ensure users have the right to have their data erased from your database and from the databases where you have send his/her data?

Does not apply.

E. Security of processing

E.1. How do you ensure the security of your tool and the data therein?

Partners deploying the HoneyUnit are advised to adopt standard security procedures with regard to the system the HoneyUnit is deployed on and run using an unprivileged user account.

E.2. Are these measures enough to secure the information processed?

Yes, in particular taking into account that no personal data is processed by the HoneyUnit.

E.3. Have you taken into account the sensitivity of the data processed and the impact on the lives of citizens in the case of a security breach before choosing for these mechanisms?

Yes.

E.4. Do they correspond to the state-of-the-art?

Yes.

PDF Scrutinizer

A. Preliminary questions

A.1. Are you processing personal data?

No.

A.2. Are you processing any non-personal data?

Yes.

A.3. Have you tried to collect anonymised data?

No.

A.4. Are you sure it is not possible to achieve the same result by anonymising this data after collection?

Does not apply.

A.5. Is it possible to pseudonymise these data at any stage?

Does not apply.

A.6. Are you a controller or a processor?

As a tool provider, neither operating the tool nor receiving any data from it, we are neither.

A.7. If you consider yourself a processor, who is the controller of the processing you are involved in?

Does not apply.

A.8. Are the data Protection Directive and/or the e-Privacy Directive applicable to your case? Have you identified the national laws that have implemented these directives in your country?

The Data Protection Directive does not apply since we are not processing any personal data.

B. Purpose specification, legitimate grounds and data quality principles

B.1. What is the purpose of your tool?

The PDF Scrutinizer determines whether a PDF file, provided either as reference to a local file or a link to a PDF file provided through a web server, tries to attack the client's PDF viewer with a set of known attacks or whether there are indicators for attempts to attack the viewer with an unknown attack.

B.2. How do you technically ensure the data are only used for that limited purpose?

The result of the analysis is provided as a structured document that does not contain any personal data, hence there is no data that could be used for other purposes.

B.3. Are any of the legitimation grounds of Article 7 of data Protection Directive applicable to your tool? How do you justify this?

The PDF Scrutinizer does not process any personal data, so the Data Protection Directive does not apply.

B.4. If not, are you aware this means you cannot process personal data lawfully?

Does not apply.

B.5. How can you prove you are keeping the data to a minimum and that you cannot reach the same purpose with less or anonymised data?

Does not apply.

B.6. How do you justify the storage period of these data?

Does not apply.

B.7. How will you ensure the data are deleted after the purpose is achieved? Can you define in concrete terms when this is going to take place?

The PDF Scrutinizer creates a temporary local copy when a PDF document is submitted for analysis providing a web address. This copy will be deleted as soon as the analysis is completed.

B.8. How do you ensure the data collected and analysed is absolutely accurate and up to date?

The PDF Scrutinizer either retrieves a document to analyse either directly or through a proxy server from the server that provides that document or is provided with a local copy of a document. In the former case, it analyses the most recently published version of that document, in the latter, it analyses the document provided by the user.

B.9. Is there an entity or agent responsible for overseeing your processing, inside your institution?

Since there is no processing inside our institution: No.

C. Proportionality of processing

C.1. Who is the legitimate interested party in your processing?

End users, staff acting on their behalf or their equipment provider (e.g. a company) as well as law enforcement who want do determine whether a given document attempts to attack the client's PDF viewer.

C.2. What is the nature of the legitimate interest pursued by your tool?

The PDF Scrutinizer serves to prevent infections, i.e. criminal attacks against IT systems.

C.3. Which fundamental rights does your tool act upon?

It supports users protecting their personal data, which would be compromised if their IT systems would be successfully attacked.

C.4. How do you inform users about the reasons you believe the purpose interests are not overridden by the data subject's interests or fundamental rights and freedoms?

The PDF Scrutinizer does not interfere with any data subject's rights since it does not process any personal data.

C.5. Did you evaluate the actual impact of your tool in the lives of citizens?

We evaluated the effectiveness of the PDF Scrutinizer in respect to whether it was able to distinguish malicious from non-malicious PDF documents.

C.6. Did you evaluate the possible damages that could be caused to data subject in the case of false positives or any other mistake happens?

No.

C.7. How invasive is your tool and how do you respond to this?

The PDF Scrutinizer does not process any personal data and is thus not invasive at all.

C.8. How sensitive the data being processed by your tool?

The PDF Scrutinizer only processes data retrieved from a public web server or directly provided by its user as a local file. In the first case, the data is considered not sensitive at all. In the second case, it is up to the user providing the document to take the necessary precautions to protect the file she or he provides.

C.9. How do you empower data subjects to exercise their rights?

Data subject's rights are not influenced by the use of the PDF Scrutinizer.

C.10. Will you enable mechanisms for the data subject to access, modify, delete, transfer, or otherwise further process (or let third parties further process) their own data?

Since there is no such data, there is no impetus for such a mechanism.

C.11. What additional safeguards have you put in place to prevent undue impact on the lives of citizens?

Does not apply.

C.12. Who is accountable for any damage caused by your tool?

The PDF Scrutinizer is provided under an open source license that requires the person or entity using it to assume full accountability.

C.13. How do you plan to repair any damages caused by your tool?

Does not apply.

D. Data Subjects' rights

D.1. Who will be responsible for ensuring data subjects' rights in your processing?

