European Journal of Law and Technology, Vol 10, Issue 1, 2019

EJLT European Journal of **Law and Technology**

No contradiction between Cyber-Security and Data Protection? Designing a Data Protection compliant Incident Response System

Stephanie von Maltzan[1]

Abstract

Incident Response has become an important component of cybersecurity. The usual security measures are often powerless against new and targeted attacks, also known as IT-Security incidents. Key issues such as information exchange formats and sharing platforms remain on the agenda of the cybersecurity community, especially for incident responders. Incident Response activities require additional processing of personal data, so may themselves create a privacy risk. Current developments towards Incident Response show that systems are increasingly insecure to data breaches, especially due to the massive amounts of personal data and the possibility of linking this data to personal identifiers. Therefore, the joint project ITS.Overview[2] has set itself the goal of creating a detailed overview of IT-Security incidents in different industrial sectors that can be correlated and exchanged among companies to be able to quickly identify cyberattacks.

This article aims to offer an initial assessment of data protection measures using Incident Response management. The key problems in this context are legal and technical barriers. The main factors are the possibility of entering free text in Ticketing Systems and the legal obligations for sharing information under the General Data Protection Regulation (GDPR), as well as lack of interest and, due to trust issues, the fear of sharing information. Furthermore, the conflict between IT-Security on the one hand and informational self-determination on the other hand must be resolved by the technically and legally correct use of Incident Response.

Keywords: Cyber-Security; Data Protection; Incident Response; Ticketing System; Malware Information Sharing and Threat Sharing Platform, Data Minimisation, Privacy by Design and Default

1. Introduction

Today's world is not only characterised by the processing of a massive amount of personal data but also by an increasing number of data breaches.[3] The increasing amount of breaches suggests that not only the number of security breaches are going up, but they are increasing in severity as well. Cybersecurity is a rapidly evolving sector. In the German economy, cybercrime costs businesses more than 10 billion Euros annually.[4] New types of security-related incidents[5] emerge frequently. Due to the volatility, force and pace with which technological innovation is occurring in the global economy, cyber risk has become a huge contemporary threat to all actors. Preventive measures are important to secure IT systems. To overcome this challenge, a successful Cyber Security strategy must be able to quickly identify and resolve attacks as well as offer a detailed overview of IT-Security incidents to ensure appropriate IT-Security. Incident Response is an organised approach used by IT-Security officers to detect and mitigate attacks and vulnerabilities on IT-Security processes and falls under the generic term "Risk Management" which is an activity that deals with the evaluation and prioritisation of risks and the analysis, implementation, control and monitoring of implemented measurements in order to manage IT risks. This involves preparatory measures and processes such as addressing vulnerabilities before they are exploited, reactive measures such as detecting attacks in real-time and prioritising them for response, and post-incident measures such as removing any vulnerabilities that were exploited. The concept of Incident Response has become widely accepted and implemented in the business environment. Responding to an incident immediately will help a company minimise losses, mitigate exploited vulnerabilities, restore services and processes, and reduce the risks that future incidents pose. Continually monitoring incidents is therefore essential. Establishing clear policies and procedures for prioritising the handling of incidents is critical, as is implementing methods of collecting, analysing and sharing of data. These methods raise various legal questions.

In view of the increasing threats posed by both external and internal attacks on IT systems, the increasing complexity of cyber-attacks requires more effective information sharing among companies and authorities. Companies that want to resist current attacks must be able to assess in real time which of their systems are or could be affected by a cyber-attack or a data breach. Identifying and dealing with such vulnerabilities and security incidents as quickly as possible is one of the basic principles of information security. For this reason, a reliable and detailed overview of the situation and prognosis of the incidents that occur is of immense importance. In order for this to happen, secure and effective information exchange and the sharing of information must take place.[6]

Incidents are usually documented by using a Ticketing System. A Ticketing System offers a variety of possibilities for processing security incidents. The ticket, which is associated with an incident, is continuously updated by analysts during the process until the incident has been resolved. To resolve incidents, the Incident Response team needs to use this information itself and may also share it with other companies. By combining the Ticketing System with a collaboration sharing platform such as Malware Information Sharing and Threat Sharing Platform (MISP)[7], these security incident indicators can be shared and correlated with other companies as trusted partners. Based on this data analysis, the companies can quickly take suitable steps to ensure appropriate IT-Security. The ticket will also be correlated and enriched with Open Source Intelligence (OSINT) – publicly available information, from open sources such as blogs and other feeds – to create an overview about the IT-Security threats in different industrial sectors. Such a picture consists of a variety of technical and non-technical information. The creation, exchange and correlation of these pictures makes it possible to prevent and solve attacks. This is applied to a range of practical detection, notification and information sharing techniques commonly used in Incident Response. The aim of this article is to show how these do in fact protect, rather than threaten, the privacy[8] and data protection rights.

This data analysis requires the processing of several types of data and information that is associated with identifiers, such as IP and email addresses and server logs, which can be subject to stringent rules applicable to personal data and require companies to comply with data protection.[9] Due to the collection and correlation of a massive amount of data, which is inherent to this system, particular attention must be paid to implementing Ticketing Systems and MISP in accordance with data protection requirements.

