



HORIZON 2020

Digital Security: Cybersecurity, Privacy and Trust

H2020-DS-2015-1

DS-04-2015 Information driven Cyber Security Management

Grant n° 700176



Secure Information Sharing Sensor Delivery Event Network¹

Deliverable D2.2:

Preliminary legal requirements

Abstract: The following document examines the techniques used by SISSDEN in terms of their criminal law and data protection law admissibility. The document also looks at whether and how technologies developed by SISSDEN can be protected with the help of an intellectual property rights management.

¹The research leading to these results has received funding from the European Union Horizon 2020 Programme (H2020-DS-2015-1) under grant agreement n° 700176.

Contractual Date of Delivery	31 January 2017
Actual Date of Delivery	31 January 2017
Deliverable Security Class	Public
Editor	Stefan Hessel (Saarland University)
Contributors	Stefan Hessel, Ninja Marnau, Frederik Möllers, Stephanie Vogelgesang (Saarland University) Bryn Thompson (Cyberdefcon)
Internal Reviewers	Arturo Campos (Cyberdefcon)
Quality Assurance	Iwona Jarosz, Adam Kozakiewicz (NASK)

The *SISSDEN* consortium consists of:

Naukowa i Akademicka Sieć Komputerowa	Coordinator	Poland
Montimage EURL	Principal Contractor	France
CyberDefcon Limited	Principal Contractor	United Kingdom
Universitaet des Saarlandes	Principal Contractor	Germany
Deutsche Telekom AG	Principal Contractor	Germany
Eclxys SAGL	Principal Contractor	Switzerland
Poste Italiane – Società per Azioni	Principal Contractor	Italy
Stichting The Shadowserver Foundation Europe	Principal Contractor	Netherlands

Table of Contents

Table of Contents	3
1 Introduction.....	5
2 Scope of this document	5
3 Considered Techniques.....	6
3.1 Honeypots.....	6
3.1.1 Spampot.....	6
3.1.2 DDoS Honeypot.....	6
3.2 Sandboxes	7
3.2.1 Sample Data.....	8
3.3 Netflow Monitoring.....	8
3.3.1 Sample Data.....	8
3.4 Darknet Logs.....	9
3.4.1 Sample Data.....	9
3.5 Intrusion Detection	9
3.6 Portscans / Active Network Probes.....	9
3.6.1 Sample Data.....	10
3.7 Data sharing platform	10
3.7.1 Sharing data inside the project.....	10
3.7.2 Sharing data with ISPs/CERTs.....	10
3.7.3 Sharing data with the public.....	10
3.7.4 Sharing data with law enforcement agencies.....	11
4 Criminal law.....	11
4.1 DDoS Attack Monitoring.....	11
4.1.1 Possible criminal liability for DDoS attacks	11
4.1.2 Criminal liability for honeypot deployment	19
4.1.3 Use of honeypots with limited data rate	23
4.1.4 Risk considerations	24
4.2 Sandboxes	24
4.3 Port scans / Active Network Probes.....	24
5 Privacy and data protection law	25
5.1 Collection of personal data.....	25
5.1.1 According to Directive 95/46/EC	25
5.2 Data sharing platform	32
5.2.1 Data sharing inside the project.....	32

5.2.2	Data sharing with ISPs and CERTs.....	32
5.2.3	Data sharing with the public.....	33
5.2.4	Reference Data Set.....	33
5.2.5	Sharing data with law enforcement agencies.....	33
5.3	Data transfer to third non-EU states	34
5.3.1	EU-U.S. Privacy Shield.....	34
5.3.2	EU Standard Contractual Clauses.....	35
5.3.3	Binding Corporate Rules (BCR)	41
6	Intellectual Property Rights Management.....	43
6.1	Introduction to IPR Management	43
6.1.1	Patents.....	44
6.1.2	Trademarks	44
6.1.3	Industrial design.....	44
6.1.4	Trade secrets.....	44
6.1.5	Copyrights & related rights	45
6.1.6	Protection of layout-designs or topographies of integrated circuits	45
6.2	SISSDEN assets - a provisional IPR Audit	46
6.3	Risks to SISSDEN assets.....	48
6.4	Asset protection.....	49
6.4.1	Patent & IP searches relating to SISSDEN.....	49
6.4.2	Utility models.....	49
6.4.3	Trademarks	49
6.4.4	Others.....	49
6.4.5	Licensing of IP assets	50
6.5	Towards a business strategy	51
7	Glossary & Acronyms.....	53

1 Introduction

The SISSDEN project aims to collect information about malware infections and other network threat activities. To this end, SISSDEN will deploy an extensive sensor network, collecting and processing this threat information. Therefore, it is necessary to ensure legal compliance of our envisioned sensor network architecture and data processing as well as assess means to safeguard the consortium's intellectual property. In this deliverable we will provide an initial assessment of the criminal and data protection law implications as well as IPR management regarding the SISSDEN network.

2 Scope of this document

From a methodological point of view, this document first summarizes the techniques used by SISSDEN to subsequently subject them to a legal assessment. This approach was chosen in order to ensure that all essential characteristics of the technical infrastructure were adequately depicted. The abstraction is intended to ensure that small technical changes do not cause any changes in the legal assessment, while changes that differ greatly from our initial assumptions can be easily detected as they may require a new legal assessment. Although the data protection policies aim to be neutral to the underlying technology, a thorough understanding of the techniques deployed in SISSDEN will help to provide actionable legal guidelines.

At the level of data protection, this document examines mainly the Directive 95/46/EC (Data Protection Directive). However, the Directive will be replaced by the Regulation (EU) 2016/679 (General Data Protection Regulation - GDPR) on 25 May 2018. For this reason, the GDPR must also be taken into account as part of SISSDEN's legal consideration. The legal assessment of the GDPR compliance will be part of Deliverable D2.8. This document does not include a legal consideration of the Directive 2002/58 / EC (E-privacy Directive), as it applies only to publicly available electronic communications services (access providers) pursuant to Article 3 1) of Directive 2002/58 / EC.

At the level of criminal law, there are no EU wide regulations that apply to this project. However, within the scope of SISSDEN, it is not feasible to assess the national criminal law of *all* member states or even globally. Hence, we will focus on the national law of three member states chosen by the SISSDEN consortium as an initial example. In this report we will focus on German national law. We will extend this assessment to Dutch and Polish national law in Deliverable 2.8, given that these countries will play a fundamental role in deploying the SISSDEN architecture.

Furthermore, this document will discuss intellectual property laws. IPR laws are well-established through a system of patents, copyright and trademarks, formed to enable recognition of, or financial benefit, from an invention or creation. Successful IPR management can be complex and time-consuming. SISSDEN must ensure that assets created by the project are fully protected through the appropriate means. Assets brought to the project by partners also require careful rights administration. As a first step, an IP Audit will assess the current situation and aid in the planning of future IP protection as the project progresses through its various stages.

In relation to IPR, this document broadly describes the legal processes that the SISSDEN project must adhere to and the protections available to: a) minimize the risk of legal infringement of the IP of others, b) reduce the need to initiate legal action against others in order to preserve the rights of SISSDEN and its partners and, c) outlines why IP is a valuable business asset. Due to the

complexity of the law on IP protection, SISSDEN partners should decide if this is a task that can be effectively performed in-house or if the services of key specialists in this area should be employed.

3 Considered Techniques

This section gives an overview of the techniques that are relevant within the scope of SISSDEN and provides descriptions for each technique that can also be understood by non-technical readers.

3.1 Honeypots

SISSDEN will deploy a variety of different types of honeypots. These are intended to accept malicious traffic and malware aimed at exploiting the vulnerable system the honeypot emulates. The network of honeypots is described in detail in deliverable D3.3 Initial technical architecture. It will initially include: *glstopf*, *conpot*, *cowrie*, *honeytrap*, *elasticpot* and *dionaea*. Although each of these honeypots vary in the services that they emulate, they operate similarly from a legal point of view. They all passively collect the network traffic which attempts to access the emulated vulnerable service.

We will therefore focus our legal assessment on two types of honeypots that, first, exemplify the general legal assessment regarding their deployment and, second, have specific additional properties regarding criminal law and data protection law.

3.1.1 Spampot

Spampot is intended to collect spam (unsolicited bulk emails) in order to track active spam campaigns, their way of distribution, and their malicious attachments. The specific deployment within SISSDEN and the collected data is not yet agreed upon. As the data collection may include email addresses of spam victims it may require a detailed data protection assessment, which we will include in D2.8.

3.1.2 DDoS honeypot

Reflective Distributed Denial of Service (DDoS) attacks follow a common pattern: The attacker searches for so-called amplifiers on the Internet and abuses them to flood the victim's system with packets so the service is no longer reachable.

3.1.2.1 Source Address Spoofing

A big part of the DDoS attacks exploit the design of the stateless UDP protocol. The attacker abuses a property of the UDP transport protocol. UDP is itself connectionless, the packets are single datagrams with no reference to other packets. This means that each packet has to carry enough information for the receiving system to send an answer. In particular, each packet holds the IP address of the source system. Due to the fact that the receiving system cannot verify this address, it has to trust the sender to provide its correct IP address. However, it is also easily possible to provide a bogus source address so that the response will be sent to a third system instead of the original source. This third system has no means of identifying the original source other than trying to cooperate with the intermediate (second) system, since the packet it receives does not carry any information about the original source.

3.1.2.2 Amplifiers

First and foremost, an amplifier is a service which utilizes the UDP protocol to answer requests. Furthermore, it exhibits one important characteristic: The answer to a request is larger than the request itself (in terms of the amount of data) by the so-called amplification factor. This means that if a system sends requests to the amplifier at a rate of X , it will receive responses at a rate of (amplification factor) times X .

A DDoS attack now combines these two techniques. The attacker finds a suitable hosting provider where he/she can send crafted requests to (multiple) amplifiers using UDP packets and fakes the source IP address to be that of the victim's system. Each amplifier thus sends replies to the victim's system, clogging its Internet connection with useless data. Genuine packets from other clients cannot reach the victim's system and consequently the service is unreachable.

The honeypots used as part of the SISSDEN project are implemented as special cases of the aforementioned amplifiers. They offer the same basic functionality to an attacker as regular amplifiers, but employ rate limiting: Once they receive a certain number of packets containing the same (genuine or spoofed) source address within a fixed time frame (e.g., 10 packets within one minute), the source (victim) address is put on a blacklist and the honeypot stops sending replies to it for a certain duration (e.g., one day). By limiting the amount of network traffic an attacker can generate using a honeypot, the operators try to make sure that if the honeypot is discovered by scanners and later abused for a DDoS attack, its contribution to the overall traffic is minimal and that the honeypot is not ultimately responsible for the unreachability of the DDoS victim.

3.1.2.3 Sample Data

An acquired data set can contain the following data:

Nature of the data	Example
IP address of the victim	192.168.0.106
Protocol (ISO Layer 7)	DNS/NTP/SSDP/...
Timestamp of the attack	Thu 30 Jun 12:21:39 CEST 2016
Full packet	IP header, UDP header, payload (depending on the protocol)

3.2 Sandboxes

Analysing the behaviour of malware is a complex task. It is near impossible to determine the exact underlying algorithm of a malware sample as modern attacks often react to the conditions on the victim's system and sometimes come in a trimmed-down version which only receives the actual instructions later on from the attacker directly.

Because of this and the increasing complexity of malware, analysis tools often employ dynamic analysis, which means that the sample is executed and its behaviour observed during runtime. Among the tracked features are disk accesses, system APIs called by the malware, a screenshot of its visual appearance, and its network activity.

The technique used within the SISSDEN project focuses on analysing network activity of malware samples, as this activity is key to form a botnet. The samples are run on virtual machines (sandboxes) and any communication with other machines on the Internet is monitored and

captured by the host. When samples are executed all content, including the full requests as well as the responses of the contacted hosts is recorded for further processing. By doing so, the operators of the sandbox gain a detailed insight on the communication behaviour of the malware sample.

To counter the possibility that the malware forces the sandbox to perform attacks against other computers, protection and mitigation measures are included within the sandbox. For example, spam emails are captured and not sent and large network traffic volumes are throttled by applying rate limiting, similar to the DDoS honeypots mentioned above. While these measures does not guarantee full prevention of all possible attacks, it effectively reduces the impact of the most common ones.

3.2.1 Sample Data

An acquired data set can contain the following data:

Nature of the data	Example
Full program file	Locky.exe
Network communication as PCAP-file	IP header, UDP/TCP header, payload (depending on the malware)
Screenshot of the System	Image from Desktop with changed background after executing a CryptoLocker
System behaviour	List of API calls called by the malware, disk accesses, etc.

3.3 Network Traffic Monitoring

All connections to our network of honeypots will be centrally monitored by a Netflow collector and a network threat detection engine. Netflow is a technique to summarize and aggregate network communication to provide statistical data of certain communication streams. Netflow typically does not record the content (payload) of the communication.

Recording of full PCAPs is a more complex matter and is still being researched. The full analysis will be completed before such functionality is activated in the system and will be provided in deliverable D2.8.

The precise version of Netflow to be used in SISSDEN (v5 vs IPFIX) is still to be decided. However, in general, we expect a data format as follows.

3.3.1 Sample Data

Data captured through the use of Netflow collectors includes:

- Timestamps (start and end of stream)
- Source and destination IP address
- Source and destination UDP/TCP port numbers
- Protocol type
- Number of packets in flow, per direction
- Number of bytes in flow, per direction

The collected data and activity of the Netflow monitoring does not seem to exceed the data already collected directly by the honeypots. Nevertheless, as soon as the sensor network of SISSDEN will get deployed we will have to assess whether the collection of all Netflow data is proportionate to the purpose. The result of this assessment will be included in Deliverable D2.8.

3.4 Darknet Logs

SISSDEN considers to additionally monitor connection attempts on darknets. A darknet is a routed but unused IP address space that records all network traffic that arrives at any of the IP addresses that are part of the darknet. Darknets are purely passive and do not actively send out traffic. That is, they do not attempt emulation of any services nor do they respond to connection attempts in any way. Connection attempts to an IP serving as a Darknet will be logged through the supporting data capture mechanisms. Since this monitoring will only passively collect incoming traffic we do not see any relevance for a criminal law assessment. Data protection law regarding darknets will be investigated in Deliverable D2.8.

3.4.1 Sample Data

Data captured through the use of darknets includes:

- Packet timestamp
- Source and destination IP address
- Source and destination UDP/TCP port numbers
- TCP/UDP/ICMP and other protocol header information
- Any packet payload other than header (typically for UDP/ICMP)

3.5 Intrusion Detection

All connections to honeypots/darknets will be centrally monitored by instances of Suricata IDS and Montimage Monitoring Tool (MMT). It is an event-based monitoring solution that allows analysing network traffic according to a set of security properties. The main objective of these properties is to formally specify security goals and/or attack behaviour related to the application or protocol that is being monitored.