Does not apply, the PDF Scrutinizer does not process any personal data.

D.2. How transparent is your tool in terms of informing users about what you are doing?

Does not apply.

D.3. How will you inform users about the operation of your tool?

Does not apply.

D.4. How will you inform users about what types of data will be collecting and analysing?

Does not apply.

D.5. How will you inform users about the identity of the third parties that may have access to their data?

Does not apply.

D.6. How do you ensure users have the right to object to the processing?

Does not apply.

D.7. How do you ensure users have the right to have their data erased from your database and from the databases where you have send his/her data?

Does not apply.

E. Security of processing

E.1. How do you ensure the security of your tool and the data therein?

Partners deploying the PDF Scrutinizer are advised to adopt standard security procedures with regard to the system the PDF Scrutinizer is deployed on and run using an unprivileged user account.

E.2. Are these measures enough to secure the information processed?

Yes, in particular taking into account that no personal data is processed by the PDF Scrutinizer.

E.3. Have you taken into account the sensitivity of the data processed and the impact on the lives of citizens in the case of a security breach before choosing for these mechanisms?

Yes.

E.4. Do they correspond to the state-of-the-art?

Yes.

3. INCIBE

TOOL: CONAN MOBILE (COM)

A. Preliminary questions

Are you processing personal data? If so, what types of personal data are you processing?

Now in production:

Device serial number

Next version:

IP: Public IP address of the mobile device, if a security threat is detected. Blacklist of IPs considered malicious.

Device serial number

Are you planning to anonymise these personal data at any stage of the processing (e.g. after collection; before analysis; before sharing with the CCH)?

Yes.

Now in production:

Device serial number is hashed before being stored.

Next version:

IP addresses (origin of connection to COM server) are not stored, only used to extract country code and ASN in order to get stats of the service.

IP addresses in blacklist are hashed before sending to client.

Device serial number is hashed before being stored.

Are you sure it is not possible for your tool to achieve the same planned result/impact by anonymising these data after collection or before sharing it with the CCH?

Is it possible to pseudonymise these data at any stage?

After reading section 2.4.6 of D1.8.1 (pp. 28-30), do you consider yourself a controller or a processor?

INTECO is a controller.

If you consider yourself a processor, who would be the controller of the processing you are involved in?

N/A

B. Purpose specification, legitimate grounds and data quality principles

What is the purpose of your tool?

The general description of the tool Conan can be found in the document "D2.3 Technology Development Framework" (pages 66 and 108) which is currently available on the workspace:

https://workspace.acdc-project.eu/index.php?c=files&a=file_details&id=2379

Also, information can be found on the ACDC Community Portal.

In short, Conan is an end user application for Android devices that helps users to know the security state of the device configuration and installed apps, through three main activities: configuration devices analysis, analysis of installed applications and use of proactive services.

More information has been sent to KUL on the document:

ACDC_LegalRequirements_UseCases_INTECO.doc

How do you technically ensure the data are only used for that limited purpose?

Conan Mobile is under the scope of our ISMS (Information Security Management System). INTECO's processes and systems are certified under ISO 27001 that includes technical security measures to be legal compliant, specifically with personal data processing. (See http://www.inteco.es/what_is_inteco/como_trabajamos_en/)

Some examples of these measures are:

Access Control to the data stored and authorization by roles in server

Encrypted communications (HTTPS) between client and server

Also, security audits are performed to ensure the effectiveness of the measures implemented.

After reading section 2.4.9 and Chapter 4 of D1.8.1 (pp. 36-40, pp. 53-63), are any of the legitimation grounds of Article 7 of Data Protection Directive applicable to your tool? How do you justify this?

7(e), INTECO is a National Governmental CERT.

How can you prove you are collecting only the data which are necessary to achieve the purpose of the processing and that you cannot reach the same purpose with less or anonymised data?

N/A. Data is anonymised

How do you define how long the data should be stored?

Conan Mobile does not store personal data.

How will you ensure the data are deleted after storage period is finished?

N/A

How do you ensure the processed data (e.g. stored by your tool) is accurate and up to date?

We have internal quality and security mechanisms to assure this. The framework used manages the accurateness of processed data and in certain operations (for example, data synchronization from external sources => there are procedures of re-try in case of fault to be reduced the period without updated data, monitoring, alerts, etc).

Is there an entity or agent responsible for overseeing your processing, inside your institution?

Yes. INTECO has appointed a member of the Company Management Team as Head of Internal Security Management (RGI) who oversees it, ultimately, both corporate management for the protection of personal data as the maintenance and improvement of the Information Security Management System (ISMS) that has implemented and certified according to the UNE - ISO / IEC 27001: 2007.

This role (the RGI) assumes among its main functions: a) contact with the national bodies for the protection of personal data (AEPD), b) proper maintenance and updating of the Security Document, c) the registration of files in the RGPD (Data Protection General Register), d) the supervision of the audit processes both in the field of personal data protection management as part of information security management, e) the supervision of the processes of risks analysis and risks management, f) the implementation and supervision of action plans or risk treatment, etc.

C. Proportionality of processing

If you answered Art. 7(f) in B.3, what is the nature of the legitimate interest pursued by your tool (private or public)?

N/A. We are covered by 7(e). We are a governmental entity with competencies on cyberspace security.

Who directly benefits from your tool (e.g. end users, ISPs, customers, etc.)? Are there any indirect beneficiaries (e.g. the organisation, ISPs, law enforcement)?