The research is motivated by the lack of privacy protection features in Incident Response IT systems.[10] This project aims to embed privacy protection into the development of technologies starting from its earliest phase, and at every subsequent stage of development, to ensure a level of security appropriate to the inherent risk in the data being processed. This will include, for example, measures to ensure that any data is unintelligible to any person who is not authorised to access it. Wider sharing will be covered by a clear policy by using Traffic Light Protocol (TLP), to indicate whether recipients can distribute data further. Protocols such as TLP allow for information to be shared in a more structured way in face-to-face communication. With special regard to the General Data Protection Regulation (GDPR) the project considers the legal requirements and privacy enhancing technologies[11] when processing personal data for legitimate interests. The fines for not being compliant with the GDPR can be high. Consequently, it is vitally important that companies anticipate the regulatory environment.

The author intends to explore the issues outlined above and discuss the legal basis of data processing in the distinction of possible configurations of the framework like On Premises (On Prem) and Software as a Service (SaaS), the state of the art and give baseline examples for Privacy by Design and Default. Furthermore, the author will argue that system design is the key to bridge the gap between Cyber Security and Data Protection.

2. Incident Response by using a Ticketing System and the Malware Information Sharing and Threat Sharing Platform (MISP)

A Ticketing System as well as MISP will collect, exploit and share a massive amount of data. Because personal as well as technical data will be collected, the GDPR will be applicable. Art. 3 GDPR defines the territorial scope of the regulation. The GDPR will apply to companies which have EU "establishments", where personal data are processed "in the context of the activities" of such an establishment. [12]

In brief, under the GDPR, the concept of personal data has been expanded to include any information relating to a data subject. Art. 4 (1) GDPR defines personal data as "any information relating to an identified or identifiable natural person (data subject)". In addition, the article stipulates that identification numbers, location data and online identifiers with reference to an identifiable natural person are also personal data. It must therefore be held that data that does not constitute personal data or data which has been rendered anonymous are out of the GDPR's scope.[13] But technological advances have made it common practice to aggregate and combine seemingly non-personal information to identify individuals.[14] As a result, all data may potentially be personal and there is no "meaningless data".[15]

This project covers a three-stage processing, which includes "access" to the data shared by data collectors (Ticketing System or OSINT), analysis of the data received and distribution of this data with trusted parties. It should be noted that the collection and analysis of data for internal use within a Ticketing System is a separate purpose from the sharing of information with third parties and must comply with Art. 5 (1)(b), 6 (4) GDPR.

2.1 Collecting security incidents by the use of a Ticketing System

Incident Response is typically ticket-based. Ticketing Systems are used to create, assign, update and track tickets across an organisation. A ticket element, within the Ticketing System, is a running report on a particular problem caused by incidents or vulnerabilities. This format enables companies to describe a possible problem in IT security by entering free text and correlate or share this ticket among companies in order to generate a solution. Examples for the contents of such a ticket could be the description of an incident, attempted solutions or additional information. Additional information includes Indicators of Compromise (IOCs), company-internal sensor data - for example, through Intrusion Detection Systems (IDSs) – as well as possible pathways of infections. This data often contains information linked to personal indicators such as Internet protocols or e-mail addresses.

Where processing is necessary, the justifications in Art. 6 GDPR should be used. According to the GDPR, the collection of data can be based on the consent[16] – for example, through work agreements and an additional consent by entering a ticket – of the data subject or on a legal basis that permits processing. These requirements can be met by including relevant provisions in service level agreements and also in terms of use.

Databases and data should also be secured using technical means. Art. 5 GDPR outlines six data protection principles that companies need to follow when collecting, processing and storing personal data. The controller is responsible for complying with the principles. Where appropriate to the purpose, access controls can ensure that only authorised users have access to the content. To ensure data protection compliance, the IT-Security officer takes account of technical and organisational measures, particularly with regard to Privacy by Default. In particular, the input of free text is a challenge in relation to the GDPR. Collections of free text may contain personal data but it is almost impossible to find and might only be classified by sophisticated Data Mining procedures. Furthermore, the data protection principles – in particular, the principle of data minimisation[17] – must be discussed due to the amount of data being entered. Some of these risks are technically unavoidable but can be reduced. For example, a ticket could offer structured input fields and reduce free text entry to a minimum, and policies could be set up concerning appropriate storage times and deletion options.[18] In addition, technical and organisational measures must also be implemented and the need for protection determined, thus classifying the data. The aim of this determination is to identify what protection requirements the data has with regard to the IT principles of confidentiality, integrity and availability and what type of data protection and data backup measures are required and to what extent. This need for protection is based on the possible damage associated with the breach.

Personal content exists in inherently unstructured forms. Effective data protection requires an understanding of what is considered as personal data. Understanding where and how personal data is used drives more informed security decisions. With more accurate classification incorporating user knowledge, security officers can better protect all data. Defining classification and how the data is handled is critically important. Data classification is a process to categorise different types of data based on various criteria driven by, for example, the German Federal Office for Information Security (BSI). The 3-step model of the German Federal Office for Information Security constitutes important guidance.[19] In order to define classification categories, it may help to ask what the data types are, where the personal data is located and who the data subject is, how the personal data is used and shared and, how the personal data is governed.