According to SISSDEN deliverable D3.3 Initial technical architecture the collected data not seem to exceed the data of Netflow monitoring and thus does not require additional legal assessment. Note that the probe does in fact receive the full content of the traffic, but the additional data is not recorded in any way.

3.6 Portscans / Active Network Probes

While the current architecture in SISSDEN does not foresee performing active network scans, we still discuss scans in case this technique will be added at a later point. For example, network scans might be used to scan the Internet for hosts that are vulnerable to amplification attacks. Such active network probes are composed of port scans and fingerprinting algorithms. Port scans are used to find vulnerable protocols like DNS, SNMP, SSDP, CharGen, QOTG, NTP and NetBIOS. For this reason the project partners may setup an Internet-wide scanner to identify amplifiers for the

mentioned protocols. To inform the administrators of the scanned hosts and give them the opportunity to exercise their right to opt-out from the scans, there will be a reverse DNS record pointing at a web server containing suitable information. To ease the remediation process, the project partners may collect information about each host by processing the traffic and extracting fingerprints. Fingerprints will be protocol-specific and assist to learn the underlying hardware, the system architecture and the operating system of a potentially vulnerable system.

3.6.1 Sample Data

An acquired data set can contain the following data:

Nature of the data	Example
Full response packet	For DNS: Forwarded response of the (SISSDEN-controlled) name server For NTP: Response to the command „ monlist “ (IP addresses of the last 100 clients; these are not relevant and will not be stored) For SSDP: All media device in the local network as name (e.g. “Medion TV”) Otherwise: indefinite data
IP address of the victim	192.168.0.106
Timestamp	Timestamp of the response

3.7 Data sharing platform

The project requires that partners share data among themselves and among third parties. A detailed legal assessment for all subsequent sharing use cases is included in Sections 5.2 and 5.3.

3.7.1 Sharing data inside the project

The project partners will have access to the raw data of the honeypots, sandboxes and active network probes. The raw data could include personal data (in a legal meaning). Therefore the project partners might need a legal reason for sharing personal data and it is possible that the data must be secured in a special way (cf. Sections 5.2 and 5.3).

3.7.2 Sharing data with ISPs/CERTs

SISSDEN aims to inform ISPs and CERTs about ongoing attacks and vulnerable systems that fall under their responsibility, which involves sharing data with ISPs/CERTs. This shared data can contain personal data, so that the project partners might need a legal reason for this data transfer.

3.7.3 Sharing data with the public

The project partners want to inform the public and other researchers about ongoing attacks and malware trends, as well as enable advanced security research with a curated data feed. To avoid the disclosure of personal data, such data feeds may need to be pseudonymized or even anonymized. Additionally, SISSDEN will also want to share reference data sets for research purposes which are not anonymized.

3.7.4 Sharing data with law enforcement agencies

It is imaginable that the project partners uncover a larger case of cybercrime activity and want to inform a law enforcement agency. For this case it would be useful to know on which legal basis this data exchange stands and which data can be given to the agency and which must not. National data retention requirements need also to be considered.

4 Criminal law

4.1 DDoS Attack Monitoring

In general, those who operate honeypots are not primarily a target of criminal prosecution. In fact, law accepts honeypots in order to monitor the network.² However, honeypots can be used to commit DDoS-Attacks, which are punishable by law.³

In other words, honeypots and DDoS-Attacks can be seen from different (legal) points of view. The problems associated with the use of honeypots is that these emulated systems offer the same functionality as "normal" amplifiers and therefore initially participate in the attack. This is why, first of all, it must be said which criminal offenses come into question when performing a DDoS-Attack (see 4.1.1). Subsequently the accomplice liability of the honeypot operator must be investigated (see 4.1.2).

4.1.1 Possible criminal liability for DDoS attacks

The increasing use of networked devices has also lead to an increased potential for DDoS attacks. Computers and computer networks are not only the instrument to perform attacks. Instead, they can also be target of different forms of digital attacks. With this in mind the German legislator extended the Criminal Code in the 1980s by introducing specific digital crime offenses such as Section 202a Criminal Code (data espionage), Section 303a Criminal Code (data tampering) or Section 303b of the Criminal Code (computer sabotage). These new criminal offenses, whose main goal is to fight digital crime, were continuously adapted and expanded during the following years.

4.1.1.1 *Computer sabotage, Section 303b of the Criminal Code*

Section 303b of the Criminal Code contains three variants of digital criminal offenses. With regard to DDoS attacks, the extension made in 2007 of Section 303b of the Criminal Code is of particular interest. Due to this new provision, Section 303b I Nr. 1 of the Criminal Code is to be applied (explicitly) to Denial-of-Service attacks.⁴

² Schweda, Bundestag verabschiedet IT-Sicherheitsgesetz, ZD-Aktuell 2015, 04737.

³ BT-Drs. 16/3656, p. 13.

⁴ BT-Drs. 16/3656, S. 13; Weidemann, in: BeckOK StGB, 32. Edition, 01.09.2016, Section 303b, Recital 10; Laue, Strafrecht und Internet – Teil 1, jurisPR-StrafR 13/2009 Annotation 2.

*Section 303b⁵**Computer sabotage*

(1) Whosoever interferes with data processing operations which are of substantial importance to another by

- 1. committing an offence under Section 303a(1); or*
- 2. entering or transmitting data (section 202a(2)) with the intention of causing damage to another; or*
- 3. destroying, damaging, rendering unusable, removing or altering a data processing system or a data carrier,*

shall be liable to imprisonment not exceeding three years or a fine.

(2) If the data processing operation is of substantial importance for another's business, enterprise or a public authority, the penalty shall be imprisonment not exceeding five years or a fine.

(3) The attempt shall be punishable.

(4) In especially serious cases under subsection (2) above the penalty shall be imprisonment from six months to ten years. An especially serious case typically occurs if the offender

- 1. causes major financial loss,*
- 2. acts on a commercial basis or as a member of a gang whose purpose is the continued commission of computer sabotage, or*
- 3. through the offence jeopardises the population's supply with vital goods or services or the national security of the Federal Republic of Germany.*

(5) Section 202c shall apply mutatis mutandis to acts preparatory to an offence under subsection (1) above.

a) Requirements of Section 303 b I Nr. 2 of the Criminal Code

On the basis of Section 303 b I Nr. 1 of the Criminal Code, anyone who interferes with data processing (Section 202a II of the Criminal Code) either by modifying or entering data, with the intention of causing disadvantages to others, will be punished. This only applies to data processing which is of substantial importance to some party.

The first aspect to be considered is the “transmitting data”. Transmission means any transmission of data from one computer to another within an existing network or telecommunication system.⁶ This criterion makes it clear that the scenarios must be examined exhaustively from a technical point of view. Only then is a methodical and complete legal investigation possible.

⁵ Translation of the German Criminal Code by Prof. Dr. Michael Bohlander https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html#p2482.

⁶ Weidemann, in: BeckOK StGB, 32. Edition, 01.09.2016, Section 303b, Recital 12; Fischer, Kommentar StGB, 64. Aufl. 2017, Section 202a, Recital 6.

During a DDoS attack, the server is overloaded in its response capacity due to a large number of received requests. As a consequence its recording and processing capacity is stressed out. Access to the server by legitimate users is thus blocked or at least impeded. Therefore the “sending of requests” (from the aggressor to the victim) is to be understood as a data transmission.

In most cases the intention to cause someone a disadvantage is also given. Disadvantage means the damage to legitimate interest, which do not have to be of an economic nature per se.⁷ Material damages or damages to the public image of the victim are possible.⁸ The main goal of these attacks is usually the damage, which the operator of the attacked system suffers from, if the attacker is successful.

A drastic deterioration of the system access or a (temporary) total breakdown of the web presence of a company, which promotes goods, offers services, informs, advises customers or provides some kind of customer service, would lead to considerable image damages and financial losses. It is exactly this motivation, which the perpetrator of the attack has (in most of the cases); hence he fulfils the subjective criterion of the case.

All varieties of Section 303b of the Criminal Code require a data processing of significant importance to someone, which is significantly disturbed. The term of “data processing” is to be interpreted broadly and covers not only the individual data processing, but also the further handling of data and its utilization.⁹ As a consequence, the totality of computational processes is covered.¹⁰ Websites are also included by this term: the user sends requests to the server; the server then processes them and replies back to the user. For this reason the criterion “Data processing” in terms of Section 303b I of the Criminal Code is fulfilled.¹¹

Furthermore the “processing of data” must be of substantial importance to another person. Trivial cases are therefore excluded from Section 303b I.¹² Whether a case is trivial has to be decided individually and cannot be determined with a general rule. However, a significant meaning is assumed when the respective task of the person or his organization is wholly or at least predominantly dependent on the operability of the data processing.¹³ This is typically assumed to be true in practical cases. The attacker’s goal is usually the disruption of data processing that serve an important purpose for the victim.¹⁴ This type of data processing typically falls under the criterion of “substantial”.¹⁵

The processing of data does not stop being important because the task it fulfils can be accomplished in some other way.¹⁶ In practice, such assurances, as well as ensuring functionality of the system during an ongoing attack, are very challenging. Measures must be taken ahead of

⁷ Fischer, Kommentar StGB, 64. Aufl. 2017, Section 303b, Recital 12a.

⁸ Ratkic, Denial-of-Service-Attacken im österreichischen und deutschen Strafrecht, Graz, 2014, 2.1.1.

⁹ BT-Drs. 10/5058, p. 35.

¹⁰ Fischer, Kommentar StGB, 64. Aufl. 2017, Section 303b, Recital 4.

¹¹ Fischer, Kommentar StGB, 64. Aufl. 2017, Section 303b StGB, Recital 4ff.

¹² BT-Drs. 16/3656, p. 13.

¹³ Fischer, Kommentar StGB, 64. Aufl. 2017, Section 303b, Recital 6.

¹⁴ OLG Frankfurt, Beschluss v. 22.5.2006 – 1 Ss 319/05 = MMR 2006, 547.

¹⁵ Heger, in: Lackner/Kühl, StGB, 28. Aufl. 2014, Section 303b, Recital 2.

¹⁶ Fischer, Kommentar StGB, 64. Aufl. 2017, Section 303b StGB, Recital 8.

time to be able to react appropriately towards an attack. In particular, restarting the system or resetting the Internet connection are not helpful.

As a consequence of the offence, the processing of data must suffer from a significant disturbance. A disturbance is given if the smooth processing of data is more than insignificantly impaired.¹⁷ Any non-trivial impairment of the functionality is sufficient.¹⁸ When it comes to a DoS attack, the service (e.g. website) is blocked, usually because of a massive data transmission.¹⁹ The system is flooded with information; hence it is overloaded and collapses. This flooding is also punishable according to Section 303b of the Criminal Code.

In order to not penalize every low or moderate impact, which an attack can cause, the malfunction of the data processing itself must be of significant importance.²⁰ This relevance threshold can already be reached if a single other possible data processing operation cannot be carried out because of the attack.²¹ This importance can thus be assumed in case of a DoS attack, which blocks other intended transmissions.

b) Requirements of Section 303 b I Nr. 1 of the Criminal Code

Section 303b I Nr. 1 is an extension (in German legal terms: qualification) of Section 303a of the Criminal Code.²² Section 303b I Nr. 1 of the Criminal Code requires that the offender significantly disturbs data processing, which is of substantial importance for another, by committing the criminal offence of Section 303a I of the Criminal Code. Therefore, the prerequisites of Section 303a of the Criminal Code have to be fulfilled.

Section 303a

Data tampering

(1) Whosoever unlawfully deletes, suppresses, renders unusable or alters data (section 202a (2)) shall be liable to imprisonment not exceeding two years or a fine.

(2) The attempt shall be punishable.

The “suppression” of data means that access to the data by authorized parties is prevented for more than an insignificant period of time, and that for this reason, they cannot be used (though their physical integrity is preserved).²³

One has to distinguish between the data of the service (for example, the website) and the users’ inputs. As a result of DoS attacks, which overload the Internet connection, the service is blocked. This means that only authorized persons with physical access to the server can access the data. “Small” websites of private persons can be stored on the PC, which would then act as a server. But

¹⁷ Fischer, Kommentar StGB, 64. Aufl. 2017, Section 303b StGB, Recital 9.

¹⁸ Wieck-Noodt, in: Münchener Kommentar zum StGB, 2. Aufl. 2014, Section 303b, Recital 19.

¹⁹ Laue, Strafrecht und Internet – Teil 1, jurisPR-StrafR 13/2009 Annotation 2.

²⁰ Hilgendorf/Valerius, Computer- und Internetstrafrecht, 2. Aufl. 2012, p. 180.

²¹ Stree/Hecker, in: Schönke/Schröder, StGB, 29. Aufl. 2014, Section 303b, Recital 9.

²² BT-Drs. 10/5058, p. 36.

²³ Fischer, Kommentar StGB, 64. Aufl. 2017, Section 303a StGB, Recital 10.

in most cases—especially when it comes to major website operators—the servers are located in a data centre, which they cannot access if the Internet connection is overloaded. Under these circumstances the service provider, who is the authorized entity, cannot access the data submitted by the users. The result is thus the suppression of that data.

It is disputed if the criterion of “suppression” is also fulfilled when the data is just temporarily inaccessible. The prevailing opinion in the literature assumes that it is.²⁴ On the other hand, the OLG Frankfurt differs from them because of the principle of legal certainty (Art 103 II GG).²⁵ According to the court, there must be other limiting evaluation criteria besides the time aspect: the extensiveness and intensity of the interference.

In any case, an attack that lasts for a long time constitutes a crime according to Section 303a I Nr 1 of the Criminal Code.

Furthermore Section 303a of the Criminal Code requires the right of disposal of the authorized party to be affected.²⁶ The accessibility of the website for third parties is not a crucial aspect for the data suppression. The decisive issue is the inability of the service provider to reach the data.²⁷ As said before, when it comes to large (website) operators, this is generally the case.

Next we will analyse the criterion of “rendering unusable”. This variant is relevant if the usability of the data is affected in such a manner that it can no longer fulfil its purpose.²⁸ An example mentioned in German legal literature is a software that stops functioning after a certain number of execution unless a new license key is entered.²⁹ If a DoS attack leads to a server overload and inaccessibility of the data provided by that server, this implies that the usage of the data (regarding to its intended purpose) is restricted. If the damage is of little impact, however, the criterion of being “rendered unusable” is not fulfilled.³⁰

The goal of a DDoS attack is to cause a malfunction of the target system by sending a large data volume. As a result, the perpetrator meets both criteria (suppressing data and rendering them unusable). Thus he commits an act that is punishable according to Section 303a of the Criminal Code. This result is not surprising. The legislator was aware that both criteria are not mutually exclusive.³¹ The intention was to close gaps in criminal liability. It is assumed that the remaining criterion of Section 303b I of the Criminal Code (namely, data processing of substantial importance) is fulfilled.

c) Requirements of Section 303 b I Nr 3 of the Criminal Code

Concerning Section 303 b I Nr 3 of the Criminal Code, the DoS attack does not meet all criteria. For Section 303 b I Nr 3 of the Criminal Code it is necessary that the perpetrator destroys, damages,

²⁴ Schönke/Schröder/Stree/Hecker StGB Section 303a Recital 6; Weidemann, in: BeckOK, Section 303a, Recital 10.2; Gercke, in: Spindler/Schuster, Recht der elektronischen Medien, 3. Aufl. 2015, Section 303a Recital 5.