Final users.

Have you identified the impact this tool has on fundamental rights such as privacy or confidentiality of communications (e.g. in case of mistakes, false positives, etc.)?

Low impact. INTECO has established a set of security guidelines and criteria required, prior to the put in production any tool, service or application.

This set of guidelines are contained in a formal procedure that is integrated into the corporate ISMS documentation structure, in which coverage is given to the high safety requirements contained in paragraph 14 of Annex A of the standard 27001, version 2013, based the acquisition, development and maintenance of information systems.

This procedure requires a prior evaluation of the tools, services or applications according to the set criteria to determine the level of criticality with respect to the security (confidentiality, integrity and availability). Also, it is not only applicable to new solutions but also in the maintenance cycle.

Which measures have you taken to mitigate the impact of the tool on fundamental rights of citizens?

INTECO has implemented and formally described in the Security Document, a set of technical and organizational measures to comply with the legislation regarding personal data safety measures.

These measures are based on the regulations implementing the Data Protection Act, which provides three different levels of protection based on the nature of the information processed (basic, intermediate and high).

These security measures describe the policies, standards and procedures applicable such as identification and authentication of users in information systems, access control, media management or backups among others.

Do you process sensitive data (personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life)?

NO.

Are you accountable for any damage caused by your tool? If not, who would be?

See section 1.4. – LIABILITY- in the Legal terms of use for CONAN Mobile that are available at:

http://www.inteco.es/OSI/Conan_Mobile_TOS/?realLang=en

What additional safeguards have you put in place to prevent undue impact on the lives of citizens?

As we have said, in addition to the set of security measures required by the legislation on personal data protection (See C.4), INTECO has implemented and certified a Information Security Management System (ISMS) according to ISO 27001: 2007 (currently being adapted to the new 2013 version of the standard).

This compromise of INTECO with information security, significantly increases the safety level of processes, services and information systems that are part of the scope of the System, including corporate applications.

The ISO 27001 standard allows INTECO to manage the risks trying to keep safe our services / assets and minimize the impact of the damage in case of any risk materialization.

D. Data Subjects' rights

D.1. Has your organization appointed someone to answer data subjects' requests?

Yes. In the Legal terms of use for CONAN Mobile that are available at (section 3 - Information Collection):

http://www.inteco.es/OSI/Conan_Mobile_TOS/?realLang=en

Free channels (email address) are given to answer data subjects requests.

D.2. How will you inform users about your processing, types of data involved and the identity of the third parties that may have access to their data?

In the Legal terms of use for CONAN Mobile that are available at (section 3 – Information Collection):

http://www.inteco.es/OSI/Conan_Mobile_TOS/?realLang=en

D.3. How do you empower data subjects to exercise their rights (objection, erasure and blocking) and enable mechanisms for them to access, modify, delete, transfer, or otherwise further process (or let third parties further process) their own data?

In the Legal terms of use for CONAN Mobile that are available at (section 3 - Information Collection):

http://www.inteco.es/OSI/Conan_Mobile_TOS/?realLang=en

E. Security of processing

E.1. How do you ensure the security (integrity, availability and confidentiality) of the data processed by your tool?

It is ensured by:

• Performing the process of risks analysis and management within our ISMS. Our strategic development process for cybersecurity technologies, including in the scope of the ISMS, is assessed annually at the stage of AGR under the MAGERIT methodology (using PILAR software), being evaluated the processes / services and systems that support them on the three dimensions of security.

• Conducting technical security audits of applications depending of the level of criticality, previously evaluated.

• Compliance with safety requirements established under the procedure of developing and maintaining software applications, among which include: source code security requirements, secure development OWASP, internal processing control, security among controlled environments promotion processes, software quality, etc.

E.2. Have you taken into account the sensitivity of the data processed and the impact on the lives of citizens in the case of a security breach before choosing for these mechanisms?

Yes. Risk analysis has been done and the appropriate measures have been adopted according our ISMS.

E.3. Do they correspond to the state-of-the-art?

Yes

TOOL: FLUX DETECT

A. Preliminary questions

A.1. Are you processing personal data? If so, what types of personal data are you processing?

IP: The public IP addresses that resolve a fast flux domain name. This IP, with the detection timestamp is necessary but not enough in any case to identify a data subject. Only ISPs can do that.

A.2. Are you planning to anonymise these personal data at any stage of the processing (e.g. after collection; before analysis; before sharing with the CCH)?

No, because this data is essential for the final purpose of the tool, that is disinfection of devices affected and this cannot be done without the full IP. This IP, with the detection timestamp is necessary but not enough in any case to identify a data subject. Only ISPs can do that.

A.3. Are you sure it is not possible for your tool to achieve the same planned result/impact by anonymising these data after collection or before sharing it with the CCH?

Yes, It is not possible as explained before.

A.4. Is it possible to pseudonymise these data at any stage?

A.5. After reading section 2.4.6 of D1.8.1 (pp. 28-30), do you consider yourself a controller or a processor?

INTECO is a controller.

A.6. If you consider yourself a processor, who would be the controller of the processing you are involved in?

N/A

B. Purpose specification, legitimate grounds and data quality principles

B.1. What is the purpose of your tool?