In addition, a pop-up message could be used to point out data processing when entering personal data. However, this has a minimum level of, or even no, security, since such a message is usually clicked away without being read.[20]

Reducing free text fields is also important to prevent data quality errors that result from the manual data entry. Data quality management mechanisms in this context are an important issue.[21] By using different kinds of data formats and transport mechanisms, such as STIX[22] and TAXII[23], a lot of effort is put into structuring information.[24]

2.2 The legal basis for collecting data from Open Source Intelligence (OSINT)

In the context of ubiquitous computing and Open Source Intelligence[25] (OSINT) a vast array of information has become retrievable with the click of a mouse. This, in turn, has led to new perceptions about how the processed data – known as big data – may be used for Cyber-Security purposes. The use of OSINT is growing significantly.[26] This includes the mining of Social Media Intelligence (SOCMINT).[27] Data Mining techniques have enormously expanded the possibilities and the powerfulness of detecting and mitigating risks as they allow managing larger amounts of data and processing them in a faster and more sophisticated way. New strategies for using OSINT are also designed to anticipate national security threats such as international terrorism. It is not widely known that information from social media is being gathered and monitored. From a data protection rights perspective, the gathering of OSINT demands proper checks and balances. This is especially important, when using and exchanging this data. OSINT is data collected from publicly available sources, including social media, that has been discovered, determined to be of intelligence value.[28] It is the information “that anyone can lawfully obtain by […] observation”.[29] Social media can also include forums or blogs as well as platforms such as Twitter. Twitter occupies a certain hybrid position because it also offers users non-public communication channels. Twitter is nevertheless focused on the presentation of public communication. The term "publicly available" is not defined by law. This includes information in any form that is generally available to a wide range of people.[30] It is only important that the content is accessible to the public and not to a specific group of people through privacy settings. The decisive factor for determining the public is whether the data was made available to the public or only within a closed group or circle.

This is not a problem if data can be freely accessed on the Internet without registration. Social media sets different thresholds for access. This raises the question which information can no longer be regarded as accessible if – for example by registration – access barriers exist. According to the term, data is regarded as public if there is no, or only an insignificant, de facto restriction. This applies in particular to technical access barriers to make the access more difficult for bots and crawlers – if no additional individual requirements for access are made. An individual access exists if the login is specifically used to check that the content belongs to the group of addressees. For registration on, for example, Twitter, there are no special technical restrictions. It is accessible to everyone without a special access threshold. In the present case, the information shared by the network is to be regarded as public.

An important problem with the processing of the information is that numerous data, available on open social media, is related to individuals. For most people this data mining takes place without knowing that the data subject is being “profiled”. In addition, the Council of Europe highlighted the risk of automatic data processing.[31] Contrarily, officials[32] and some legal commentators[33] argue that social media is part of the public domain and therefore anyone is able to access it and justify it on the basis that where users disclose personal data on social media, they do so knowing that the terms and conditions of the social media platforms almost invariably state their data may be shared with others. This does not reflect the reality of social media use. Even in the simplest case, where the data subject has knowingly disclosed personal data, it is simply not credible to argue that accepting the terms and conditions negates any kind of expectation of privacy. Such consent is neither specific nor informed and has become effectively illusory.[34] Hence the lack, in the main, of a legal debate around the collection and sharing of OSINT without consent and usually, knowledge, of the data subject. Regardless of the fact that some data subjects provide this information voluntarily and that it can be accessed online without significant barriers, it is comprehensively protected as personal data by the GDPR.[35]

The first question to be asked is whether a legal basis is necessary regarding the use of “generally accessible data"[36]. Under the GDPR, the term "generally accessible data"[37] does not appear explicitly, although generally accessible data provides, for example, the basis for scoring and big data analyses. The GDPR is mainly focused on the purpose of processing and not on the origin of the data. As a result, the processing of generally accessible data is also subject to restrictions.[38] Its mere existence in public space does not authorise third parties to use the data.[39] It should be noted that the information is rarely given deliberately by the person it relates to. For information that is obviously not made public and consent is not apparent from the circumstances, Art. 6 GDPR may be considered in addition to consent. Therefore, Art. 6 (4) GDPR specifies general conditions for lawfulness of data processing – not based on consent – for different purposes other than those for which the personal data was initially collected. Leaving the controller to conduct the assessment, the different purpose should be compatible with the original purposes, including taking into account “(…) c) the nature of the personal data (…); d) the possible consequences of the intended further processing for data subjects”. Recital 47 states that the reasonable expectations of users of social media should be taken into account. As a result of the public availability, the data subject, who expressly provides his or her data to the public, renounces the specific protection of GDPR regarding the balancing test.[40] Ultimately, it depends on the distinction between primary and secondary data and the processing context. The mere knowledge which corresponds to the type of use by permission does not require any legal basis. However, the collection and evaluation of information are accompanied by a greater intensity of intervention, which requires a legal basis. It should be noted that in the case of primary data the public availability means a partial renunciation of confidentiality. An absolute protection would not justify the circumstance of a conscious sharing. Based on this, the possible use of secondary data could override the interest of the controller. At least in those cases where it can be expected – for example when reporting security incidents – that these data is of interest to the public and is not perceived only by a limited group of people, the interest of the processing overrides the fundamental rights of the data subject.

It is, thus, of utmost importance to draw the limits of data processing, integrate the appropriate data protection safeguards into the applications and find the right balance between making use of Incident Response and protecting personal data. There remain, as necessary prerequisites for legitimising the processing, obligations which must be met concerning principles of fairness and data minimisation referred to in Art. 5 GDPR.[41] This will be explained later on.

2.3 The legal basis regarding the processing of data in sharing information about incidents

As well as detecting incidents within Ticketing Systems, companies may well wish to disclose and share this security-related information about a relevant attack or vulnerabilities to outside parties. Vulnerabilities and security incidents are rarely specific to a single company. Knowing how an attack was detected and mitigated can help other companies to take preventive and repressive actions. However, sharing security-related information among companies by using the MISP[42] sharing platform poses key challenges for data protection. MISP is a trusted collaborative platform that allows the sharing and correlation of security incident indicators.[43] In this platform the company can create and manage groups (peers) with other companies and share information with those groups. New threats can be detected and mitigated more quickly in a joint-effort and the response can be adequately coordinated throughout the whole community. Therefore, the need for having reliable information sharing platforms in place will be key to successful collaboration.