²⁵ Anmerkung OLG Frankfurt/M, Beschluss v. 22.5.2006 – 1 Ss 319/05, MMR 2006, 546.

²⁶ Weidemann, in: BeckOK StGB, 32. Edition, 01.09.2016, Section 303a, Recital 5.

²⁷ Hilgendorf/Valerius, Computer und Internetstrafrecht, Recital 197.

²⁸ BT-Drs. 10/5058, p. 35.

²⁹ Würmeling, Einsatz von Programmsperren – Zivil- und strafrechtliche Aspekte, CR 1994, 592.

³⁰ Fischer, Kommentar StGB, 64. Aufl. 2017, Section 303a Recital 11.

³¹ BT-Drs. 10/5058, p. 35; Fischer, Kommentar StGB, 64. Aufl. 2017, Section 303a StGB, Recital 8.

renders unusable, removes or changes the data processing system. The currently prevailing view sees this criminal offence committed when the attack causes a direct damage to the hardware.³² However, this is not commonly the case for DoS attacks.

d) Requirements of Section 303 b II of the Criminal Code

The perpetrator commits the qualification of Section 303 b II of the Criminal Code when the data processing is done by another person's company, another person's enterprise or by an authority. This makes it clear that this paragraph contemplates two different types of victim groups. Paragraph one is dedicated to private persons and paragraph two is dedicated to other's companies, enterprises and authorities. In the second case, the law increases the sentence.

4.1.1.2 Data Espionage, Section 202 a of the Criminal Code

Section 202a

Data espionage

(1) Whosoever unlawfully obtains data for himself or another that were not intended for him and were especially protected against unauthorised access, if he has circumvented the protection, shall be liable to imprisonment not exceeding three years or a fine.

(2) Within the meaning of subsection (1) above data shall only be those stored or transmitted electronically or magnetically or otherwise in a manner not immediately perceivable.

Furthermore the perpetrator could be facing the penalty of Sections 202a, 202b and 202c of the Criminal Code. According to Section 202a I of the Criminal Code, it is a punishable offense to obtain access (for oneself or another person) to protected data without authorization by circumventing security measures.

However, DoS attackers do not penetrate the system. They just overload them and render them unreachable. By this action, the offender does not gain access to the data. This is why he is not liable to prosecution under the charge of Section 202a of the Criminal Code.

4.1.1.3 Data interception, Section 202 b of the Criminal Code

Section 202b

Data Interception

Whosoever unlawfully intercepts data (section 202a(2)) not intended for him, for himself or another by technical means from a non-public data processing facility or from the electromagnetic broadcast of a data processing facility,

³² Weidemann, in: BeckOK StGB, 32. Edition, 01.09. 2016, Section 303b, Recital 13; Fischer, Kommentar StGB, 64. Aufl. 2017, Section 303b StGB, Recital 13.

shall be liable to imprisonment not exceeding two years or a fine, unless the offence incurs a more severe penalty under other provisions.

Section 202 b of the Criminal Code incorporates a subsidiarity clause. This paragraph is not applied when the perpetrator's action faces other, higher penalties. Especially Section 202a of the Criminal Code replaces Section 202b.³³

As determined above, the criteria of Section 202a of the Criminal Code are not met by a DoS attacker. Section 202 b of the Criminal Code might therefore be applicable.

Section 202b addresses anyone who, without being authorized to do so, intercepts another person's data from a non-public data transfer or from electromagnetic emissions of a data processing system, by using technical tools. Eavesdropping (e.g. on phone calls) is also covered by Section 202 b of the Criminal Code.³⁴

However, the perpetrator of a DoS attack neither gets access to the data nor "eavesdrops". As a consequence, the criteria of Section 202 b of the Criminal Code are not fulfilled.

Because the perpetrator does not attempt to commit Section 202a of the Criminal Code or Section 202b, an investigation of a (possible) penalty under Section 202c does not have any relevance.

Section 202c

Acts preparatory to data espionage and phishing

(1) Whosoever prepares the commission of an offence under section 202a or section 202b by producing, acquiring for himself or another, selling, supplying to another, disseminating or making otherwise accessible

*1. passwords or other security codes enabling access to data (section 202a(2)),
or*

*2. software for the purpose of the commission of such an offence,
shall be liable to imprisonment not exceeding one year or a fine.*

(2) Section 149(2) and (3) shall apply mutatis mutandis.

4.1.1.4 Trespassing, Section 123 of the Criminal Code

Section 123

Trespassing

(1) Whosoever unlawfully enters into the dwelling, business premises or other enclosed property of another, or into closed premises designated for public

³³ BT-Drs. 16/3565, p. 11.

³⁴ BT-Drs. 16/3656, p. 11.

service or transportation, or whosoever remains therein without authorisation and does not leave when requested to do so by the authorised person, shall be liable to imprisonment not exceeding one year or a fine.

(2) The offence may only be prosecuted upon request.

DoS attacks could be considered as an offense to the property (trespassing). If an attacker obtains digital access to a website, he enters a private area and commits a “digital trespass”. Section 123 is a “classic” criminal sanction of the Criminal Code. This paragraph penalizes those who enter a residence or other enclosed property without authorization. According to the prevailing opinion in the literature this paragraph requires a physical transgression into a private area. Even unauthorized access to a web site does not meet this criterion, let alone the prevention of access by others. As a result, DoS attacks do not fall under Section 123 of the Criminal Code.

4.1.1.5 Blackmail, Section 253 of the Criminal Code

Section 253

Blackmail

(1) Whosoever unlawfully with force or threat of serious harm causes a person to commit, suffer or omit an act and thereby causes damage to the assets of that person or of another in order to enrich himself or a third person unlawfully shall be liable to imprisonment not exceeding five years or a fine.

(2) The act shall be unlawful if the use of force or the threat of harm is deemed inappropriate to the purpose of achieving the desired outcome.

(3) The attempt shall be punishable.

(4) In especially serious cases the penalty shall be imprisonment of not less than one year. An especially serious case typically occurs if the offender acts on a commercial basis or as a member of a gang whose purpose is the continued commission of blackmail.

The perpetrator can use the fact that the website is unavailable (as a consequence of sending a large data volume) as a means of pressure, in order to force the victim to make a payment. This would be considered as blackmail in the sense of Section 253 of the Criminal Code.

4.1.1.6 Other offenses

Damage to property according to Section 303 of the Criminal Code should also be considered. This could be the case, for example, if the attacker is pursuing the goal of overloading the Internet or network connection of a nuclear power plant, so that he can interfere with the control and thereby damage the reactor.

Section 303

Criminal damage

(1) Whosoever unlawfully damages or destroys an object belonging to another shall be liable to imprisonment not exceeding two years or a fine.

(2) Whosoever unlawfully alters the appearance of an object belonging to another substantially and permanently shall incur the same penalty.

(3) The attempt shall be punishable.

It is also conceivable that the perpetrator deliberately attacks a hospital in order to disrupt internal digital systems. Damage to life supporting systems, for example, could cause patients to suffer from physical injury or even lead to their death. Here, Section 223 of the Criminal Code would apply for bodily harm and Section 212 of the Criminal Code for homicide.

The attacker, however, does not always intend to harm his victim or to commit homicide. Would it be the case that someone ends up being injured or killed, the perpetrator would commit negligence in a personal injury (Section 229 of the Criminal Code) or negligent homicide (Section 222 of the Criminal Code).

Conclusion: The main perpetrator of a DDoS attack commits a criminal offence according to the German Criminal Code, Section 303b.

4.1.2 Criminal liability for honeypot deployment

From an objective point of view, the honeypot operator could be seen as someone who participates in DDoS attacks. In Germany there are two forms of participation during a criminal offense: either the person is the principal of the committed crime (Section 25 of the Criminal Code) or he is an accessory (Sections 26, 27 of the Criminal Code).

4.1.2.1 Perpetration and incitement

The honeypot neither performs this type of attack by his own nor incites others to do so. Therefore, the operator is neither a principal nor an indirect perpetrator of the crime according to Section 25 I of the Criminal Code.

Inciting a crime according to Section 26 of the Criminal Code requires a communication element between the author and the indirect perpetrator. It is necessary that the instigator influences the indirect offender to commit the crime. This communication element does not take place when it comes to a DDoS attack. A criminal responsibility as an instigator to a crime under Section 26 of the Criminal Code is therefore out of the question.

4.1.2.2 Accessory in computer sabotage, Section 303b I Nr. 2, 27 of the Criminal Code

However, the operator could be seen as an accessory or accomplice during the computer sabotage (Section 303b I Nr. 2, 27 of the Criminal Code). For this to be the case, the honeypot's operator

would need to have the intention to assist the (principle) perpetrator during the crime. The DoS attack itself is an illegal act under Section 303b I Nr 2 of the German Criminal Code (see above).

Section 27

Accessory

(1) Any person who intentionally assists another in the intentional commission of an unlawful act shall be convicted and sentenced as an accessory.

(2) The sentence for the accessory shall be based on the penalty for a principal. It shall be mitigated pursuant to section 49(1).

A) Assistance to the crime

The perpetrator must have committed the crime through the honeypot. “Assistance to the crime” means every action that facilitates or leads to the execution of the crime. The assistance can be both: physical and psychological.

Seen from an objective point of view, honeypots are meant by the attacker to become part of the DoS attack. Honeypots transfer data to the victim which may cause the server to shut down. It is doubtful whether each participating bot in a DDoS attack is cause for the success. Many requests may even arrive after the shut down and therefore not be causal. Assistance according to the meaning of Section 27 of the Criminal Code does not have to be causal in the sense of the “condition sine qua non” formula for the success. It is sufficient if the risk for the success is facilitated. In this case, the honeypots contribute to overloading the system. Thus, honeypots support the offense, according to Section 303b I Nr 2.

B) Criminal Intent

For the subjective part, in order to be considered as an assistant to the crime, the operator must have a so-called “doubled accessory intent”. This means that he must both accept the intentional (main) offense, and intend to facilitate it.

aa) Intent towards the crime

In this case, the main offense is the computer sabotage (Section 303b I Nr. 2 of the Criminal Code). The accomplice’s intention has to refer to this offense. The accomplice does not need to know the exact circumstances of the case. It is sufficient if the accomplice has an approximate idea of the crime.

It is sufficient for the intention of the accomplice if he tacitly accepts the main crime (so-called eventual intent).

The honeypots are installed with the intention to be found by potential attackers. The situation is different if the operator is confident that the attack will not take place. It would then be considered only as a negligent act, which would not be punished.

In case of a DDoS attack, there could be doubt if the accomplice (operator) actually tacitly accepts the crime or not. The fact of operating a honeypot does not mean (in principle) that the operator agrees with the DDoS attack. However, this also does not mean that the possibility of complicity is to be excluded. It is generally accepted that the accomplice does not necessarily have to have a particular interest in the crime. Even if the accomplice disapproves of the crime itself, he can still be punished as an accomplice.

However, the operator of the honeypot has to have at least a vague concept of the specific crime. It is not sufficient, if the operator tacitly accepts all potential IT-related criminal offences.³⁵ But for the planned SISSDEN honeypots the later seems to be the case. They are meant to passively await connections and collect all sorts of malware that may be used for criminal offenses, including e.g. DDoS attacks, ransomware, trojans, data espionage, data theft, data sabotage, or even bitcoin mining. The whole point of honeypots in the SISSDEN scenario is that the researchers don't have a clear picture of the current threat landscape and therefore gather information via those honeypots. The intent therefore is not sufficiently appropriated with regard to the specific DDOS attacks exploiting the honeypots.

Conclusion: The operators of honeypots most likely lack the necessary knowledge and intent to act as an accessory for data sabotage (Section 303b I Nr. 2, 27 of the German Criminal Code).

(bb) The intent regarding the aid action

It is necessary to analyse if there is really the intention to aid the offender. The main offender does not necessarily need to recognize the support. For the operator to be punished as an accomplice, the offender does not have to know that he has fallen into the honeypot trap. The vulnerable system of the honeypot may facilitate the attack. The operator of the honeypot is aware of that.

However, the deployment of honeypots by CERTs or researchers would be considered as "occupationally typical" and therefore "neutral" behaviour. Courts and scholars agree that, if the aid action itself is considered occupationally typical, there are additional requirements regarding the intent on the aid action. They require positive knowledge of the crime or even malicious intent.³⁶ Since the honeypot operators in our SISSDEN case do not know specifics of the criminal offences trying to exploit the honeypots – these may even happen months or years after the initial deployment – they have neither knowledge or malicious intent.

(C) Illegitimacy

Additionally, the operator of the honeypot could be legally justified.

There is no "emergency aid" (Section 32 of the Criminal Code) situation to justify the support. Configuring a honeypot is not a suitable means to avert DDoS attacks.

The consent of the victim could also be seen as a justification. This presupposes knowledge of the "victim". This is not the case, basically due to the anonymity of the Internet. The situation is different when the attacked company has its own IT security department and establishes a honeypot for analysis purposes.

³⁵ See BGH, Beschluss vom 28. 2. 2012 – 3 StR 435/11.

³⁶ See for more details Joecks, Münchener Kommentar zum StGB, 3. Auflage 2017, Section 27 Rn 49-78.

Because attacks do not stop taking place due to honeypots and the threatening situation is in general not recognizable for the victim, the idea of a “presumed consent” of the victim does not help, either.

Section 34 of the Criminal Code, which provides a justification in case of imminent danger, also does not apply because the operation of a honeypot does not aver the concrete danger to the victim.

The act (operating a honeypot) could be justified, however, under the aspect of fundamental rights (freedom of scientific research).

In other aspects of (criminal) law we can find justifications, which are also derived from the freedom of scientific research. Section 184 b V of the Criminal Code is an example. According to this paragraph, those who distribute child pornography will not be punished, if the act serves exclusively the lawful fulfilment of official or professional obligations. This exemption intends to exclude, among other reasons, scientists from a punishment, when their intention is to perform scientific research. Even though this recognized justification is derived from the fundamental right of freedom of scientific research, it cannot be used as a general rule: It relates to one specific section of the Criminal Code only.

A justification might, however, be derived directly from the freedom of scientific research, as laid down in **Article 5 III Alt. 2 of the German constitution**.