The general description of the tool Flux-Detect can be found in the document "D2.3 Technology Development Framework" (pages 66 and 106) which is currently available on the workspace:

https://workspace.acdc-project.eu/index.php?c=files&a=file_details&id=2379

In short, Flux-Detect is a tool that, for a given list of domains, detects those ones that are using Fast-Flux techniques (so we consider them as malicious) and monitors them until the fast flux activity ends. It also permits an active tracking of “bots” or public IP addresses behind those domains.

More information has been sent to KUL on the document:

ACDC_LegalRequirements_UseCases_INTECO.doc

B.2. How do you technically ensure the data are only used for that limited purpose?

All of our tools are under the scope of our ISMS (Information Security Management System). INTECO’s processes and systems are certified under ISO 27001 that includes technical security measures to be legal compliant, specifically with personal data processing. (See http://www.inteco.es/what_is_inteco/como_trabajamos_en/)

Some examples of these measures are:

- Access Control to the data stored and authorization by roles in server
- Encrypted communications (HTTPS) between client and server

Also, security audits are performed to ensure the effectiveness of the measures implemented.

B.3. After reading section 2.4.9 and Chapter 4 of D1.8.1 (pp. 36-40, pp. 53-63), are any of the legitimation grounds of Article 7 of Data Protection Directive applicable to your tool? How do you justify this?

7(e), INTECO is a National Governmental CERT.

B.4. How can you prove you are collecting only the data which are necessary to achieve the purpose of the processing and that you cannot reach the same purpose with less or anonymised data?

In this case, without the IP it is impossible to identify the end-user affected. INTECO must notify owner ISPs with their IP addresses list and the detection timestamp. Without this info is not possible to identify the end-user and notify him.

B.5. How do you define how long the data should be stored?

This is under study of our legal team. The data will be stored only the time allowed by law.

B.6. How will you ensure the data are deleted after storage period is finished?

Including the new policy in the storage policy and implementing the operative processes.

B.7. How do you ensure the processed data (e.g. stored by your tool) is accurate and up to date?

Continuous monitoring of fast flux domains.

B.8. Is there an entity or agent responsible for overseeing your processing, inside your institution?

Yes. INTECO has appointed a member of the Company Management Team as Head of Internal Security Management (RGI) who oversees it, ultimately, both corporate management for the protection of personal data as the maintenance and improvement of the Information Security Management System (ISMS) that has implemented and certified according to the UNE - ISO / IEC 27001: 2007.

This role (the RGI) assumes among its main functions: a) contact with the national bodies for the protection of personal data (AEPD), b) proper maintenance and updating of the Security Document, c) the registration of files in the RGPD (Data Protection General Register), d) the supervision of the audit processes both in the field of personal data protection management as part of information security management, e) the supervision of the processes of risks analysis and risks management, f) the implementation and supervision of action plans or risk treatment, etc.

C. Proportionality of processing

C.1. If you answered Art. 7(f) in B.3, what is the nature of the legitimate interest pursued by your tool (private or public)?

N/A. We are covered by 7(e). We are a governmental entity with competencies on cyberspace security.

C.2. Who directly benefits from your tool (e.g. end users, ISPs, customers, etc.)? Are there any indirect beneficiaries (e.g. the organisation, ISPs, law enforcement)?

Directly: ISPs, other CERTs

Indirectly (if ISPs notify them or if they implement security measures): final users and companies.

C.3. Have you identified the impact this tool has on fundamental rights such as privacy or confidentiality of communications (e.g. in case of mistakes, false positives, etc.)?

Low. Data processed by flux detect at INTECO cannot be associated to any final user, only the owner ISPs can do this.

INTECO has established a set of security guidelines and criteria required, prior to the put in production any tool, service or application.

This set of guidelines are contained in a formal procedure that is integrated into the corporate ISMS documentation structure, in which coverage is given to the high safety requirements contained in paragraph 14 of Annex A of the standard 27001, version 2013, based the acquisition, development and maintenance of information systems.

This procedure requires a prior evaluation of the tools, services or applications according to the set criteria to determine the level of criticality with respect to the security (confidentiality, integrity and availability). Also, it is not only applicable to new solutions but also in the maintenance cycle.

C.4. Which measures have you taken to mitigate the impact of the tool on fundamental rights of citizens?

INTECO has implemented and formally described in the Security Document, a set of technical and organizational measures to comply with the legislation regarding personal data safety measures.

These measures are based on the regulations implementing the Data Protection Act, which provides three different levels of protection based on the nature of the information processed (basic, intermediate and high).

These security measures describe the policies, standards and procedures applicable such as identification and authentication of users in information systems, access control, media management or backups among others.

C.5. Do you process sensitive data (personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life)?

NO.

C.6. Are you accountable for any damage caused by your tool? If not, who would be?

Under study.

C.7. What additional safeguards have you put in place to prevent undue impact on the lives of citizens?

As we have said, in addition to the set of security measures required by the legislation on personal data protection (See C.4), INTECO has implemented and certified a Information Security Management System (ISMS) according to ISO 27001: 2007 (currently being adapted to the new 2013 version of the standard).

This compromise of INTECO with information security, significantly increases the safety level of processes, services and information systems that are part of the scope of the System, including corporate applications.

The ISO 27001 standard allows INTECO to manage the risks trying to keep safe our services / assets and minimize the impact of the damage in case of any risk materialization.

D. Data Subjects' rights

D.1. Has your organization appointed someone to answer data subjects' requests?