2.3.1 Assessment of compatibility

As noted above, the information handled by the project is generally associated with identifiers such as IP- and e-mail addresses. When personal data is shared in MISP, this must also be legitimised by a legal basis. Special attention must be paid to the principle of purpose limitation.[44] Purpose limitation protects data subjects by setting limits on how controllers are able to use their data. This makes the purpose of data processing binding. Under this principle, Art. 5 (1)(b) GDPR states that personal data will only be collected and used for specified, explicit and legitimate purposes that are compatible[45] with the purpose for which they were originally collected. The concept of purpose limitation has two main building blocks: purpose specification and compatible use. In this case, no legal basis except from that which allowed the collection of the personal data is required. Art. 5 (1)(b) GDPR does not prohibit further processing of personal data for different purposes, but only for purposes incompatible with those originally specified. Therefore, further processing of personal data different from, but compatible with, the original purpose is not precluded. A change of purpose is only possible within the limits of Art. 6 (4) GDPR.[46] Art. 6 (4) GDPR provides a broad exception from the requirement of compatible purpose. If the new purpose is incompatible with the original purpose, the data subject’s consent must be obtained, or a different legal basis for the processing invoked. Compatibility needs to be assessed on a case-by-case basis. A substantive compatibility assessment requires an assessment of all relevant circumstances. In particular, the following key factors should be taken into account as they are factors that have been identified by the Art. 29 Working Party.[47] Whilst Art. 29 Working Party opinions are not legally binding they are considered to be indicators of good practice. [48] First of all, the relationship between the purposes for which the personal data has been collected and the purposes of further processing should be considered. According to the Art. 29 Working Party, the greater the distance between the purposes of collection and further processing, the more problematic the compatibility assessment. The other factors focus on the context in which the personal data has been collected and the reasonable expectations of the data subjects as to their further use, the nature of the personal data and the impact of further processing on data subjects and the safeguards adopted by the controller to ensure fair processing and to prevent any undue impact on the data subjects. Recital 50 states that the reasonable expectations of the data subject are decisive factors. The more surprising the further processing is, the more problematic this would be for the compatibility assessment.[49] Therefore, different kinds of safeguards, including technical and organisational measures to ensure functional separation, such as full or partial anonymisation, pseudonymisation, aggregation of data, and privacy-enhancing technologies should be taken into account.[50] The concept of technical and organisational measures will be explained later on.

In the present case, there is a change of purpose according to Art. 6 (4) GDPR. The collected personal data from a variety of different sources, was originally not collected for the purpose of detecting security incidents and ensuring IT security. The consent or the contractual basis are usually not covered by this. It requires a new legal basis and must be available not only for entire data sets but also for each individual data. This raises a number of practical difficulties. In practice, these problems require extensive and detailed contracts, work agreements and Data Protection Impact Assessments. The Art. 29 Working Party has published the final version of its Guidelines in Data Protection Impact Assessments.[51] Under Art. 35 GDPR, performing a Data Protection Impact Assessment is mandatory for any processing activity that represents a high risk to data subjects. The guidelines provide a list of nine criteria of processing – like evaluation or scoring, automated decision making with significant effect, systematic monitoring, matching or combining datasets – which require a Data Protection Impact Assessment. A table of examples provides useful comparisons for organisations assessing their own activities.

2.3.2 Legal basis of further processing

The principle of lawful processing of data is complemented by Art. 6 GDPR, which lists six categories for the legitimate processing of data. In line with the principle of lawfulness of processing, the approach of the GDPR is to not permit processing, unless this is permitted under circumstances provided in Art. 6 GDPR. The most general justification is provided by Art. 6 (1)(f) GDPR.

In the following paragraphs, five legal grounds which could be used for information sharing of personal data for the general purpose of ensuring IT-Security will be detailed.

Consent is enshrined under Article 7 GDPR and defined under recital 32. Consent should be freely given by a specific, unambiguous and informed indication of the data subject's agreement to the processing of personal data relating to him. Proper information and transparency is a key issue in any data processing operation.[52] The practical requirements are outlined in Art. 12 - 14 GDPR.[53] The transparency requirements in the GDPR apply irrespective of the legal basis for processing and throughout the technical cycle of processing. In order to be able to decide freely, informed consent is necessary. Consent involves the need for disclosure of all the relevant information that may influence the judgement and the choice of the data subject. This requires all information about the controller, the purpose of data processing and whether the controller may pass on the data to third parties. The controller must provide information so that the data subject can assess the importance and the scope of his or her consent.[54] The general information, that data is passed on to third parties, is not sufficient. It should, therefore, be noted that the consent of the data subject is not based on the consent of the transmitting party, such as the OSINT source. However, the consent of the data subject can be declared to the OSINT source. Finally, the consent can be withdrawn at any time with effect for the future. This means that the legal basis for data protection can be withdrawn ex nunc at any time. In most cases, OSINT sources cannot rely on the consent of data subjects. This follows from the type of data and the source of information itself. In summary, consent must be rejected as a legal basis. It is hardly practicable.