However, deriving a direct justification from fundamental rights is highly controversial. The German Federal Constitutional Court is of the opinion that there is an interdependency between fundamental rights and criminal law, so a justification is not generally excluded. This leads to the question whether it is possible or not to derive a justification from this specific fundamental right. In criminal law, there is a system of recognized justifications, but this does not mean that other justifications are excluded.⁷⁶ Therefore, a justification from Art 5 III 2 of the German constitution is conceivable.

There is, however, much uncertainty when it comes to the question whether fundamental rights can be used or not directly as a justification in a criminal case. Opinions in the jurisprudence are divided. The prevailing doctrine however denies the possibility of directly applying fundamental rights as a justification. This means that the effects of fundamental rights must be considered when applying the “simple” existing justifications. For example, Art 8 of the German constitution grants the fundamental right to demonstrate. When interpreting Section 240 II of the Criminal Code, one has to decide whether a coercion is reprehensible; here, the value of Art 8 of the German constitution must be considered. In the context of Section 193 of the Criminal Code, fundamental rights, such as freedom of expression (Art. 5 of the

Because of methodological reasons, the idea of the freedom of science as a general justification must be rejected. The problem of honeypots is that the individual case plays a decisive role in the end. The operator (scientist) does not know the victim of the DDoS attacks, thus he cannot perform a risk assessment.

Moreover, the system of justifications conceived in the Criminal Code is sufficient to consider fundamental rights, so there is no room for additional justifications by directly applying the freedom of scientific research.

The requirements for a “wrong assumption of being justified” are also not given. The operator of the honeypot is not mistaken about the existence of a recognized justification.

Conclusion: Based on these considerations: Although the honeypot operator is not justified by research purposes, deploying and operating honeypots does not constitute sufficient intent for an accessory of computer sabotage (Section 303b I Nr. 2, 27 of the German Criminal Code).

4.1.2.3 Aid for further offenses

As initially outlined, DDoS attacks can also cover other offenses such as extortion (Section 253 of the Penal Code) or damage to property (Section 303 of the Penal Code). Therefore, the question if the operator helps the perpetrator to do these “other” offenses rises again.

An aid to extortion under the aspect Sections 253, 27 of the Criminal Code cannot be considered due to a lack of subjective facts.

To be punished, the operator would need to have double intention: concerning the aid provided and concerning the main offense. The aid must therefore know that the main offense is extortion. However, the operator of the honeypot will usually not know the peculiarities of the individual case.

This also means that neither the aid to commit damage to property (Sections 303 I 27 of the Criminal Code), nor injury to others (Sections 223 I, 27 of the Criminal Code) nor homicide (Sections 212 I, 27 of the Criminal Code) come into question.

The aid to a negligent personal injury according to Section 229 of the Criminal Code or to a negligent homicide according to Section 222 of the Penal Code is not possible from a dogmatic point of view, according to Section 27 I of the Penal Code.

4.1.2.4 Negligence of the accomplice

Before investigating negligence crimes it must be said that the differentiation between principal and accomplice/accessory outlined is only related to intentional offenses. When hospitals are victims of DDoS attacks, and (for example) life sustaining systems fail as a result, people could be injured or end up dead. This brings then into question if the honeypot operator commits a negligent injury according to Section 229 of the Criminal Code or even a negligent homicide according to Section 222 of the Criminal Code. This would be the case if the operator could realistically expect that health or life is being threatened by the attack.

4.1.3 Use of honeypots with limited data rate

In the criminal investigation it was assumed that honeypots are used without a limited data rate. However, limiting the rate of data could have an impact on the previous criminal analysis.

In the case of a limitation the potential threat to the victim is considerably reduced. Limiting the data rate exercises reasonable care thus ruling out negligence.

Conclusion: Deploying and operating honeypots may constitute the risk for a negligent offense, if individuals are hurt in the attack.

4.1.4 Risk considerations

The present investigation concludes that the operation of honeypots is may be associated with criminal risks.

It should be clear that there is no assured jurisprudence regarding the legal issues related to honeypots. In particular, there is still a lack of relevant court rulings. Ultimately the courts will be the ones who decide on the liability to prosecution of the honeypot operator.

The intensity of the attack or its impact on the victim are decisive criteria for the criminality of the operator. Section 303 b of the Criminal Code requires that a data processing is significantly disturbed. It depends on the respective system of the victim whether it is enough (and what kind of intensity is required) to disturb his system.

Recommendation: To minimize the risk of negligent offenses, it is important to rate limit outbound traffic of the honeypot to the minimum necessary for analysing the attack.

4.2 Sandboxes

Regarding the operation of sandboxes to execute malware samples, the assessment of criminal law holds similar results. The operator does not have sufficient knowledge or intent regarding the specific offence the malware performs and thus cannot be considered accessory. To avoid negligence, it is equally important as for honeypots to limit the outgoing communication to the absolute minimum and to closely monitor and intervene, if harmful network activity is detected.

Recommendation: To minimize the risk of negligent offenses, it is important to restrict network access of the malware in the sandbox and the outbound data rate to the minimum necessary for analysing the malware behaviour. In addition, reasonably expectable harmful actions that are typically performed by malware should be contained, such as sending email spam.

4.3 Port scans / Active Network Probes

TCP or UDP port scans for research purposes could be punishable as data espionage, Section 202a I of the German Criminal Code. According to Section 202a it is a punishable offense to obtain access to protected data without authorization by circumventing security measures. The operator of the port scan or active network probe gains data regarding the services without authorisation of the services owner. However, the most relevant criterion regarding the assessment of potential data espionage via port scans is the circumvention of security measures. As port scans can be

definition only get data from open ports – whether they are open intentionally or unintentionally – there are no security measures in place which would be circumvented. The potential fact that the owner of the system is unaware or opposed to the port scan is not considered a security measure.

Conclusion: Port scans and network probes are not considered criminal offenses according to German criminal law.

Recommendation: If a port scan accidentally overloads the scanned system, the same argumentation as for DDoS attacks above is applicable. Thus, it is recommended to monitor port scans and exercise reasonable care to limit the (unlikely) risk of overloading systems with the port scan requests.

5 Privacy and data protection law

5.1 Collection of personal data

5.1.1 According to Directive 95/46/EC³⁷

It is questionable whether the saving of data, gained through honeypots, sandboxes and port scans (see above), is a relevant process in terms of data privacy, for example collection of personal data according to Article 2 (b) Directive 95/46/EC, and whether this is legally permissible.

5.1.1.1 *Applicability of Directive 95/46/EC*

First of all the Directive 95/46/EC must be applicable in a substantive and territorial way.

5.1.1.1.1 *Substantive applicability*

Article 3 (1) of the Directive 95/46/EC applies for the processing of personal data in a wholly or partly automatic way.

5.1.1.1.1.1 Personal data

Pursuant to Article 2 (a) of the Directive, personal data are all information concerning a particular or identifiable natural person. The natural person is then referred as data subject. A person can be considered determinable if he can be identified directly or indirectly. This applies if there is an identification number or if specific elements allow conclusions to be made on the physical, psychological, economic, cultural or social identity. For the DDoS attack monitoring and portscans, it is in particular the IP address of the victim, which could represent personal data. For IP addresses, the ECJ ruled in its judgment of 19 October 2016 that both static and dynamic IP addresses represent personal data.³⁸ For dynamic IP addresses this only applies if the responsible authority has legal means which allow it to determine the data subject by means of the additional information about the Internet access provider.³⁹ Whether this is the case depends on the legal

³⁷ <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046>

³⁸ ECJ, Judgment from 19.10.2016, Case C-582/14, ECLI:EU:C:2016:779, para. 49.

³⁹ Ibid.

possibilities within the respective Member State⁴⁰ and therefore cannot be assessed globally. For the SISSDEN project, it seems reasonable to assume that IP addresses, regardless of national law, are to be viewed as personal data. In the case of malware analysis, it is not impossible that a malware tries to download personal data, such as email addresses, in order to carry out further attacks. Furthermore, the responses of portscans may include personal data, in addition to IP addresses, e.g. in the response to "monlist" (NTP) or in SSDP packets.

Conclusion: Within the framework of SISSDEN personal data is present.

5.1.1.1.1.2 Processing of personal data

In addition to the existence of personal data, their processing according to Article 3 (1) of the Directive is also a prerequisite. The concept of processing is broadly defined in Article 2 (b) and encompasses not only the recording and transmission of personal data but also the collection of such data. The form of data processing must be fully or partially automated happen. In the case of the DDoS honeypots, SISSDEN stores the packet sent by the attacker to the honeypot. This packet contains the IP address of the victim. The IP address of the victim is a personal data (see above) regardless of whether it is relative or absolute. Thus, this technique provides for the collection of personal data. For the sandboxing of malware, it is initially unclear from the perspective of SISSDEN whether or not the malware downloads personal data, such as e-mail addresses, to the sandbox. If this is the case, there is a processing of personal data, otherwise the use of sandboxes is not a data protection relevant process. Portscans search the Internet for open ports that can be misused for DDoS attacks. If a vulnerable port is detected on a system, the system's IP address and response packets are stored. In the case of NTP, the response packets contain the IP addresses of the last 100 clients. In the case of SSDP the device names on the local network are included. For DNS, SNMP, CharGen, QOTD, and NetBIOS, the response packet contains undefined data. As already stated, IP addresses represent personal data. This also applies to NTP. SSDP response packets can also include personal data, for example when a device bears the name of a natural person. The content of the response packages is not relevant in the case of SSDP and NTP. After a measurement of the size of the response packets (number of bytes), the content can therefore deleted. Nevertheless, there is a collection of personal data in case of SSDP and NTP from a legal point of view. A subsequent deletion therefore does not eliminate the previous collection. The other IP addresses (honeypots) are stored, used for analysis purposes, and transmitted to ISPs and CERTs (see below). This is also done in an automatic way.

Conclusion: The prerequisite "processing of personal data" is regularly fulfilled.

5.1.1.1.1.3 Exemptions from the applicability

Article 3 (2) of the Directive contains several exemptions which are not covered by the processing of personal data. On the one hand, the Directive is not intended to apply to data processing in the context of an activity which is not covered by the law of the European Union. This means, for example, public security, defence or the security of the state. Furthermore, the Directive is not intended to apply to the processing of personal data if it is carried out by a natural person solely for private or family purposes. For SISSDEN, none of these exemptions are relevant.

5.1.1.1.1.4 Controller

Although it is not a written prerequisite for the applicability of Directive 95/46/EC, there must be a responsible body for data processing. The responsible body is defined in Article 2 (d) of the

⁴⁰ ECJ, Judgment from 19.10.2016, Case C-582/14, ECLI:EU:C:2016:779, para. 47.

Directive and referred to as a "controller". Controller is any natural or legal person, authority or entity that alone or together with others decides on the purposes and means of the processing of personal data. Initially, SISSDEN is not an independent organization but a research project. However, this does not preclude a joint controllership for processing if the project partners jointly decide on the purposes and means of the processing of personal data.⁴¹ The data protection obligations from the Directive then apply to all project partners.⁴² The key question when assessing whether a joint controllership is whether one party alone decides on the purposes and means or whether this decision is taken jointly.⁴³ Within the framework of the joint control, the participation must not be equally shared and may take different forms.⁴⁴ The central element of the joint controllership is that responsibility for compliance with data protection regulations and possible violations of these provisions is clearly assigned.⁴⁵ For SISSDEN, all project partners determine the purpose and the means by which the processing of personal data takes place. To a large extent, these are already defined in the work of the research project. For this reason, SISSDEN can therefore be regarded as a joint controller.

Conclusion: SISSDEN is joint controller.

Recommendation: All project partners of SISSDEN should declare themselves responsible for compliance with data protection regulations. One project partner should act as a first point of contact for data protection requests and be mentioned in this function on the website.

5.1.1.1.2 Territorial applicability

Directives are binding for all Member States of the European Union.⁴⁶ All Member States have transformed the provisions in a Directive into national law.⁴⁷

Conclusion: The Directive 95/46/EC is applicable in a substantive and territorial way.

5.1.1.2 Principles relating to data quality

Under the title "Principles Relating to data quality" the European legislator has established a number of principles for the processing of personal data in Article 6 of the Data Protection Directive. In principle, according to subparagraph (a), personal data must be processed fairly and lawfully. According to subparagraph (b), this must be done for clear and legal purposes. Further data processing for historical, statistical or scientific purposes is not to be regarded as generally incompatible with previous purposes. For SISSDEN, this means that data collected on a different legal basis can nevertheless be used for the research work, when there is an appropriate safeguard. Subparagraph (c) and (d) specify that only necessary data may be collected (data minimization) and that the data must be accurate. Latter means that incomplete or incorrect data must be deleted or corrected. After subparagraph (e), personal data may be collected or further processed only to the fulfilment of purpose. If this is done, data may only be processed in an anonymous form. For historical, statistical or scientific purposes, the Member States are required to adopt a regulation. For this reason, no global statements can be made here.

⁴¹ Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor", adopted on 16 February 2010, 00264/10/EN, WP 169, P. 18.

⁴² Ibid.

⁴³ Ibid.

⁴⁴ Ibid., P. 19.

⁴⁵ Ibid., P. 22.

⁴⁶ Art. 288 Treaty on the Functioning of the Union (TFEU).

⁴⁷ Ibid. ent

5.1.1.3 *Criteria for making data processing legitimate*

A justification is necessary for the legal processing of personal data. The European law prohibits the processing of personal data unless a permission is given. Article 7 of the Directive provides possible permissions in descending form from consent to a legitimate interest. The legal grounds mentioned in subparagraphs (a) to (e) are not considered within the framework of the project. The project partners can neither recover the consent of the affected person nor are they in agreement with this. Another legal obligation to collection of personal data is also not visible. Similarly, the justification in subparagraph (d) for processing in the event that the interests of the data subject are of vital concern are, regularly, not present. Subparagraph (e) allows the processing of data in the case of the performance of a task which is in the public interest or is carried out in the exercise of public authority. In both cases a formal act of entrusting is mandatory which is not available in the case of SISSDEN.