No. QUESTION: ¿How can be done in this case? In this tool there is no way to identify data subjects. IP addresses are obtained from public DNS servers.

D.2. How will you inform users about your processing, types of data involved and the identity of the third parties that may have access to their data?

No. QUESTION: ¿How can be done in this case? In this tool there is no way to identify data subjects. IP addresses are obtained from public DNS servers.

D.3. How do you empower data subjects to exercise their rights (objection, erasure and blocking) and enable mechanisms for them to access, modify, delete, transfer, or otherwise further process (or let third parties further process) their own data?

No. QUESTION: ¿How can be done in this case? In this tool there is no way to identify data subjects. IP addresses are obtained from public DNS servers.

E. Security of processing

E.1. How do you ensure the security (integrity, availability and confidentiality) of the data processed by your tool?

It is ensured by:

• Performing the process of risks analysis and management within our ISMS. Our strategic development process for cybersecurity technologies, including in the scope of the ISMS, is assessed annually at the stage of AGR under the MAGERIT methodology (using PILAR software), being evaluated the processes / services and systems that support them on the three dimensions of security.

• Conducting technical security audits of applications depending of the level of criticality, previously evaluated.

• Compliance with safety requirements established under the procedure of developing and maintaining software applications, among which include: source code security requirements, secure development OWASP, internal processing control, security among controlled environments promotion processes, software quality, etc.

E.2. Have you taken into account the sensitivity of the data processed and the impact on the lives of citizens in the case of a security breach before choosing for these mechanisms?

Yes. Risk analysis has been done and the appropriate measures have been adopted according our ISMS.

E.3. Do they correspond to the state-of-the-art?

Yes

4. EII

EII

ACDC Community Portal

A. Preliminary questions

A.1. Are you processing personal data? If so, what types of personal data are you processing?

Yes, we are processing personal data. The personal data that we are processing are: e-mail address, full name, working position and other information related to the organization that a member of the Community Portal represents.

A.2. Are you planning to anonymise these personal data at any stage of the processing (e.g. after collection; before analysis; before sharing with the CCH)?

No, because we collect only the personally identifiable information needed in order to provide the member a unique account. Moreover, the personal data collected by us will not be analysed or shared with the CCH, or anyone else.

A.3. Are you sure it is not possible for your tool to achieve the same planned result/impact by anonymising these data after collection or before sharing it with the CCH?

No. As already mentioned we collect only the personally identifiable information needed in order to provide the member a unique account and to guaranty a safe service to other members. The information collected won't be shared at any stage and all personal information related to a member will be deleted once the account will be cancelled.

A.4. Is it possible to pseudonymise these data at any stage?

No, because the aim of the community portal is to link people from different organization to work together and share information. By pseudonymise people identity most of the trust that is achieved by people working together will be lost.

A.5. After reading section 2.4.6 of D1.8.1 (pp. 28-30), do you consider yourself a controller or a processor ?

We consider ourselves controllers.

A.6. If you consider yourself a processor, who would be the controller of the processing you are involved in?

-

B. Purpose specification, legitimate grounds and data quality principles

B.1. What is the purpose of your tool?

ACDC Community portal purposes are:

-Share information and knowledge, taking part to specific activities such as participating to experiments, providing information about initiatives, providing and acquiring information about tools & services to fight botnets;

-Improve communication with the other stakeholders active in the cyber security area;

-Access the Data Clearing House and be supported in the fight against botnets

B.2. How do you technically ensure the data are only used for that limited purpose?

Data are stored in the community portal database, that is only accessible for members through the community portal web application. Therefore the use of information is constrained to the functionalities implemented by the portal application.

B.3. After reading section 2.4.9 and Chapter 4 of D1.8.1 (pp. 36-40, pp. 53-63), are any of the legitimation grounds of Article 7 of Data Protection Directive applicable to your tool ? How do you justify this?

The legitimation ground applicable to Community Portal is unambiguous consent (Article 7(a)). A person, before joining the Community Portal, must authorize the treatment of the personal data accordingly to the ACDC Legal Terms, where we explain what type of data we collect, why, who will have access to these data and under which conditions and for how long we retain these data.

B.4. How can you prove you are collecting only the data which are necessary to achieve the purpose of the processing and that you cannot reach the same purpose with less or anonymised data?

The purpose of the processing is to enable people of the ACDC community to work together. For this reason we need to identify the community participants (by their name and organisation information) and be able to send them notifications (by their email address) This would not be possible with less or anonymised data.

B.5. How do you define how long the data should be stored?

As mentioned in the ACDC Legal Terms, the data will be stored as long as a person is member of ACDC Community Portal. Once the account will be cancelled, all the information related to the account, including personal information, will be deleted.

B.6. How will you ensure the data are deleted after storage period is finished?

The data are deleted by the automatic process linked to the account deletion functionality that is implemented in the community portal web application.

B.7. How do you ensure the processed data (e.g. stored by your tool) is accurate and up to date?

As mentioned in the Legal terms, the processed data is shared directly by the individuals and it is their responsibility to provide accurate and up to date information:

“As a registered representative to the Community Portal, you agree to:

(a) provide true, accurate, current, and complete information about yourself and about the organisation you are representing as prompted by the Community Portal application form (such information hereinafter being the "Application Data"),

(b) maintain and promptly update the Application Data to keep it true, accurate, current, and complete. “

B.8. Is there an entity or agent responsible for overseeing your processing, inside your institution?