Nevertheless, the policies of some Computer Emergency Response Teams (CSIRTs) provide that consent is required when the data subject is the victim or the target of a threat. In addition, the information of an attack is usually not obtained directly from the attacker. Instead it is a result of an analysis thereof. In this case Art. 14 GDPR is usually applicable. This article requires that specific information, such as the identity and contact details of the controller, is provided to the data subject. Art. 14 GDPR carves out a broad set of exceptions to the requirement of the transparency principle where personal data has not been obtained from the data subject. "These exceptions should, as a general rule, be interpreted and applied narrowly".[55] Specifically, in the case of sharing attacks, Art. 14 (5)(b) GDPR is the most relevant, stating that Art. 14 (1) to (4) GDPR shall not apply if "the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing". To rely on this exception, controllers must demonstrate that the mere provision set out in Art. 14 (1) GDPR would undermine the objectives of Incident Response. This restriction needs however, to be balanced with appropriate measures such as making the information publicly available. The Art. 29 Working Party has pointed out, that, "reliance on this aspect of Article 14.5(b) pre-supposes that the data processing satisfies all of the principles set out in Article 5 and that most importantly, in all of the circumstances, the processing of the personal data is fair and that it has a legal basis"[56]. Controllers should carefully consider the circumstances and context of each situation where transparency information is required, including the potential impact of security-related incidents. Information on the existence of automated decision-making deals with the same problem. The Art. 29 Working Party has produced guidelines on automated individual decision making, which should be referred to for further guidance on how transparency should be given effect.[57]

The provision of Art. 6 (1)(b) GDPR covers the case in which the processing of personal data is necessary for a contractual or pre-contractual context. The requirements are strict as the necessity criteria will not be considered as such unless the processing is truly central and unavoidable in order to complete the transaction. The data processing in ITS.Overview is not required for the performance of a contract with the data subject.

According to Art. 6 (1)(c) GDPR, processing may be permitted in the case of a legal obligation to which the controller is subject. Control, monitoring and order functions in accordance with Art. 23 (1)(h) also justify such processing. A legal obligation could also result from the obligation to report critical infrastructures pursuant to the Directive on Security of Network and Information Systems (NIS Directive). However, this obligation does not imply that a comprehensive transfer of data such as this one is permissible in order to comply with the reporting obligation. The obligation is to detect security incidents and not to process data. Data processing is only a necessary part of the obligation to report.

Another basis for lawful processing of personal data is when processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. The scope of Art. 6 (1)(e) GDPR is twofold: it covers cases in which data controllers may be required to meet certain obligations in the public interest as well as situations in which data controllers operate as delegated authorities from government institutions. Recital 45 states that there must be a legal basis for this in Union law or in the law of a Member State. Ensuring security of the network is in the public interest, but not explicitly defined by legislation. This may be the case for CERTs or CSIRTs (collectively Computer Emergency Teams), which can use this exception to legitimise their data processing. Obviously, this option would only apply if the CERT has been given a specific legal mandate to that effect. However, neither the NIS Directive nor the GDPR expressly includes the legal basis for the processing and transfer of personal data between companies and CERTs. Only recital 72 of the NIS Directive mentions the need to process personal data when exchanging information on incidents and when complying with the obligation to report security incidents to the competent national authorities or CSIRTs. The GDPR refers to this issue in recital 49, which identifies IT-Security as a legitimate interest. The collection and further processing of personal data from OSINT and Ticketing Systems ensures appropriate IT security. However, according to Art. 6 (1)(e) GDPR, this public interest must be explicitly defined by law. Nevertheless, recitals have a strong legal character in European Union acts. Article 296 of the Treaty on the Functioning of the European Union states that acts must be accompanied by a statement, which makes the recitals part of a regulation and important for its interpretation. In the event of a contradiction – as is the case here – between recital and article, the text of the article takes immediate precedence. The legislature must, therefore, create the legal basis for data processing of personal data for CERTs. All in all, this is not applicable at large to the ITS.Overview project, as private sector partners do not operate as delegated authorities nor exercise functions of a public nature in the public interest.

Finally, Art. 6 (1)(f) GDPR may be used as a legal ground for the processing of personal data in ITS.Overview. This article, formulating the legitimate interest clause, allows the controller to process personal data if, in particular, none of the other circumstances listed in Art. 6 GDPR can be invoked as a legal basis. The lawfulness of Art. 6 (1)(f) GDPR asks for a test based on the legitimacy and necessity of the processing, and balance between the interests of controllers and data subjects. Art. 6 (1)(f) GDPR justifies this, however any particular use or sharing must satisfy the requirements "necessary", "legitimate interest"[58] of the controller or a third party and that these interests are not overridden by the fundamental rights and freedoms of the data subject. According to the Article 29 Working Party, "this balance of interest test should take into account issues of proportionality, the relevance of the personal data to the litigation and the consequences for the data subject". Comparing the assessment of the necessity and legitimacy of the proposed processing with the assessment of harm that may be caused to the data subject's fundamental rights, make it apparent whether the proposed action is necessary for the legitimate purpose or whether this purpose is overridden by the need to protect individual rights of the data subject.[59] This assessment is likely to vary from case to case. The 3-step test – necessity, legitimacy and balance of the interests – is therefore a helpful guideline. These low requirements for a justified interest are compensated for by the data subject's rights.

In the case of ITS.Overview, the main purpose of their legitimate interest, ensuring appropriate IT-Security, should be balanced against the need to protect the fundamental rights of the data subject. Recital 49 states that network and information security is an overriding legitimate interest. CERTs and CSIRTs are explicitly mentioned. The necessity of such a framework to efficiently fight incidents is justified by the character of cybercrime and the significant threat posed by attacks. The need for cooperation and information sharing is thus vital. Due to cooperation and sharing, the framework has a concrete potential to mitigate incidents. However, it must be recalled that, in the context of widespread cybercrime, users cannot fully enjoy protection of data without effective cybersecurity. Therefore, the need for security and the exercise of the fundamental right to data protection are complementary.