A justification for the processing must therefore be based on the reasons given in subparagraph (f). Article 7 (f) requires a balance between the interest of the controller and the privacy interest of the data subject.⁴⁸ For the benefit of the data subject, it must be taken into account that any data processing is associated with dangers. The heart of the SISSDEN project is a global sensor network, which is operated by the project consortium. This provides insights about ongoing attacks within the Internet. The network is supplemented by a malware analysis and other external data sources. This allows SISSDEN to inform not only the victim but also other organizations such as CERTs, ISPs, hosting providers and law enforcement agencies about ongoing attacks. This is particularly the case for the citizen, but also for small and medium-sized enterprises, which alone do not have the capacity to counter such attacks. For this reason, SISSDEN provides an important contribution to the prevention of cybercrime and creates the possibility of effectively preventing security breaches. In addition, the data collected by SISSDEN is a major contribution to research on cybersecurity and thus also serves the development of new defense strategies. It should also be borne in mind that no specific categories of personal data (Article 8) will be processed. Rather, the data processed by SISSDEN is classified as less sensitive because conclusions on the data subject are not immediately possible for everyone (even for SISSDEN). In order to achieve the purposes pursued with SISSDEN, it is necessary to store the IP addresses in a non-anonymized form. Only in this way is it possible to carry out a permanent analysis and evaluation of cybercrime. In the field of malware sandboxes it is unclear whether SISSDEN receives any personal data through possible downloads of a malware. It is also unclear which category of personal data it might be. However, this makes the operation of sandboxes from a data protection perspective not illegal. Rather, if a malware downloads personal data to the sandbox, SISSDEN must perform a case-by-case analysis. Within the framework of this individual case analysis, it is necessary to examine whether data subjects or authorities have to be informed, or whether the deletion of the data is sufficient. In the case of NTP and SSDP response payloads, these are only examined with regard to their size (see above). After this, the personal data will be deleted. In view of the interests pursued by SISSDEN and the interest of the individual in the protection of his personal data, this solution appears to be justified. In principle the interests of SISSDEN in data processing seems to predominate, however bearing in mind that the design of the justifications provided for in Article 5 is a task of the Member States.

⁴⁸ Brühann in: Grabitz/Hilf, Das Recht der Europäischen Union, 40. Auflage 2009, Art. 7, Rn. 20.

Conclusion: SISSDEN may process the data obtained by honeypots and port scans. The personal data in the case of NTP and SSDP response payloads must be deleted after measuring the size of the response payload. Other use cases, such as malware downloads in sandboxes, or collecting spam emails in spampot, require further investigation in D2.8.

5.1.1.4 Rights of the data subject

The data subject is entitled to the right of notification, the right of access and the right of objection.

5.1.1.4.1 Data subject's right of information

Articles 10 and 11 of the Directive provide an obligation for the controller to inform the data subject about the processing. Article 10 is applicable only if the data are collected directly from the data subject. This requires at least an active involvement of the data subject.⁴⁹ The data subject must know and consent the collection of data for the purpose of processing.⁵⁰ In the case of SISSDEN, however, the data are collected without the data subject being aware of it. For this reason, there is no obligation to provide information under Article 10 of the Directive. However, information might be provided in accordance with Article 11 of the Directive. An information according to Article 11 has to take place about the identity of the controller, the purposes of processing and other information such as the categories of data concerned, the recipients or categories of recipients (in the case of disclosure by transmission) and the data subjects rights of information and rectification. Article 11 does not specify a time for the information. However, the information should be given at the earliest possible time.⁵¹ The Directive provides derogations from the information obligation in Article 11 (2). Paragraph 1 should not be applied if the information of the data subject is impossible or involves a disproportionate effort. This applies in particular to data processing in the context of scientific research. A distinction between impossibility and disproportionate effort can be difficult, but is not absolutely necessary because of identical legal sequences.⁵² A lot of effort for the information of the data subject justifies alone no exception.⁵³ The decisive factor is, rather, an individual case-balancing between the amount of the effort and the interest of the data subject on an information.⁵⁴ In the case of SISSDEN, a notification of the data subject is normally only possible with the aid of the IP address. This means that the project partners would have to find out which person is behind the corresponding IP address and then inform them in a different way. Such a search is not possible for SISSDEN, since the IP address without further additional knowledge does not allow to identify the data subject without a doubt. However, SISSDEN does not have any legal basis for gaining additional knowledge, for example by requesting an ISP. Furthermore, current research results show that a contact via the WHOIS information in the case of the Alexa Top 10,000 websites has only a success rate of 16.2%.⁵⁵ In the case of the Alexa Top 1 million, the success rate already drops to 6.3%.⁵⁶ For

⁴⁹ Ibid., Art. 10, Rn. 7.

⁵⁰ Ibid.

⁵¹ Ibid., Art. 11, Rn. 5.

⁵² Ibid., Rn. 8.

⁵³ Ibid.

⁵⁴ Ibid.

⁵⁵ STOCK, B., PELLEGRINO, G., ROSSOW, C., JOHNS, M., AND BACKES, M. Hey, You Have a Problem: On the Feasibility of Large-Scale Web Vulnerability Notification. In USENIX Security Symposium (2016).

⁵⁶ Ibid.

this reason, and with regard to the high-ranking interests pursued with SISSDEN, an information on the data subject is not required. Furthermore, an information can be dispensed if a law allows the storage or transfer of personal data. This can be relevant to SISSDEN in case of data transfer to law enforcement agencies (see below).

5.1.1.4.2 Data subject's right of access

The right of access includes, in Article 12 (a), essentially the right of the data subject to get information on the data processing without constraint at reasonable intervals and without excessive delay or expense. According to subparagraph (b), the data subject is entitled to rectification, erasure or blocking of data if the data are not processed in accordance with the Directive. In the case of rectification, erasure or blocking of data, the controller must, in accordance with subparagraph (c), also communicate the changes to third parties to whom the data have been transmitted, if this is not impossible or disproportionate. According to Article 13 (1), the Member States may restrict the right of information in the listed cases, e.g. national security. Although the national law of the Member State applies here, it can be assumed that there is no exception to Article 13 (1) for SISSDEN. Article 13 (2) provides that Member States may adopt exceptions to Article 12, in particular for scientific research where there is obviously no risk to the private sphere of the data subject. A more detailed design is the task of the Member States, which in exceptional cases must provide legal safeguards.

5.1.1.4.3 Data subject's right to object

Article 14 provides a general right of opposition (Article 14 (a)) as well as a right of opposition in the case of direct advertising (Article 14 (b)). The latter seems not relevant to SISSDEN. Within the framework of Article 14 (a), the data subject is at least entitled to a right of objection in the cases referred to in Article 7 (e) and (f). This has an increased relevance for SISSDEN because data processing will be regularly justified by Article 7 (f) (see above). The right to object exists if the data subject provides a legitimate reason which arises from a particular situation of the data subject. By taking into account important individual interests, the data subject should be given the opportunity to influence the overall assessment according to Article 7 (f).⁵⁷ This person may, for example, have a legitimate interest in being excluded from portscans or network probes. In the case of an effective objection, data processing is prohibited and the controller can no longer refer to the data.⁵⁸ In order to give the data subject the possibility of an opt-out, SISSDEN will provide a contact opportunity on the website of the project.

Conclusion: For SISSDEN there is no obligation to inform the data subject about the processing. The data subject, however, has a right of access and a right to object.

Recommendation: SISSDEN has to provide a contact opportunity on the website of the project to allow the data subject to opt-out from data acquisition and processing.

5.1.1.5 Confidentiality and security of processing

Any data processing must be confidential and secure in accordance with Articles 16 and 17 of the Directive. Article 16 stipulates that persons who are under the responsibility of controller or the

⁵⁷ Ibid., Art. 14, Rn. 7.

⁵⁸ Ibid., Rn. 9.

data processor may only process personal data on the instructions of the controller. The persons referred to in Article 16 are, for example, workers, freelancers, self-employed subcontractors and their workers, who carry out certain activities on the instructions of the controller.⁵⁹ All these persons are bound to confidentiality, which must be materially arranged by the controller.⁶⁰ For this purpose, the controller must make an instruction, for example, within the framework of a work or service contract.⁶¹ The Directive provides for an exception only if there is a legal obligation. This is the case, for example, when a witness makes a statement in court.⁶² The rules on the security of the data processing referred to in Article 17 shall cover both the data processing by the data controller and the contract data processing. In the case of SISSDEN, the figure of the contract data processing is not relevant so far, so that the focus is on the obligations of the controller. These are laid down and described in Article 17 (1) and (4). Accordingly, the responsible authority must take appropriate technical and organizational measures to ensure the security of the data processing. The measures are intended to protect the data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access and against all other unlawful forms of processing. The Directive aims to provide the widest range of protection possible by listing these alternatives.⁶³ All necessary measures must be taken to prevent potential hazards.⁶⁴ This must be done before data processing is started.⁶⁵ The nature of the measures is not defined by the Directive. However, the physical security of the server rooms, the strict regulation of access to data, the control of access by means of access protection, and the protection of the data from external intrusion, should be considered.⁶⁶ The key concepts of information security provide a useful guide for the design of a security concept.⁶⁷

Conclusion: SISSDEN must ensure that any data processing is confidential and secure.

5.1.1.6 Notification to the supervisory authority

According to Articles 18 and 19 of the Directive, the controller must notify any data processing to the cognizant supervisory authority. This is done by the SISSDEN partners in accordance with the respective national law.

Conclusion: SISSDEN is jointly responsible in the sense of the data protection directive and is bound to the directive for data processing. As long as the data processing is performed on the examined scale, it is legally permissible.

⁵⁹ Ibid., Art. 16, Rn. 5.

⁶⁰ Ibid., Rn. 6.

⁶¹ Ibid., Rn. 7.

⁶² Ibid., Rn. 11.

⁶³ Ibid., Art. 17, Rn. 3.

⁶⁴ Ibid., Rn. 4.

⁶⁵ Ibid.

⁶⁶ Ibid., Rn. 6.

⁶⁷ Y. Cherdantseva and J. Hilton, "A Reference Model of Information Assurance & Security," Availability, Reliability and Security (ARES), 2013 Eighth International Conference on , vol., no., pp.546-555, IEEE, doi: 10.1109/ARES.2013.72, 2–6 September 2013. [<http://users.cs.cf.ac.uk/Y.V.Cherdantseva/RMIAS.pdf>]

5.2 Data sharing platform

5.2.1 Data sharing inside the project

5.2.1.1 According to Directive 95/46/EC

The SISSDEN project partners are joint controllers for the data processing in the project (see 5.1.1.1.4), so no further justification for the data transmission between the project partners is necessary.

Conclusion: Since SISSDEN is a joint controller for data processing, personal data can also be passed on within the project.

5.2.2 Data sharing with ISPs and CERTs

5.2.2.1 According to Directive 95/46/EC

Within the framework of SISSDEN, project partners want to share their insights about ongoing attacks with ISPs and CERTs. These should be able to inform the operators of affected systems, so that they can close existing security gaps. The passed records contain the IP address of the affected system, i.e., personal data (see above). Only the IP addresses that belong to their assigned address range are passed on to the respective ISPs and CERTs. This ensures that only those organizations obtain personal data that can actually influence the course of an attack. We consider initially only ISPs and CERTs within the EU. Data transfers to organizations in third countries must be considered separately. ISPs and CERTs are third parties within the meaning of Article 2 (f) of the Directive. A legal basis for the data transfer can only be Article 7 (f) of the Directive (see above). It is questionable whether the balance of interests will change in favor of the person concerned if personal data are not only collected, but also passed on to the above-mentioned organizations. As already pointed out, SISSDEN provides an important contribution to the prevention of cybercrime and creates the possibility of effectively preventing security breaches. Data transfer to the responsible ISPs and CERTs is an essential part of the intended function. Without the possibility of data transfer to the organizations mentioned, a defense or hindrance of attacks is not possible. This is offset by the interest of the person concerned that his ISP or the respective CERT is not informed about a security breach on his system. At this point it is to be considered that the data subject at least is regularly in a contractual relationship with his ISP and the data transfer by SISSDEN is only transferred to combat security problems. In this case, SISSDEN's interest in the data transfer to improve IT security again underscores contradictory interests of the data subject. In many cases, transmission will also be in the interest of the data subject. Data transfer to CERTs for the purposes of incident response is also expressly acknowledged as a legitimate reason in the GDPR.⁶⁸

Conclusion: SISSDEN may pass on the relevant IP addresses to the relevant ISPs and CERTs without the consent of the data subject.

⁶⁸ A. Cormack, "INCIDENT RESPONSE: PROTECTING INDIVIDUAL RIGHTS UNDER THE GENERAL DATA PROTECTION REGULATION", scripted, Volume 13, Issue 3, December 2016, DOI: 10.2966/scrip.130316.258, <https://script-ed.org/wp-content/uploads/2016/12/13-3-cormack.pdf>.

5.2.3 Data sharing with the public

5.2.3.1 According to Directive 95/46/EC

The data shared with the public is anonymized in accordance with Recital 26 of the Directive in order to dispense with a person's reference. The data that is then available are no longer personal data within the meaning of Article 2 (a) of the Directive. To ensure that the anonymization is carried out within the applicable data protection law, SISSDEN will implement the requirements of Article 29 Data Protection Working Party.⁶⁹ The Article 29 Data Protection Working Party has recognized that, in the case of search engines, the removal of the last octet of an IPv4 address is usually an adequate anonymization.⁷⁰ This is considered sufficient because the IPv4 address then only allows the conclusion to the provider or the subnet but it is no longer possible to identify an individual.⁷¹ This means in specific that the information could belong to any of the 254 IP addresses. This form of anonymization is also considered to be sufficient in the case of SISSDEN. Since, after the anonymization, no personal data are available, the data can be shared publicly.

Conclusion: SISSDEN can share anonymized IP addresses with the public.

Recommendation: The last octet of the IP addresses should be stripped for anonymization. However, the consortium is considering to hand out a non-anonymized reference data set for research purposes, as described in the following.

5.2.4 Reference Data Set

Additionally, SISSDEN may want to share reference data sets for research purposes which are not anonymized. In this case the consortium has to install contractual safeguards with the recipient to ensure that the personal data is appropriately handled. Depending on the location of the recipient these safeguards may be terms of use or Standard Contractual Clauses (see Section 5.3.2).

5.2.5 Sharing data with law enforcement agencies

5.2.5.1 According to Directive 95/46/EC

The Directive is, by virtue of an exception under Article 3 (2), not applicable in the event of data transfer to law enforcement agencies.

5.2.5.2 According to Directive (EU) 2016/680

Directive (EU) No 2016/680 concerns the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

⁶⁹ Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques, adopted on 10 April 2014, 0829/14/EN, WP 216.

⁷⁰ Article 29 Data Protection Working Party, Opinion 01/2008 on data protection issues related to search engines, adopted on 04 April 2008, 00737/EN, WP 148, P. 20.

⁷¹ Ibid.

The Directive shall apply, in accordance with Article 2 (1), only to competent authorities. These are finally listed in Article 3 (7). Article 3 (7) covers only a public authority or another body or entity entrusted by Member State law to exercise public authority and public powers. This is not the case with SISSDEN, which is why Directive (EU) 2016/680 is not applicable.

5.2.5.3 Application of national law

In the absence of a European regulation, data transfers to law enforcement authorities must be based on the respective national law of the Member States.

Conclusion: There is no European law for data transfer between SISSDEN and law enforcement agencies. Therefore, national law must be applied.

5.3 Data transfer to third non-EU states

This section will introduce contractual and company-internal instruments to cope with the legal issues of international data transfers by the SISSDEN project partners.

The legislative regulation of European data protection enables the transmission of personal data within the area of the European Union. Still, any further disclosure across the borders of the EU/EEA into a third country is not per se covered by such statutory permission. The decisive factor for a lawful disclosure is the existence of an adequate level of protection for the personal data in question. For some countries outside the European Union, this adequate level of protection through legislative measures was acknowledged by the European Commission. These countries are: Andorra, Argentina, Canada, Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland and Uruguay.