The Community Portal is run by EII, under the responsibility of ECO, which oversees the process.

C. Proportionality of processing

C.1. If you answered Art. 7(f) in B.3, what is the nature of the legitimate interest pursued by your tool (private or public)?

-

C.2. Who directly benefits from your tool (e.g. end users, ISPs, customers, etc.)? Are there any indirect beneficiaries (e.g. the organisation, ISPs, law enforcement)?

ACDC Community Portal is open to public and private organisations that have a legal representation in Europe (including EEA/EFTA and neighbouring countries). In certain cases, non-legal bodies may be accepted into the portal. ACDC is not open to individuals – natural persons, but to organisations which would nominate one or more individuals to represent them in ACDC Community Portal.

C.3. Have you identified the impact this tool has on fundamental rights such as privacy or confidentiality of communications (e.g. in case of mistakes, false positives, etc.)?

Given the tool purposes (introduced in section B) the impact on fundamentals rights will be very limited to negligible. Moreover, the email address used to register in the portal is the work email address of the user, so having minimum impact on user private life and confidentiality of his communications.

C.4. Which measures have you taken to mitigate the impact of the tool on fundamental rights of citizens?

No specific measures as the impact is negligible.

C.5. Do you process sensitive data (personal data revealing racial or ethnic origin,

political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life)?

No

C.6. Are you accountable for any damage caused by your tool? If not, who would be?

The ACDC Community Portal is under the responsibility of ECO, therefore ECO is accountable for any damage caused by the portal.

C.7. What additional safeguards have you put in place to prevent undue impact on the lives of citizens?

No specific safeguards as the impact on citizens lives is negligible.

D. Data Subjects' rights

D.1. Has your organization appointed someone to answer data subjects' requests?

Yes, all the questions or comments regarding the protection of privacy are handled by Peter Meyer, as mentioned in the Legal Terms.

D.2. How will you inform users about your processing, types of data involved and the identity of the third parties that may have access to their data?

The users are informed about the process, types of data and the identity of third parties since the beginning, through the Legal Terms, that users must accept before joining the Portal. Any changes to the Legal Terms will be notified to the members via a suitable announcement on the ACDC Community Portal. The substantial changes regarding the rights and obligations of the members will be presented in detail in the announcement.

D.3. How do you empower data subjects to exercise their rights (objection, erasure and blocking) and enable mechanisms for them to access, modify, delete, transfer, or otherwise further process (or let third parties further process) their own data?

The members of the Community Portal have the possibility, through “my account”, to add, change and delete information regarding the organisation or personal information. If they have any questions, comments or complains regarding the rights to the protection of privacy or to the intellectual property they can reach ACDC by email or mail address. Each member has the right to ask the cancellation of their account and all the information related to the account, including personal information, will be deleted.

E. Security of processing

E.1. How do you ensure the security (integrity, availability and confidentiality) of the data processed by your tool?

All the data are stored in the portal database. The access to the database is constrained to the portal application only, and protected with authentication (username and password).

Access to the administrative interface of the community portal is again protected with authentication and limited to the administrators of the platform itself.

E.2. Have you taken into account the sensitivity of the data processed and the impact on the lives of citizens in the case of a security breach before choosing for these mechanisms?

Yes, the choice of maintaining minimal information for portal users as well as the fact that the information is limited to the working context of users makes the security measures adequate for the case.

E.3. Do they correspond to the state-of-the-art?

Yes, we deploy latest version available for the community platform, and we keep the underlying technology and libraries periodically updated.

5. FCCN CERT

A. Preliminary questions

Are you processing personal data? If so, what types of personal data are you processing?

Yes, IP and emails

Are you planning to anonymise these personal data at any stage of the processing (e.g. after collection; before analysis; before sharing with the CCH)?

No, we are not planning anonymise these data.

Are you sure it is not possible for your tool to achieve the same planned result/impact by anonymising these data after collection or before sharing it with the CCH?

No.

Is it possible to pseudonymise these data at any stage?

Conceptually it is possible, this only depends on the capabilities of the tool. We are installing two sensors (developed by project partners): A netflow sensor from Atos and a Honeypot Sensor from Carnet.

As such, our knowledge on the internals of the software goes as far as the documentation offers. The developers/project partners (Atos and Carnet) shall better answer this question.

After reading section 2.4.6 of D1.8.1 (pp. 28-30), do you consider yourself a controller or a processor?

A processor

If you consider yourself a processor, who would be the controller of the processing you are involved in?

The ACDC consortium

B. Purpose specification, legitimate grounds and data quality principles

What is the purpose of your tool?

This is not our tool. They were installed in order to participate in the project experiences.

Netflow sensor for behavioural analysis (from Atos): This type of sensors analyse, primarily, Netflow traffic data generated by routing and switching devices that are Netflow-capable (e.g. CISCO, Adtran, NEC, etc). But also software capture tools, such as softflow or nProbe, are able to sniff the network traffic and produce an output in Netflow format that can be analysed by these sensors. The analysis of Netflow data aims at identifying botnets by discovering anomalous behaviour in the network traffic. Botnets detected by these sensors normally compromise a vulnerable router or switch device (usually not properly configured). Other botnet types can be detected by observing http headers in the Netflow data, allowing the identification of malware distribution content web servers.