The collection and sharing of a massive amount of data, which is inherent to the Ticketing System and MISP, goes hand in hand with a loss of transparency, which could speak for its outweighing data subject's rights. However, publicly available data from OSINT sources is also processed. As explained above, at least in those cases where it can be expected – for example when reporting security incidents – this data is of interest to the public and not only perceived by a limited group of people. Thus the interest of processing overrides the fundamental rights of the data subject.

While the need to ensure IT Security is clearly legitimate, the proportionality assessment will bear upon the adequacy and necessity of the means used to achieve this goal, thus on the design of the ITS.Overview solution. Ensuring compliance with the essential IT-Security principles of confidentiality, integrity and availability, suitable security measures are therefore indispensable. These protection goals should be implemented in as many layers of the IT environment as possible, following a layered defence approach. The conditions of a layered defence are related to the system itself and therefore include both the hardware and software components as well as the network level. Actions, such as Privacy by Design and Default[60], that provide better protection for those rights are therefore more likely justified under Art. 6 (1)(f) GDPR. Different factors can affect the individual rights of the data subject: "what identifier, if any, is associated with the information being processed or disclosed; whether the information was gathered by a process that limits the information gathered (…) or one with no built-in limits (…); and how widely and to whom information will be disclosed"[61]. When sharing personal information, the project can add metadata that designates how this data should be handled by the recipient, especially if it might be distributed further. The most common method is the Traffic Light Protocol (TLP)[62], which defines four simple sharing levels. In addition, if a company decides to share with an external company, information is often transformed in order to remove selected personal elements. Nevertheless, anonymisation has theoretical limitations and, there are methods that can be used to reveal the original data by correlating the anonymised information with other datasets. Therefore, some very personal information elements should be removed completely – if possible for further use – from the information shared with external parties.

A practical example for sharing security-related information to trusted parties is the disclosure of IP addresses. The IP address is undoubtedly of significance for Incident Response as it is used to identify the source of an incident. The processing of personal data is an essential part of the investigation of security incidents through detection and repression.[63] However, according to the Article 29 Working Party, IP addresses can be considered as personal data because of the possibility of IP addresses being linked to a natural person.[64] Thus, whenever IP addresses are to be exchanged, GDPR is likely to be found applicable.[65] Internet protocols or e-mail addresses are indispensable for an Incident Response management. IT-Security without cooperation and information exchange is difficult to implement. The IP address is undoubtedly essential to the Incident Response management[66], as an example of personal data that is frequently used to identify the source of an incident. This can, however, put Incident Response in a complicated position. Specifically, if companies obtain information that may lead to the identification of a harmed data subject. It is quite likely that they may not be permitted to exchange this information freely with other companies, as it qualifies as personal data that may not be processed without appropriate justifications as described above. Thus, even if a company can successfully explain why it has a mandate to process an IP address under Art. 6 GDPR, this does not necessarily imply that the sharing of such personal data with third parties is also lawful. Incident Response should be cautious on this point, as a violation of the GDPR principles may expose liability. This requires a case to case balancing test. Furthermore, it should be noted that some Member States[67] have implemented specific protections and additional safeguards with respect to judicial information. Incident Response may be confronted with diverging national restrictions. Several instances of this problem are mentioned in ENISA.[68]

Data protection is regarded as the most important legal aspect concerning information sharing. More specifically, the broad scope of the personal data concept causes challenges in practice, as it can cover a large number of data types commonly collected and exchanged by Incident Response. Other difficulties include the differences between laws in different countries, and the law profession's lack of understanding of IT and security incidents in particular as well as the poor implementation of data protection safeguards in Incident Response. In summary, it can be said that, unless the information from social media is private, sensitive or otherwise confidential and/or the data is generally inaccessible, it cannot be assumed that the data subject's right of informational self-determination outweighs the legitimate interest in ensuring appropriate IT security of the controller when sharing is required to mitigate a clear and serious threat. It must also be recognised that the sharing of information – including in cross border scenarios – should not be examined fundamentally as a risk to the fundamental right to privacy, without also acknowledging that this sharing is a precondition for responding effectively to incidents. The controller can rely on Art. 6 (1)(f) GDPR – in a case to case balancing test – as justification for further processing. It should be noted that the collection of data for internal uses is a separate purpose from the sharing with third parties. This issue is made even more complicated by the cross border aspect. Indeed, Incident Response would need to be aware of what the limits of their obligations are, and what this implies with respect to the data processing.

In brief, the concept of data controller in a sharing environment is not always trivial. According to Art. 4 (7) GDPR the controller "determines the purposes and means of the processing of personal data", either alone or in partnership with other data controllers. In a peer-to-peer collaboration network, all the peers are separate data controllers for the processing activity "share information". When the peers decide to process the shared information, they become the data controller of the separate processing. It is the responsibility of the controller to ensure appropriate safeguards.

3. Risk management and data protection

New information technologies change the privacy risks we are facing, but technology can also help to minimise or even avoid risks. With the GDPR, the most relevant obligations for controllers concern data protection by design and default[69]. In particular, according to GDPR security equally covers confidentiality, integrity and availability and should be considered following a risk-based approach. This follows the principle of accountability that is enshrined in Art. 5 (2) GDPR, establishing that the data controller shall be responsible for and able to demonstrate compliance with GDPR. The higher the risk, the more rigorous the measures that the controller needs to take. Art. 5 GDPR puts data security at the core of data protection together with the rest of data protection principles, i.e. lawfulness, fairness and transparency, purpose limitation, accuracy and storage limitation.