Nevertheless, this leaves the question open how such an acknowledgement could be achieved in other countries that do not provide such automatic protection by national law. The EU has installed a list of instruments that are deemed to provide the necessary adequate level of protection for personal data, hence permitting the transfer thereof.

Such instruments are:

- The EU/US Privacy Shield
- EU Standard Contractual Clauses (EU SCC)
- Binding Corporate Rules (BCR)

In the following subsections, these instruments will be described and examined with regard to their suitability for data transfers within the SISSDEN project.

5.3.1 EU-U.S. Privacy Shield

On 6 October 2015, the Court of Justice of the European Union had declared the Commission's 2000 Decision on EU-US Safe Harbor invalid. To install a new legal basis for transfer of personal data to the US, the Commission adopted on 12 July 2016 its decision on the EU-U.S. Privacy Shield. Currently, more than 1,000 U.S. companies have registered under the Privacy Shield.

Although the new framework for the adequacy decision has been improved based on the ECJ's criticism, several parties have attacked the validity of the Privacy Shield.

Especially, the Art. 29 Working Party⁷² has criticized the lack of specific rules on automated decisions and of a general right to object. Additionally, the Article 29 Working Party would have expected stricter guarantees concerning access by public U.S. authorities and the independence and the powers of the Ombudsperson mechanism. It regrets the lack of concrete assurances that bulk collection and indiscriminate collection of personal data do not take place.

The Privacy Shield has already been challenged before the ECJ similarly to its predecessor. On September 16, 2016 privacy advocacy group Digital Rights Ireland asked for the annulment of the adequacy decision.⁷³

Conclusion: During the project duration of SISSDEN, consortium partners could base data transfers to U.S. data controllers on the Privacy Shield, if the recipient was registered. To this end, Shadowserver U.S. already started the registration process for Privacy Shield. Alternative legal grounds for the transfer may provide a more long-lived solution.

5.3.2 EU Standard Contractual Clauses

An instrument to achieve the adequate protection of personal data, compliant with the requirements of the EU Data Protection Directive 95/46/EC, could be the usage of the European Standard Contractual Clauses provided by the European Commission. These complement the contract entailing the primary contractual service agreement and specify them with respect to the European requirements of minimal data protection standards. The possibility of using these clauses is at disposal for European citizens and organisations due to the principle of freedom of contract that underlies the contract law of all European countries. In 2011, this “freedom of contract” principle has been explicitly affirmed by the Commission's expert group on European Contract Law in its feasibility study. Besides the other affirmed principles of “contractual certainty” and “contractual fairness” it serves as a basis for the further harmonisation of contract law.⁷⁴ The European Data Protection Directive 95/46/EC explicitly open up the possibility of lawful data transfers on the basis of appropriate contractual clauses (Article 26 (2) European Data Protection Directive 95/46/EC).

According to Article 26 of the European Data Protection Directive 95/46/EC the European Commission is competent to find that specific Standard Contractual Clauses pose an adequate guarantee within the meaning of Article 26 Paragraph 2 in the context of the procedure described in Article 31 (2) 95/46/EC. The Standard Contractual Clauses developed by the Commission are not

⁷² Article 29 Working Party Statement on the decision of the European Commission on the EU-U.S. Privacy Shield http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160726_wp29_wp_statement_eu_us_privacy_shield_en.pdf .

⁷³ Digital Rights Ireland v Commission, Case T-670/16. <http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:62016TN0670&from=DE>

⁷⁴ Commission Expert Group on European Contract Law, Feasibility study for a future instrument in European Contract Law, 3 May 2011.

the only Contractual Clauses that can be recognized as adequate. In Principle, every company or trade association may draw up contracts and hand it in for the Commission's approval.⁷⁵

5.3.2.1 Objectives

The first and foremost goal of providing these standard contractual clauses for usage is the warranty of adequate safeguards for the lawful transfer of personal data. Their contractual guarantees of data protection and provisioning of data subject's rights enable legal certainty and compliance with the European Commission's requirements regarding a sufficient level of protection for the data.⁷⁶ The European Commission has adopted several sets of Standard Contractual Clauses covering different roles of the data recipient. The recipient can either take the role of a data controller or a data processor. So an important pre-condition of using these clauses is the determination which role the involved parties obtain. This depends on the explicit and implicit competence as well as the factual control of the party. In a nutshell, the amount of decision power over the purpose and means of the data processing determines the classification either as controller or solely as processor.⁷⁷ Once the involved parties have been identified either as controller and processor, they need to use the fitting set of standard contractual clauses provided by the European Commission in the correct context. The Commission provides three different sets of clauses currently in force, whose applicability is determined to which parties the data is transferred. There are two different constellations of data transfers:

- Transfer of data from controller to another controller (C2C)
- Transfer of data from controller to a processor (C2P)

Two of the three sets provided by the European Commission cover the C2C constellation. These Commission decisions on these two sets are from the years 2001 and 2004:

- Commission Decision of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC (2001/497/EC)

And the alternative set, amending the first:

- Commission Decision of 27 December 2004, amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries (2004/915/EC)⁷⁸

The two controller-controller sets are alternatively. Companies may choose their preferred contractual clauses.

The third set covers the C2P constellation, decided by the Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (2010/87/EU).

⁷⁵ Cf. article 26 (4) EU Data Protection Directive 95/46/EC

⁷⁶ See also Article 29 Working Party, WP 74, Working document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, adopted on 3rd June 2003, p.7

⁷⁷ Article 29 Working Party, WP 169, Opinion 1/2010 on the concepts of "controller" and "processor", adopted on 16 February 2010, p. 10 ff.; for an overview of and introduction to the criteria for role determination, see TClouds report R1.2.1.2 (Analysis of EU Law), p. 14 ff.

⁷⁸ This set was approved by the Commission as a result of a request by an affiliation of business associations led by the International Chamber of Commerce (ICC)

Before May 2010, a former version of clauses was implemented by Commission decision and in force since 2001.⁷⁹ This Commission decision however, was repealed and replaced by the 2010/87/EC Decision. So for the controller-processor data transfer there is no possibility to choose from the 2001 or the 2010 clauses. In cases of newly allocated agreements, the involved parties are bound to implement the 2010 version if using the European standard contractual clauses. An exception just may be valid for older contracts concluded before 15th May 2010, as long as the original agreements remain unamended to that date. Any substantial change of the agreement, for instance by involving new parties or changing the purpose of the transfer, leads to the downgrading of the old clauses as ad-hoc contract, that must be brought into line with the principles and safeguards entailed by the newer clauses of the decision 2010/87/EU. Also, such an ad-hoc contract must be examined and authorised by the concerned data protection authorities. Usually, in such cases it would be more appropriate and easier to directly install a new contract using the newer standard contractual clauses. 2010/87/EU.

5.3.2.2 Regulated content

This section will illustrate the substantive points of the standard contractual clauses sets and their most significant differences and effects compared to each other. One of the most prominent arrangements is the definition of a data exporter and the data importer. The data exporter is the controller entity that transfers the data while the data importer is the entity that receives the data from the controller. In contrast to the exporter, who is always the controller, the importer can be a controller as well as a processor entity. The specific definition of the data importer can be acquired out of the individual standard contractual clause that should be used, depending on the classification of the receiving party as controller or processor. As already introduced in the prior section, two of the three sets currently in force are related to transfers of personal data from a controller to another controller entity (C2C clauses). In contrast, the third set focuses on the data transfer from a controller to a processor and further sub-processing connections (C2P clauses). Thus, the analysis of the clauses will be broken down in two following sections, thematically divided into C2C clauses and C2P clauses.

5.3.2.3 C2C clauses 2001/497/EC and 2004/915/EC

The C2C clauses may be used within the SISSDEN project to cover personal data transfer from the SISSDEN consortium to e.g. ISPs or CERTs in third party countries. The recipient (data importer) in this case would be a data controller.

The foremost purpose of the EU standard contractual clauses is the creation of an adequate level of protection for the personal data, allowing the disclosure of said data from the controller to another party. This comes with the regulation of obligations for the individual contract parties and corresponding rights for concerned persons, namely the data subjects to enforce these. The breach of contractual obligations with regard to the personal data is explicitly subject to the liability of the data exporter and the data importer. Difficulties arise once several layers of vendors and customers are involved, igniting the need to conclude a multitude of contracts. This especially applies if data are transferred in a chain of several sub-processors, because each data exporter needs to conclude a contract with each data importer in a third country. The adjustment of contracts is even more complex in cases of changes regarding the data transfer itself. Also, once

⁷⁹ Commission Decision of 27 December 2001 on standard contractual clauses for the transfer of personal data to processors established in third countries, under the Directive 95/46/EC (2002/16/EC)

units of an internationally operating corporation are involved or the legal structures of the corporate form change, considerable administrative effort has to be made to align, adjust and newly conclude existing contracts. This also affects contractual structures such as master agreements with added appendices, e.g. related to economic aspects, such as Service Level Agreements, sales and distribution, marketing, or pricing.⁸⁰ In the standard contractual clauses provided by the Commission, the applicable law will also be regulated, which is especially of importance for companies with an establishment outside the EU, the EEA respectively. This also implies the determination of concerned data protection authorities and the enforcement of civil law claims against group companies in third countries.

The two sets of clauses 2001/497/EC and 2004/915/EC for the controller-controller data transfer however, show some essential differences. This affects partially some terminology but mostly obligations and liability regulations on both sides of the contract parties. So in the 2001 version (hereinafter: set I), clause 6 (2) provisions joint and individual liability of data importer and data exporter, regardless of causation and possibilities of indemnity and compensation agreements. This regulation was replaced by a liability rule following the causation principle under III. (a) of the 2004 version (hereinafter: set II). Also, punitive damages were explicitly excluded. Furthermore, in cases of dispute, the set I provided under 7 (2) an agreement of international commercial arbitration. This solution however, is quite intricate and expensive for the contract parties, thus in most cases not fitting for disputes in the data protection field. Set II does not provide such an arbitration clause. Furthermore, clause 5 (c) of set I requires the contract partners to abide the advice of the concerned supervisory authorities while set II just provisions the accordance with binding decisions (clause II. (h) - (ii)). Beneficial for the contract parties is also the fact that set II opens up the possibility under clause VII. to supplement the contract with commercial clauses and to update the Annex B (under the condition that the concerned authority is informed).

Conclusion: Set II may appear much more desirable for companies intending to use the EU standard contractual clauses.

This also applies in the SISSDEN context, since the potential variety of involved parties and the increased flexibility in regard to data flows may require a more flexible coordination and content management of contractual agreements. Thus, set II seems more convenient for use within the project.

5.3.2.4 C2P clauses 2010/87/EU

The clauses for controller to processor transfer might become relevant for the SISSDEN consortium, if Shadowserver US would act as a processor on behalf of the SISSDEN consortium.

The new set of C2P clauses based on the Commission Decision 2010/87/EU cover the constellation of data transfers from a controller to a data processor in a third party country.

The most significant regulations are:

- Determination of the governing law, being the law of the data exporter's country
- Liability scheme, deploying the data exporter as primarily liable

⁸⁰ These may under certain circumstance be valid as long as they do not contradict the standard contractual clauses, see recital (5) of the Commission Decision 2001/497/EC or recital (4) of the Commission Decision 2010/87/EU.

- Introduction of a sub-processing clause
- Obligation regulations with explicit constraint demands for sub-processors
- Disclosure of contract copies to data subjects and exporters
- DPA powers for auditing and decision authority on agreements with sub-processors under contradicting law
- Deletion of arbitration clause

Clause 9 of the 2010 set of SCC explicitly determines the governing law with regard to data protection aspects as being the one of the member state the data exporter is established in. This rule also applies for sub-processing services through the whole chain of data processing operations. Corresponding to the applicability of the data exporter's national law, the new set of clauses introduces a liability scheme via clause 3 that determines the data exporter, namely the controller, as primarily liable towards the data subject's claims (clause 3 (1)). However, if the data exporter factually disappeared, ceased to exist in law or became insolvent, according to paragraphs (2) and (3), the data subject may follow the chain of contracts and issue his claim against the data importer, which is in this set of clauses and constellation the processor. The same procedure may take place if also the data importer is not assessable for the data subject's claims. In these cases the data subject may even issue his claim against the sub-processor. However, his liability is limited to his own processing operations under the clauses; thereby he may only be held responsible for issues that are within his own factual control. In conclusion, clause 3 (2) and (3) create kind of successor liability to ensure the protection of the data subject through the case-dependent utmost accessibility of a liable party.

The main novelty of the Commission Decision 2010/87/EU is the introduction of a regulation for sub-processing agreements, enabling a chain of processors and sub-processors. Currently, we do not foresee the need for involvement of sub-processors within the SISSDEN project.

Beyond the sub-processing regulations, the new set of clauses entails some more specific provisions. Just as in the set II of 2004 for C2C constellations, the arbitration clause has been deleted. Another fundamental regulation extracts from clause 5 (f), according to which the data importer is bound to make a copy of the sub-processing agreement available upon request of the data subject. This obligation however, is limited to the extent that he must disclose the contract copy but just a summary of security measures and may exclude commercial information. This procedure may suffice to suitably perform this information duty towards the data subject. Furthermore, clause 5 (j) provisions the sub-contracting must be communicated to the data exporter per default, regardless of a filed request. Clause 11 (4) regulates that the data exporter must keep a list of all sub-processing agreements to be able to eventually provide them to the data protection authority. This list shall be updated once a year. This kind of know-thy-sub-processor procedure entails the data importer sending a full contract copy so the data exporter may be able to fulfil his own obligation to keep track of the closed sub-contracts concerning his transferred data.

By the introduction of the new set of standard contractual clauses via Commission Decision 2010/87/EU, the data protection authorities have been empowered by clause 8 (2) with the authority to conduct audits of all data importers.