Spamtrap virtual appliance from (Carnet) receives spam e-mail sent to dedicated addresses(honeytokens) scattered across web sites. Addresses should be hidden from view for normal users, yet remain visible only to harvesters. Honeypot virtual appliance containing Glaspot honeypot which catches self-spreading malware and malware downloaded from malicious web sites in web site attacks. The data about attacks is stored in a temporary database in the appliance from which is regularly pulled by mediation server.

How do you technically ensure the data are only used for that limited purpose?

We will only deploy this tool after we have been assured that the tool will only process the data necessary for its purpose.

We are installing two sensors (developed by project partners): A netflow sensor from Atos and a Honeypot Sensor from Carnet.

As such, our knowledge on the internals of the software goes as far as the documentation offers. The developers/project partners(Atos and Carnet) shall answer this question.

After reading section 2.4.9 and Chapter 4 of D1.8.1 (pp. 36-40, pp. 53-63), are any of the legitimation grounds of Article 7 of Data Protection Directive applicable to your tool? How do you justify this?

Yes, Article 7 e) and f). CERT.PT's mission is to contribute to the national cibersecurity. This is achieved by coordinating security incidents resolution, producing security related alerts and recommendations and promoting a cybersecurity culture in Portugal. For this purpose CERT.PT:

Provides support to computer users in the resolution of computer security incidents, advising procedures, analyzing artifacts and coordinating with relevant stakeholders;

Gathers and disseminates information related to new security vulnerabilities and makes recommendations for potential security risks and malicious activities underway to build awareness of security among computer users;

CERT.PT also provides the service of coordinating the response to incidents within the national territory and in particular to those CSIRTS with which it has formal agreements.

How can you prove you are collecting only the data which are necessary to achieve the purpose of the processing and that you cannot reach the same purpose with less or anonymised data?

The answer to this question should be answered by the controller.

How do you define how long the data should be stored? ???(guardada onde? localmente?)

We can define how long the data could be stored for locally data, but not for the data stored in CCH.

We are installing two sensors(developped by project partners): A netflow sensor from Atos and a Honeypot Sensor from Carnet.

As such, our knowledge on the internals of the software goes as far as the documentation offers. The developpers/project partners(Atos and Carnet) shall better answer this question.

How will you ensure the data are deleted after storage period is finished?

We are responsible by the data stored locally, but not by the data stored in CCH, so we can easily delete the data, based in what was defined.

How do you ensure the processed data (e.g. stored by your tool) is accurate and up to date?

We are installing two sensors(developped by project partners): A netflow sensor from Atos and a Honeypot Sensor from Carnet.

As such, our knowledge on the internals of the software goes as far as the documentation offers. The developpers/project partners(Atos and Carnet) shall answer this question.

Is there an entity or agent responsible for overseeing your processing, inside your institution?

Yes, the cert team will be responsible for making quality auditory

C. Proportionality of processing

If you answered Art. 7(f) in B.3, what is the nature of the legitimate interest pursued by your tool (private or public)?

Public, we are a National Cert, our interest is to protect our constituent community, and this kind of tools can help in this area.

Who directly benefits from your tool (e.g. end users, ISPs, customers, etc.)? Are there any indirect beneficiaries (e.g. the organisation, ISPs, law enforcement)?

Currently, a limited and controlled group of academic community. In the future, all the Portuguese internet community.

Have you identified the impact this tool has on fundamental rights such as privacy or confidentiality of communications (e.g. in case of mistakes, false positives, etc.)?

There is two factor to be considered: The data collected (emails, Ips) and the other factor, what is being done with this data and this we cannot control.

We are installing two sensors (developed by project partners): A netflow sensor from Atos and a Honeypot Sensor from Carnet.

As such, our knowledge on the internals of the software goes as far as the documentation offers. The developers/project partners(Atos and Carnet) shall give a better answer to this question.

Which measures have you taken to mitigate the impact of the tool on fundamental rights of citizens?

We consulted our legal department to ensure that there is legal basis to store the data in question

Do you process sensitive data (personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life)?

No

Are you accountable for any damage caused by your tool? If not, who would be?

Accountable or liable??

What additional safeguards have you put in place to prevent undue impact on the lives of citizens?

The additional safeguards will be taken if necessary and defined by the project

D. Data Subjects' rights

Has your organization appointed someone to answer data subjects requests?

Our legal department

How will you inform users about your processing, types of data involved and the identity of the third parties that may have access to their data?

FCCN/Cert.pt never knows who the final owner of the data is. The objective is to provide the data available to the correspondent ISP

How do you empower data subjects to exercise their rights (objection, erasure and blocking) and enable mechanisms for them to access, modify, delete, transfer, or otherwise further process (or let third parties further process) their own data?

Nothing is planned regarding this.

E. Security of processing

How do you ensure the security (integrity, availability and confidentiality) of the data processed by your tool?

These sensors are installed behind FCCN/CERT.PT infrastructure and will be covered by our security policy.

Have you taken into account the sensitivity of the data processed and the impact on the lives of citizens in the case of a security breach before choosing for these mechanisms?

Yes, this information will be treated at the same level as the other sensitive information processed by FCCN / Cert.PT

Do they correspond to the state-of-the-art?

We only are responsible for the state-of-the-art of the infrastructure where the tools are hosted, but not by the software component developed by others.

6. SIGNALSPAM (FR)

A. Preliminary questions

A.1. Are you processing personal data? If so, what types of personal data are you processing?