Despite the benefits of collecting and sharing mentioned above, it cannot be accepted that Incident Response comes at a cost for privacy. The extensive collection and sharing of personal data has given rise to serious privacy concerns. In order to allow for all the benefits of Incident Response, it is of utmost importance to integrate appropriate safeguards into the applications and find the right balance between making use of Incident Response and protecting personal data. At the same time, the security of IT systems always requires the security of data.[70] Technical and organisational measures[71] must serve the purposes of data security and system protection.[72] The threats that the measures should prevent, ensuring integrity and confidentiality, include in particular unlawful processing and data leaks. The type of information collected and shared in these applications can be too sensitive to be exposed to third parties. These measures should be embedded into the design of technologies instead of being adopted as ex post remedies once privacy violations have already occurred.[73] Furthermore, these measures should address the whole process involving the individual's data as well as implement transparency. However, there aren't concrete guidelines on how to put GDPR principles into action. A first hurdle to be overcome is the potential conflicts or inconsistencies between privacy objectives and functional and non-functional requirements of the system. Therefore, legal experts are working closely with computer scientists during the entire project duration.

Ensuring appropriate[74] privacy safeguards, Art. 25 and 32 GDPR give a baseline concerning how to implement technical and organisational measures to ensure a level of security appropriate to the inherent risk to the data being processed. From a technical standpoint, Privacy by Design is a challenging endeavour. It is a multifaceted notion stemming from a variety of data protection principles which are generally not defined very precisely. In addition, these requirements may be in tension with others such as functional requirements, like ease of use. Privacy by Default requires a systemic approach to configuring systems, with high privacy protection being the default option. To implement all these requirements, a wide range of safeguards are available. This may include anonymisation, pseudonymisation, in particular encryption and as well as aggregation[75].[76] Furthermore, clear responsibilities must be attributed and security roles documented. It is a requirement that ensures only legitimate persons can access the processed data. Data access should be restricted to authorised personnel and only for legally authorised purposes such as data security and integrity. Therefore, implementation of a security policy with respect to the processing of personal data is of vital importance. Organisational security measures should be backed up by technical measures, including the use of privacy-enabling technologies. Any security measures will only be as good as the people applying it. Staff members must, therefore, be educated and trained in data security. These measures must be in place at all stages of personal data processing.

This requires a closer look at the privacy problems that originate when people interact with technical devices or their interactions are mediated by technical devices. Over the last few decades, perceived privacy has been fading away. To overcome this dilemma, the collection and sharing of personal data had to become user-controlled. User control of personal information disclosure supports users in deciding which personal information is released to whom and in which situation. When using platforms such as MISP, trust-based sharing of personal data between peers[77] via TLP or authentication by QR code should be taken into account. This classifies data with regard to their sensitivity, regulates conditions for further processing and creates trust through authentication amongst peers. TLP uses four colours to indicate sharing boundaries. It provides a simple procedure for indicating when and how personal information can be shared.[78] As a result, an Incident Response should have a well-defined sharing policy to determine what types of information can be provided to different companies.[79] Nevertheless, trust is the single most important feature of a successful cooperative relationship and a concept directly related to the term's credibility[80] and reliability. The exchange and sharing of information and knowledge regarding threats, vulnerabilities, incidents and mitigation strategies results from the company's growing need to protect against targeted attacks. In Incident Response, trust refers to the assumption by each involved company, that other companies which are involved in a transaction will share among peers as expected. In addition, each company trusts that all companies will use all necessary precautions and sensible measures to ensure that no data leakage will occur. Trust is undermined when only one party is active in sharing, without getting much in return from other parties. Data protection principles are a core component of the trust underlying the relationship between peers.[81]

Anonymisation[82] and pseudonymisation[83], in particular encryption of data, could allow the sidestepping of obligations as well as ensuring that any data is unintelligible to any person who is not authorised to access it. While encrypted data reduces the potential privacy risks due to unauthorised access (for example during data transfer), removal of personally identifiable information also reduces the risks of unintended disclosure and privacy violations.

Anonymisation is described in recital 26 as a process of modifying personal data in such a way that the data must be "stripped of sufficient elements"[84] such that the data subject can no longer be re identified. Data which is integrally anonymised doesn't need to comply with the principles of data protection.[85] Anonymisation removes the component – the possibility of identifying a natural person – that requires legal protection. Ensuring adequate data protection and achieving a balance between controllers and data subjects, anonymisation is sufficient data protection.

Determining whether anonymisation is fully accomplished requires a case-by-case examination.[86] Although, recital 26 refers to anonymised data as data in which the data subject is no longer identifiable, total impossibility of re-identification can be extremely difficult to achieve. Even if the direct identification through a single data source is no longer possible, by combining data sources anonymised data could become once again personal data. Moreover, progressive removal of personal elements can reduce the possible data utility to controllers. Perfect anonymisation is difficult in practice without compromising the utility of the data in Incident Response. Therefore, this measure is rarely practicable.[87] Due to the difficulties of achieving anonymisation, pseudonymisation has grown as an alternative to reduce data protection issues while preserving the value of the data.