5.3.2.5 *Validity and DPA oversight*

The European Commission stated explicitly in their decisions that the standard contractual clauses may not be altered in any way, especially not by amending the individual sets or merging them.⁸¹ However, it must be taken into account that besides the usage of the European standard contractual clauses the national law of the individual EU member states may require additional regulation. Since the EU SCC should not be changed to avoid risking their legal invalidity, such specifics consequently can only be settled in separate contracts, Service Level Agreements (SLA's) or in an annex to the SCC's, respectively. An example for such specific national requirements derives from Germany, whose law just permits the processing of personal data on behalf of others only under certain preconditions laid down in a ten point's catalogue in Article 11 BDSG (Bundesdatenschutzgesetz).⁸² Generally, the allowance of data transfers is examined in a two-step evaluation by the local data protection authorities. First, the general legitimacy of a personal data transfer within the EU or EEA is examined by means of the national data protection law. Once data transfers into a third country outside the community are involved, they must be assessed in terms of permissibility according to section 4c BDSG, which requires the fulfilment of far more stringent provisions. Also, the 2004 set of the EU SCC is seen quite critical by German data protection authorities in regard to the German employee data protection law, because the information obligation of the data exporter is limited. This may lead to gaps in the protection of said data if it is subject to company group-internal data transfers.⁸³ This issue is also seen critically by the French Data Protection Authority (Commission Nationale de l'Informatique et des Libertés, CNIL).⁸⁴ It must be noted that this second set is acknowledged by the European Commission as valid also for employee data. Still, it may be advisable to install extra protection mechanisms in favour of the company's (resp. controller's) employees.⁸⁵ Other EU member countries may have specific regulations in certain areas as well. So unlike in Germany, in the United Kingdom it is not necessary to undergo a two-step evaluation prior to the data export based on the EU SCC. Still, the UK Information Commissioner's Office (ICO) reserves the right to investigate the contractual agreement of a UK data controller in breach of contract cases.⁸⁶ In contrast, in France, the contract clauses regulating the transfer of personal data into third countries need to be reviewed and authorised by the French Data Protection Authority (CNIL). Some few and restrictively handled exceptions are made in cases of prior explicit consent of the data subject or indispensable necessity of the data transfer to safeguard the individual's life or the public interest.⁸⁷

⁸¹ Cf. recital (3) of the Commission Decision 2004/915/EC. Also, the amendment of 2001/497/EC by article 1 (1) of the 2004 decision commits the unchangeableness of the clauses. Furthermore, implemented by the Commission Decision 2010/87/EU for C2P constellations, the irrevocable nature of the clauses is stated in clause 10 of the contract text itself (Variation of the contract).

⁸² Cf. EuroCloud Deutschland eco e. V. through its Guidelines Cloud Computing German Law, Data Protection & Compliance with advice on contractual regulation to achieve compliance with the German data protection law.

⁸³ Cf. position paper of the working group "Internationaler Datenverkehr" ("International data transfer") of the German data protection authorities of 28 March 2007, p. 2 section II. 2.

⁸⁴ Laurence Dumure Lambert and Régine Goury in Meyer Brown L.L.P., New EU Standard Contractual Clauses for Commissioned Data Processing, publication of September 2010, p. 8.

⁸⁵ This is recommended by the ad-hoc working group "Konzerninterner Datenverkehr" (Intra-group data transfer) in its working report of 11 January 2005, which was constituted by initiative of the Duesseldorfer Kreis, an association of the German supreme supervisory authorities for data protection in the non-public sector.

⁸⁶ Mark A. Prinsley and Oliver Yaros in Meyer Brown L.L.P., New EU Standard Contractual Clauses for Commissioned Data Processing, publication of September 2010, p. 7.

⁸⁷ Ibid., footnote 13.

5.3.3 Binding Corporate Rules (BCR)

BCR are corporate codes of conduct that legally bind each entity of a conglomerate to company-specific, EU-compliant data handling systems. Under BCR, a multinational group develops its own in-house regulatory structure sheltering the data processing of its branches and units worldwide. Once approved, BCR empower the multinational group to transfer personal data of EU data subjects in-house, worldwide.

In WP 74, the Article 29 Data Protection Working Party states for the first time that BCR could be a suitable basis for cross-border data transfer.⁸⁸

The term “binding corporate rules for international data transfer” was suggested by the Article 29 Data Protection Working Party (WP 29) as appropriate, because it reflects adequately the purpose of their existence.

- “Binding Rules” indicates that in order for these rules to be deemed as sufficient safeguards within the meaning of Article 26 (2) 95/46/EC, they must have internal and external binding effect
- “Corporate” refers to the context in which these rules can be applied; a multinational group drafts and implements these rules, usually under the responsibility of the headquarters.
- “International data transfer” reflects the reason for the application of this code of conduct; it provides a legal basis for cross border data transfers within a multinational group.

BCR are a tailor made solution for one multinational group. Therefore, the content of BCR differs depending on different conditions and needs of each conglomerate. Further implications on the variety of possible contents have the types of data processed as well as the legal requirements and characteristics of the countries where the data transfer takes place.⁸⁹ The Article 29 Data Protection Working Party has adopted a number of Working Papers adumbrating the substantial content of BCR⁹⁰ to facilitate the drafting of BCR for the applicants.

BCRs not only have to be internally enforceable by the corporate headquarters but the data subjects’ rights have to be externally enforceable by data protection authorities and courts.⁹¹

Although, at first glance BCR may appear to be a canonical solution for data transfers between SISSDEN and US-based Shadowserver, for loose conglomerates like SISSDEN, BCR are unlikely to be a suitable tool for international data transfer. The diversity between the involved players and the broad scope of processing activities make it difficult to impossible to implement and enforce adequate BCR. For these conglomerates it would be necessary to differentiate subgroups within the same corporate group, set up severe limitations and conditions for the exchanges of information and particularise the rules.⁹² Therefore, we deem SCC as the more suited tool within the SISSDEN consortium.

⁸⁸ Article 29 Working Party, WP 74 pp. 6-7.

⁸⁹ Mesaikou, Examining the Binding Corporate Rules as the most promising solution for the cross border data transfers of multinational companies under the EU Data Protection Directive, p. 16.

⁹⁰ Article 29 Working Party, WP 108, 2005; WP 133, 2007; WP 153, 2008; WP 154, 2008; WP 155, 2008.

⁹¹ Article 29 Working Party, WP 108 p. 6.

⁹² Article 29 Working Party, WP 74 p. 9.

Conclusion: For sharing of personal data with data controllers outside of the EU we recommend the use of Standard Contractual Clauses. For the duration of the project the U.S./EU Privacy Shield may act as a sufficient legal basis for data transfer to the U.S. but its validity is already challenged before the ECJ.

6 Intellectual Property Rights Management

Intellectual property (IPR) refers to creations of the mind, such as inventions; literary and artistic works; designs; and symbols, names and images used in commerce.

IPR is protected in law by, for example, patents, copyright and trademarks, which enable people to earn recognition or financial benefit from what they invent or create. These rights are outlined in Article 27 of the Universal Declaration of Human Rights, which sets out the right to benefit from the protection of moral and material interests resulting from authorship of scientific, literary or artistic productions.

An efficient and equitable intellectual property system can help all countries to realize intellectual property’s potential as a catalyst for economic development and social and cultural well-being.

By striking the right balance between the interests of innovators and the wider public interest, the IP system aims to foster an environment in which creativity and innovation can flourish (WIPO, 2016).

6.1 Introduction to IPR Management

The individual categories of IPR and how these are protected is illustrated in Table 1 below:

Category	IPR Protection
Innovative products & processes	Patent or Utility model
Distinctive signs	Trademark, collective mark, certification mark, in some case geographical
Creative designs including textile	Industrial design
Confidential business & technical information of commercial value	Trade secrets
Cultural, artistic & literary works including in most countries software & compilation of data	Copyright & related rights
Microchips	Protection of layout-designs or topographies of integrated circuits

Table 1: How IPR is protected

A strong judicial system has been developed to deal with both civil and criminal IPR offenses that enables right-owners to enforce their rights effectively. This is especially important in a world where expanding technologies have facilitated infringement of protected rights to an unprecedented level. Rights owners can, therefore, take action against infringers in order to prevent further infringement and recover the losses incurred from any actual infringement.

Avoiding litigation is an essential element of creative projects requiring due consideration of existing IPR as well as the application of the appropriate protection of new inventions. For SISSDEN, this will require research of these areas which can be both complex and time-consuming for the novice to IPR. Reducing the risk of litigation and ensuring adequate protection of SISSDEN inventions is highly expedient.

6.1.1 Patents

A patent is an exclusive right granted by the State for an invention, which is a product or a process that provides a new way of doing something, or offers a new technical solution to a problem.

A patent provides its owner the exclusive right to prevent or stop others from making, using, offering for sale, selling or importing the patented invention without the owner's permission.

A patent is granted by either the national or regional patent office. It is, generally, valid for 20 years from the filing date of the patent application, provided the prescribed renewal (or maintenance) fee is paid on time. A patent is a territorial right and has no effect beyond the national boundaries of the country or region (group of countries) for which it was granted. In return for the exclusive rights, the inventor is required to disclose his invention to the public by describing in detail the invention in the patent application, which is published in an official journal or gazette.

6.1.2 Trademarks

A trademark is a distinctive sign that identifies certain goods or services produced or provided by an individual or a company. The system helps consumers to identify and purchase a product or service based on whether its specific characteristics and quality – as indicated by its unique trademark – meet their needs.

6.1.3 Industrial design

An industrial design refers to the ornamental or aesthetic aspects of an article. A design may consist of three-dimensional features, such as the shape or surface of an article, or two-dimensional features, such as patterns, lines or colour.

Industrial designs are applied to a wide variety of industrial products and handicrafts: from technical and medical instruments to watches, jewellery and other luxury items; from housewares and electrical appliances to vehicles and architectural structures; from textile designs to leisure goods.

To be protected under most national laws, an industrial design must be new or original and non-functional.

This means that an industrial design is primarily of an aesthetic nature, and any technical features of the article to which it is applied are not protected by the design registration. However, those features could be protected by a patent.

6.1.4 Trade secrets

In order to be protected as a trade secret, there are generally three requirements:

- The information must be confidential or secret
- The information must have commercial value because it is a secret, and
- The holder of the information must have taken reasonable steps to keep it confidential or secret

Trade secret protection lasts for as long as the information is kept confidential. Once the relevant information is made public, trade secret protection ends.

Broadly speaking, any confidential business information which provides a business with a competitive edge can qualify as a trade secret. For example, a trade secret may relate to technical matters, such as the composition or design of a product, a method of manufacture, the know-how necessary to perform a particular operation or business or commercial secrets of a very wide and potentially unlimited range of information.

6.1.5 Copyrights & related rights

Copyright laws grant authors, artists and other creators protection for their literary and artistic creations, generally referred to as “works”. A closely associated field is “related rights” or rights related to copyright that encompass rights similar or identical to those of copyright, although sometimes more limited and of shorter duration. The beneficiaries of related rights are: performers (such as actors and musicians) in their performances; producers of phonograms (for example, compact discs) in their sound recordings; and broadcasting organizations in their radio and television programs.

Works covered by copyright include, but are not limited to: novels, poems, plays, reference works, newspapers, advertisements, computer programs, databases, films, musical compositions, choreography, paintings, drawings, photographs, sculpture, architecture, maps and technical drawings.

6.1.6 Protection of layout-designs or topographies of integrated circuits

Protection for the layout designs (topographies) of integrated circuits is not yet fully unified within IPR but broadly follows the Washington Treaty of 1989, incorporated by reference into the TRIPS Agreement of the World Trade Organization (WTO) signed in Marrakesh, Morocco on 15 April 1994 subject to the following modifications⁹³:

“... the term of protection is at least 10 (rather than eight) years from the date of filing an application or of the first commercial exploitation in the world, but Members may provide a term of protection of 15 years from the creation of the layout-design; the exclusive right of the right-holder extends also to articles incorporating integrated circuits in which a protected layout-design is incorporated, in so far as it continues to contain an unlawfully reproduced layout-design; the circumstances in which layout-designs may be used without the consent of right-holders are more restricted; certain acts engaged in unknowingly will not constitute infringement.”

⁹³ https://www.wto.org/english/tratop_e/trips_e/t_agm0_e.htm

Definition of integrated circuit and layout-design

Article 2 of the IPICT Treaty gives the following definitions:

“(i) ‘integrated circuit’ means a product, in its final form or an intermediate form, in which the elements, at least one of which is an active element, and some or all of the inter-connections are integrally formed in and/or on a piece of material and which is intended to perform an electronic function,

(ii) ‘layout-design (topography)’ means the three-dimensional disposition, however expressed, of the elements, at least one of which is an active element, and of some or all of the interconnections of an integrated circuit, or such a three-dimensional disposition prepared for an integrated circuit intended for manufacture ... ”

Conclusion: There are legally defined protections for IPR that cover a wide-range of creations and innovations. These are not yet fully mature with some types of inventions remaining outside this scope. Software, for example, cannot yet be patented in the EU. This is of relevance to the SISSDEN project.

6.2 SISSDEN assets - a provisional IPR Audit

IPR audit is a systematic review of the IPR owned, used or acquired which is relevant for the assessment and management of risk, and which furthers the implementation of best practices in IPR asset management. In terms of business events such as IPO’s, mergers, takeovers, etc., the scope is necessarily a thorough and detailed assessment of an entire organisation’s assets. For SISSDEN the scope is an appropriately scaled down version that considers the architectural components relevant to the project. Project partners may contribute existing components (background) or be involved in the creation of new components (foreground). An IPR audit for SISSDEN will assess each partner component as either background or foreground in the context of the project’s architectural requirements.

The following section is a guideline on how to carry out an IPR audit and why the process is necessary. The scope of an IPR audit for SISSDEN is specific to the project and partners should discuss the relevance of the guidelines and adapt these to project requirements.

Guidelines for a SISSDEN IPR audit

An IPR audit involves undertaking a comprehensive review of IPR assets, related agreements, relevant policies, and compliance procedures.

An IPR audit helps in the process of making, and updating, an inventory of its IPR assets, and to analyse:

1. How the IPR assets are used or unused.
2. Whether the IPR assets used are owned by individual partners or by others.
3. Whether these IPR assets are infringing the rights of others or others are infringing on these rights
4. Determine, in consideration of the above, what actions are required in respect of each IPR asset, its relevance to the business goals of the project.

The purpose is to identify ownership of project assets, to identify possible threats or conflicts of interest, and to provide guidance in the making of business and IPR strategies that may help maintain and improve the competitive position of SISSDEN in the relevant market(s).

Generally, IPR audits can be classified into three main groups: General purpose IPR audit, Event-driven IP audit and Limited purpose focused IP audit. A general purpose IPR audit is mainly relevant to businesses or organisations undergoing strategic reorganisation which necessitates a comprehensive IPR audit. An event-driven IPR audit may be prompted by the need for “IPR due diligence” when a specific event such as a new joint venture, transactions involving IPR assets, launching a new product or service or licensing of an IPR asset. Thirdly, a limited purpose focused IP audit tends to be situational and is typically used to justify a certain legal position or valuation of individual IPR assets.

There is no ‘one size fits all’ set of guidelines to IPR auditing: the scope is determined by the requirement. For SISSDEN the scope is narrowly limited to existing partner background or project work foreground.

Conclusion: An IPR audit is used to assess and manage the risk to intellectual property assets. The scope can be tailored to requirement which for SISSDEN encompasses existing partner background or project work foreground.

The IPR Audit

To carry out an effective IPR audit, a relevant level of knowledge about IPR issues is required. For a thorough assessment, this would involve a team of IPR experts, which may consist of internal or external expertise. For a relatively small sized project, such as SISSDEN, a basic awareness of the issues surrounding IPR should be sufficient. For SISSDEN, the involvement of external expertise would be a costly and, most likely, an unnecessary use of resources. However, as the project develops it may be necessary to revisit and to reassess SISSDEN IPR requirements.