Yes. Signal Spam is processing spam reports – e-mails – and all related data (IP addresses, e-mails addresses, names, attached documents, URL, …)

A.2. Are you planning to anonymise these personal data at any stage of the processing (e.g. after collection; before analysis; before sharing with the CCH)?

Data is anonymised depending on who it is transferred to (whether it is the e-mail sender through a feedback loop, or answering a judicial request for instance.

A.3. Are you sure it is not possible for your tool to achieve the same planned result/impact by anonymising these data after collection or before sharing it with the CCH?

Data shared with the CCH is currently: IP addresses of identified spambots, URL contained in identified phishing spam. No personal data is shared without a strong suspicion about the badness of the spam it was extracted from.

A.4. Is it possible to pseudonymise these data at any stage?

Not without hurting the usefulness of this particular data

A.5. After reading section 2.4.6 of D1.8.1 (pp. 28-30), do you consider yourself a controller or a processor ?

I understand Signal Spam as a controller, as we assign specific use for the data we provide to partners, although some of these partners may have a hand on determining the usage of the data

A.6. If you consider yourself a processor, who would be the controller of the processing you are involved in?

B. Purpose specification, legitimate grounds and data quality principles

B.1. What is the purpose of your tool?

The tools aim at collecting spam reports from end customers

B.2. How do you technically ensure the data are only used for that limited purpose?

Signal Spam is responsible for the development of all the feeds configured for partners, and therefore controls the uses for every partner. The French Data Protection authority, as a member of Signal Spam's Board of Administrators, oversees these aspects. Technically, feeds are limited to the necessary and sufficient data enabling the partner to take the required action.

B.3. After reading section 2.4.9 and Chapter 4 of D1.8.1 (pp. 36-40, pp. 53-63), are any of the legitimation grounds of Article 7 of Data Protection Directive applicable to your tool ? How do you justify this?

End customers need to create an account and agree to terms of uses stating how the data is exploited

B.4. How can you prove you are collecting only the data which are necessary to achieve the purpose of the processing and that you cannot reach the same purpose with less or anonymised data?

Signal Spam collects spam reports, as a raw collector of data, and then refines the data for its members. The purpose described in the terms of use is very general (tackling spam, whether it is commercial e-mails or sabot or phishing…

B.5. How do you define how long the data should be stored?

Signal Spam is authorized to store data as long as law enforcement may require to use it. However, length of time to store the data is specified for each partner.

B.6. How will you ensure the data are deleted after storage period is finished?

We don't. The responsibility is down to the partner. Any infringement by a member may resolve in the exclusion of the member.

B.7. How do you ensure the processed data (e.g. stored by your tool) is accurate and up to date?

B.8. Is there an entity or agent responsible for overseeing your processing, inside your institution?

The CNIL (Commission Nationale Informatique et Libertés – Data Protection Authority) oversees the processing.

C. Proportionality of processing

C.1. If you answered Art. 7(f) in B.3, what is the nature of the legitimate interest pursued by your tool (private or public)?

Tacking spam: a mission requiring both private and public partners, as well as the public.

C.2. Who directly benefits from your tool (e.g. end users, ISPs, customers, etc.)? Are there any indirect beneficiaries (e.g. the organisation, ISPs, law enforcement)?

Law Enforcement, ISP, ESP, End Customers, Security Companies are all direct beneficiaries.

C.3. Have you identified the impact this tool has on fundamental rights such as privacy or confidentiality of communications (e.g. in case of mistakes, false positives, etc.)?

Identified on a theoretical point of view: yes. However, we have never been confronted to any practical issue. Spam is viewed as a major breakdown on trust, privacy and confidentiality, and reporting spam aims at restoring trust and privacy.

C.4. Which measures have you taken to mitigate the impact of the tool on fundamental rights of citizens?

C.5. Do you process sensitive data (personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life)?

Not at all

C.6. Are you accountable for any damage caused by your tool? If not, who would be?

C.7. What additional safeguards have you put in place to prevent undue impact on the lives of citizens?

D. Data Subjects' rights

D.1. Has your organization appointed someone to answer data subjects' requests?

Ultimately, the President of Signal Spam can answer publicly this kind of request. On a day-to-day basis, the General Secretary answers end users questions

D.2. How will you inform users about your processing, types of data involved and the identity of the third parties that may have access to their data?

Signal Spam's website explains how the collection of data works and how the intelligence is extracted. We will also develop and "retro feedback loop" to specify end users what became of their report (what was the reported spam, who was it dispatched to, what kind of action did the report allowed or empowered…)

D.3. How do you empower data subjects to exercise their rights (objection, erasure and blocking) and enable mechanisms for them to access, modify, delete, transfer, or otherwise further process (or let third parties further process) their own data?

The whole point of Signal Spam is exactly to empower end users exercising their rights. As for their account, end users can erase them on the website.

E. Security of processing

E.1. How do you ensure the security (integrity, availability and confidentiality) of the data processed by your tool?

The database's architecture has been designed by Eric Freyssinet (head of the digital crimes unit at Gendarmerie Nationale) and Philippe Antuoro (responsible of abuses at one the major ISP in France), specifically to ensure the security. Users accounts details are stored in a separate database than the reports, and key authentication is required to link the data.

E.2. Have you taken into account the sensitivity of the data processed and the impact on the lives of citizens in the case of a security breach before choosing for these mechanisms?

Yes

E.3. Do they correspond to the state-of-the-art?

Yes