Developing a provisional register of partners’ IPR assets

An essential item within an IPR audit is a register of IPR assets. For SISSDEN, it would suffice to compile a list of the background and foreground architectural components that partners are either using or will be involved in developing.

A vital element of the SISSDEN project is that existing background components, such as Access Rights to data feeds, have been granted by partners based on royalty-free non-commercial victim notifications and research for the duration of the project only. Additionally, initial honeypots will be mostly open source although, currently one exception to this scenario is that of “spampot”. The rights surrounding the use of all components shall require assessment as appropriate.

For the SISSDEN IPR asset list, or register, proposed future developments should be included to serve as a reminder that IPR issues may be involved at a later stage of the project. As the current status stands software, the architectural component being developed during the lifetime of the SISSDEN project, cannot be patented in the EU.

A register of SISSDEN Initial Technical Architecture Logical Components is available in D3.3 Initial technical architecture.

Conclusions and recommendations – It is advised that an IPR audit is adopted within SISSDEN processes. This is to incorporate a list of the background and foreground architectural components that partners are either using, or will be involved in developing,

The recommendation is for an initial IPR audit be completed by M9. This is available in D3.3 Initial technical architecture, titled ‘Initial Technical Architecture Logical Components’.

Due to the size and nature of the SISSDEN project it is not foreseen that the use of external expertise will be a requirement but this should be reassessed as the project progresses. This should be carried out by M30.

A final audit of SISSDEN IPR should be completed by M30.

6.3 Risks to SISSDEN assets

Inadequate asset protection is recognised as a major risk to IPR. An IPR audit provides an opportunity to assess the risk and to take preventative actions.

Another type of risk to intellectual property is unfair competition, which is also recognised as a major liability to intellectual assets and protection in law is available. This is provided for under Article 10bis of the Stockholm Act (1967, an amendment to the Paris Convention. It reads as:

“(1) The countries of the Union are bound to assure to nationals of such countries effective protection against unfair competition. Any act of competition contrary to honest practices in industrial or commercial matters constitutes an act of unfair competition.

The following, in particular, shall be prohibited:

- all acts of such a nature as to create confusion by any means whatever with the establishment, the goods, or the industrial or commercial activities, of a competitor;
- false allegations in the course of trade of such a nature as to discredit the establishment, the goods, or the industrial or commercial activities, of a competitor;
- indications or allegations the use of which in the course of trade is liable to mislead the public as to the nature, the manufacturing process, the characteristics, the suitability for their purpose, or the quantity, of the goods.”

This Article serves to supplement the protection of industrial property rights, such as patents and registered trademarks, in cases where an invention or a sign is not protected by such a right. Unfair competition covers many acts and requires adequate consideration during an IP audit and risk assessment.

Conclusion - For SISSDEN assessing the risk to IPR Assets is not considered a major task and can be facilitated through the Table of Initial Technical Architecture Logical Components, available in D3.3 Initial technical architecture, as outlined in 6.2.1 above.

6.4 Asset protection

6.4.1 Patent & IP searches relating to SISSDEN

The Patent protection scheme involves a number of processes and begins with; a) searching for existing patents and, b) patent filing.

- a) Searching for existing patents: There are a number of ways to search for existing patents. WIPO provides free-of-charge database suitable for initial simple searches called Patentscope, <https://patentscope.wipo.int/search/en/search.jsf>. Here, it is possible to search through 58 million patent documents including 3 million published international patent applications (PCT). Fee-paying searchable database are also available and offer value-added patent information. A list of these is available through the Patent Information Users Group (PIUG) at www.piug.org/vendors.php.
- b) Patent filing: This can be a complex process as patents are granted on a country specific basis and only for 20 years at a time. However, the Patent Cooperation Treaty (PCT) makes it possible to seek patent protection for an invention simultaneously in a large number of countries by filing a single “international” patent application instead of filing several separate national or regional patent applications.

6.4.2 Utility models

Utility models are similar to patents in providing protection for technical inventions and a limited exclusive right that prevents others from commercially exploiting the invention as a sort of “short-term patent”. This type of protection is suited to inventions making only small improvements or adaptations to an existing product, or for an invention that is intended for a short commercial life. The time scale of protection is usually between 6 to 10 years. Utility model protection is only enforceable within the country in which it is granted.

Overall, a utility model is cheaper, registration is simpler and less stringent than that required of a full patent. It is useful when innovation is intended to be incremental and is especially useful in technology and mechanical innovation.

However, there is less legal security attached to utility models and third parties may question its value when considering a licensing agreement. It is especially useful when used to complement patent registration.

6.4.3 Trademarks

In principle, a trademark registration will confer an exclusive right to the use of the registered trademark. This implies that the trademark can be exclusively used by its owner, or licensed to another party for use in return for payment. Registration provides legal certainty and reinforces the position of the right holder, for example, in case of litigation.

6.4.4 Others

Trade secrets - Another form of asset protection is provided through trade secrets. Technical information such as designs and drawings of computer programs, commercial information such as

list of suppliers and clients, advertising strategies, formulas and source code can all be protected as trade secrets.

The legal protection of trade secrets is covered under laws against unfair competition and practices such as industrial or commercial espionage, breach of contract and breach of confidence. Each case is considered independently. There is no “defensive” protection as trade secrets are not made public. Prior art may not automatically be claimed as technical information may be arrived at independently.

Defensive publication - Can be used as a form of stating prior art before filing a patent application by disclosing information in the public domain. However, this can limit the possibility of obtaining patent protection, thereafter.

6.4.5 Licensing of IP assets

Patenting an invention adds IP asset value and increases the possibility to license, sell or transfer to a third party. Legal ownership of a technology is demonstrated through appropriate intellectual property (IP) protection. Further, this alleviates suspicion between parties when discussing technology transfer. Once IP ownership is established it is possible to enter into a licensing agreement with an interested third party who will be able to use the patented product for a fee.

There are three main types of licensing agreements:

- 1) Technology License Agreement - the licensor authorizes the licensee to use the technology under certain agreed terms and conditions. It is, therefore, a contract freely entered into between two parties and contains terms and conditions so agreed. In a Joint Venture a license agreement may be concluded by the parties concerned regulating the use of the proprietary information.
- 2) Trademark Licensing and Franchising Agreement - a trademark or service mark is used to distinguish the goods and services of an enterprise with an implied reference to quality and reputation. To ensure the continued quality of reputation the trademark owner through law or by contract is advised to maintain a close connection with the licensee to ensure that the quality standards are maintained. With a franchise agreement, the franchiser may team up with another enterprise (franchisee) who may add additional expertise in providing goods or services directly to the consumer. The franchiser will ensure, through the supply of technical and management skills, that the franchisee maintains the quality and other standards in relation to the use of the trade or service mark.
- 3) Copyright License Agreement – this is mainly appropriate in creative or literary fields.

IPR ownership and licensing widens the possibility of business expansion through the manufacturing, selling, distribution and marketing of services and goods. However, a license agreement is restricted to countries where the IP is legally protected and it is important to ensure that full protection is available before entering into any license agreement.

Conclusions and recommendations - For SISSDEN the creation of IPR is mostly development of multiple discrete partner owned software components, plus generating a shared data set using a combination of these components. Since software is not currently patentable in EU, the opportunities for IPR asset protection may, at present, be limited. The situation will be monitored during the project lifetime and reassessed accordingly.

This forms part of the initial assessment for M9. The recommendation is to reassess for final analysis at M30.

6.5 Towards a business strategy

The value of IPR assets is established through a system of legal protections as outlined in previous sections. Without protections in place there is a risk that competitors may take advantage of the business opportunities that SISSDEN's new technologies will afford. For the architectural components used and created in SISSDEN, this is not considered to be a high risk although it is necessary to demonstrate that the issues have been fairly considered. As business opportunities are explored beyond the lifetime of the project the IPR situation will be revisited with a view to capitalising upon possible returns and profitability. The use of IPR protection, the possibility of licensing agreements, or other forms of agreements with third parties will be included within discussions on possible future business ventures.

In summary, the opportunities offered by IP protection are:

- IPR assets offer the opportunity to generate an income through the licensing, sale, or commercialization of the IPR-protected products or services.
- Investors and financing institutions will view IPR as added value.
- Protected IPR assets are more attractive in a potential sale, merger or acquisition.

IPR protection is a continuous process that begins with accounting for, and valuing, IPR assets. For SISSDEN this means clearly identifying all components being offered as background by individual partners and to track who owns and has access rights to them. This is provided for in the list of architectural components outlined above. As the project develops, components built as foreground necessitate review and assessment as to future business opportunities and what added value IPR can usefully, and cost-effectively, contribute.

The project's Consortium Agreement and Grant Agreement regulate the SISSDEN approach to IPR according to best practice as set out in the DESCA project (www.desca-2020.eu/). The CA is a legally approved agreement signed by all partners and, as such, forms the basis for all SISSDEN work. The rules for determining ownership of results of the project are therefore clear. However, the full range of expected results (foreground), and anticipated exploitation, is not expected to be known in detail until later in the SISSDEN project. For that reason, it is recommended that:

- an IPR review focused on exploitation of background and planned foreground as foreseen in the initial architecture is executed initially at M9,
- a final IPR review is only completed at M30, once the work on foreground results is nearing completion and the full range of developed IP assets is possible to assess.

Further information is available at the Horizon2020 IPR Helpdesk <https://www.iprhelpdesk.eu/>.

Conclusions and recommendations: It is important to know and understand the value of SISSDEN assets to be able to maximise business opportunities beyond the lifetime of the project. An initial advisory register of assets to be found in D3.3 Initial technical architecture, titled 'Initial Technical Architecture Logical Components' suffices for this first analysis at M9.

It is further recommended that this advisory register is maintained and updated as the project progresses with a final version available at M30.

7 Glossary & Acronyms

European IPR Helpdesk - The European IPR Helpdesk is a project funded by the European Commission under Grant Agreement No 641474, and managed by the Executive Agency for Small and Medium-sized Enterprises (EASME). It provides free-of-charge, first-line advice and information on Intellectual Property (IP).

European Patent Office (EPO) - The European Patent Office for Europe supports innovation, competitiveness and economic growth across Europe through its services delivered under the European Patent Convention.

Hague Agreement Concerning the International Registration of Industrial Designs - The Hague Agreement governs the international registration of industrial designs. First adopted in 1925, the Agreement effectively establishes an international system – The Hague System – that allows industrial designs to be protected in multiple countries or regions with minimal formalities.

IPIC Treaty or Washington Treaty (Intellectual Property in Respect of Integrated Circuits) - The Washington Treaty was adopted in 1989 and provides protection for the layout designs (topographies) of integrated circuits.

Locarno Agreement Establishing an International Classification for Industrial Designs – establishes a classification for industrial designs (the Locarno Classification). The competent offices of the Contracting States must indicate in official documents reflecting the deposit or registration of industrial designs the numbers of the classes and subclasses of the Classification to which the goods incorporating the designs belong. This must also be done in any publication the offices issue in respect of the deposit or registration of industrial designs.

Madrid Agreement Concerning the International Registration of Marks - the International Registration of Marks is governed by the Madrid Agreement, concluded in 1891, and the Protocol relating to that Agreement, concluded in 1989. The system makes it possible to protect a mark in multiple countries by obtaining an international registration that has effect in each of the designated Contracting Parties.

Nice Agreement Concerning the International Classification of Goods and Services for the Purposes of the Registration of Marks - establishes a classification of goods and services for the purposes of registering trademarks and service marks (the Nice Classification). The trademark offices of Contracting States must indicate, in official documents and publications in connection with each registration, the numbers of the classes of the Classification to which the goods or services for which the mark is registered belong.

Paris Convention for the Protection of Industrial Property - Adopted in 1883, The Paris Convention applies to industrial property in the widest sense, including patents, trademarks, industrial designs, utility models, service marks, trade names, geographical indications, and the repression of unfair competition. This international agreement was the first major step taken to help creators ensure that their intellectual works were protected in other countries.

Patent Cooperation Treaty (PCT) - makes it possible to seek patent protection for an invention simultaneously in multiple countries by filing an "international" patent application. Such an application may be filed by anyone who is a national or resident of a PCT Contracting State. It may generally be filed with the national patent office of the Contracting State of which the applicant is a national or resident or, at the applicant's option, with the International Bureau of WIPO in Geneva.

Patent Law Treaty (PLT) - adopted in 2000 with the aim of harmonizing and streamlining formal procedures with respect to national and regional patent applications and patents and making such procedures more user friendly. With the significant exception of filing date requirements, the PLT provides the maximum sets of requirements the office of a Contracting Party may apply.

Singapore Treaty on the Law of Trademarks - The objective of the Singapore Treaty is to create a modern and dynamic international framework for the harmonization of administrative trademark registration procedures. Building on the Trademark Law Treaty of 1994 (TLT), the Singapore Treaty has a wider scope of application and addresses more recent developments in the field of communication technologies.

Strasbourg Agreement Concerning the International Patent Classification – establishes the International Patent Classification (IPC) which divides technology into eight sections with approximately 70,000 subdivisions. Classification is indispensable in the retrieval process of patent documents during the search for "prior art", and used by patent-issuing authorities, potential inventors, research and development units and others concerned with the application or development of technology.

Trademark Law Treaty (TLT) - The aim of the Trademark Law Treaty (TLT) is to standardize and streamline national and regional trademark registration procedures. This is achieved through the simplification and harmonization of certain features of those procedures, thus making trademark applications and the administration of trademark registrations in multiple jurisdictions less complex and more predictable.

Vienna Agreement Establishing an International Classification of the Figurative Elements of Marks - establishes a classification (the Vienna Classification) for marks that consist of, or contain, figurative elements. The competent offices of Contracting States must indicate in official documents and publications relating to registrations and renewals of marks the numbers of the categories, divisions, and sections of the Classification to which the figurative elements of those marks belong.

WIPO (World Intellectual Property Organization) - An intergovernmental organization which in 1974 became one of the specialized agencies of the United Nations system.

WIPO Convention - The constituent instrument of WIPO, signed at Stockholm on July 14, 1967, came into force in 1970 and amended in 1979.

WIPO Copyright Treaty (WCT) - A special agreement under the Berne Convention which deals with the protection of works and the rights of their authors in the digital environment. In addition to the rights recognized by the Berne Convention, they are granted certain economic rights. The Treaty also deals with two subject matters to be protected by copyright: (i) computer programs, whatever the mode or form of their expression; and (ii) compilations of data or other material ("databases").

Bibliography

**WIPO Intellectual Property Handbook WIPO PUBLICATION No. 489 (E) ISBN 978-92-805-1291-5
WIPO 2004 Second Edition Reprinted 2008, <http://www.wipo.int/portal/en/>**