The concept of pseudonymisation is defined under the GDPR as processing personal data in such a manner that a data subject cannot be singled out any more without the use of additional information. Nevertheless, that data remains personal data.[88] The processing with this data involves fewer risks for the individual, but it does not necessarily reduce it significantly. The aim of such a process is to replace the identifiable characteristics of a person with a code (pseudonym), in such a way that the data can no longer be related to a specific natural person, except for by those capable of, or authorised in, executing the reversal process. The data subject's identity is disguised in a re-traceable way. This in turn leads to a greater risk to individuals when compared to anonymous data, which doesn't need to apply with the principles of data protection. However, pseudonymous data is still subject to the GDPR, as there is a concrete risk of re-traceability. Despite the risk at stake for data subjects, this remains an important tool to help mitigate data protection risks, as pseudonyms are only indirectly identifiable[89] and the reversal process can only be conducted with a key. The key should be ideally be held by a trusted third party. According to the Article 29 Working Party, the efficiency of this processing depends on different factors that can influence the possibility of the reversal process occurring. These are at which stage the data is used, how secure it is against reverse tracing, the size of the population in which the individual is hidden, the ability to link individual transactions or records to the same person, etc.[90]

Furthermore, any information from a company to a service or between companies should preferably be encrypted using modern cryptographic techniques to render it unintelligible to intruders. All types of communications from the company should be protected. Encryption[91] – in both storage and transmission – entails changing information into a secret code to prevent unauthorised access by third parties. Encryption technologies have contributed significantly to the confidentiality of personal data, but processing of encrypted data raises many difficulties, in particular in case of the reuse of the data. However, this is a task that will be resolved during the project.

In MISP, some of the information could be considered as pseudonymised. The incident's attributes are not linked to each other and usually do not enable the identification a data subject by themselves, without additional information. Yet, combining data still bears an immanent risk of identifiability.[92] Thus, entities using anonymisation or pseudonymisation need to stay updated on advancements in technology. A requirement to use Privacy by Design/Default and privacy enhancing technologies should certainly assist in data minimisation. However, due to the necessity of processing a massive amount of data, data minimisation will not be enough to deal with processing data in Incident Response. It is worth stating that these measures don't free the controller from the GDPR obligations as pseudonymisation and anonymisation are not intended to preclude any other measures of data protection according to recital 28 GDPR. Regular Risk

Management should integrate various security controls for IT-Security systems.[93] However, recital 26 GDPR constitutes that anonymisation could fulfil this purpose. In an appropriate Incident Response, it will rarely be possible to anonymise the security-related information without making them useless for preventing or detecting local instances of the same incident. Therefore, the author suggests that, because of the increasing ease of re-identification and the near-impossibility of full anonymisation of personal data, the basic approach should be to reduce the collecting and even initial storing of personal data to the absolute minimum in conjunction with role authorisations and pseudonymisation.

In summary, full anonymisation is very hard to achieve and in most cases rarely practicable, while pseudonymisation does not release data controllers from ensuring compliance with the GDPR. Therefore, companies must bear in mind the risks and standards for anonymisation and pseudonymisation.

The selection of technical and organisational measures ensuring data protection should result from the nature, scope, context and purposes of processing and the possibility of a breach and its severity. Therefore, the state of the art should be taken into account. The system's design should respond to the technology evolution. State of the art is one of the relevant criteria based on measures outlined above. By using technical standards, it is possible to define this vague term. Global standards related to regulatory compliance and security have increasingly been adopted in Germany. Standards such as the ISO 27000 series family[94] have become common benchmarks for IT-Security systems. This sets forth robust data security and protection requirements and is already widely used in the private sector. ISO/IEC 27001 intends to bring information security under explicit management control and mandates requirements that define how to implement, monitor, maintain and improve the system. It also prescribes a set of best practices that includes access control, documentation requirements as well as corrective and preventive measures. Based on this guideline and the 3-step-theory[95], it gives specific guidance on assessing risks and implementing state of the art controls for protecting personally identifiable information. Explicitly linked to ISO/IEC 27000 concepts the standard ISO/IEC 29100 is to be seen as complementary.[96] However, measures must be regularly tested and assessed for their effectiveness and should be updated where justified. The Privacy by Design and Default approach is a continuous and iterative process.

The scope and enforcement of the GDPR brings with it challenges for small and medium-sized enterprises (SMEs). SMEs must identify the level of risk depending on nature, scope, context of processing and proactively implement appropriate measures. Taking into account the "specific characteristics of SMEs, such as limited resources, unavailability of qualified personnel and specific sectorial regulatory provisions"[97], a simplified approach for an Incident Response system is necessary. Based on this, a Software as a Service (SaaS)- based solution can help SMEs in understanding the threats and calculating their occurrence probability as well as achieving GDPR objectives.

4. Software as a Service (SaaS)-based or On Premises (On Prem) solution

The framework can be configured as On Prem or SaaS. These different infrastructure solutions[98] must protect data from many types of failures. The difference is significant, as SMEs, in particular, cannot operate Incident Response management locally. One of the core obligations for businesses, including SMEs, in GDPR compliance, is that of the security of data. While bigger companies “have the possibility to respond to and appropriately implement Incident Response systems, SMEs do not have always have the necessary expertise and resources to do so”.[99] According to ENISA, “this contextual analysis of risks however, cannot be easily performed or even brought down to the level of an SME due to the broad differences among the aspects that have to be taken into account and the familiarisation required with all GDPR provisions”[100]. This can affect the way in which personal data is processed, hindering at the same time compliance with legal obligations. In order to achieve their objectives, SMEs are increasingly depending on networks, systems and applications. The SaaS-based solution provided by the project can be adopted by SMEs in order to achieve compliance with the GDPR.

The project provides guidelines for protecting data in both On Prem and cloud-based storage infrastructures. In this part, the author will discuss the main differences and the most appropriate option with regard to data protection.

Cloud Computing is a business model that facilitates the use of computing in a scalable and flexible manner thanks to the better management of computing resources.[101] SaaS offers to outsource end-user software application based on a cloud infrastructure.[102] Cloud Computing data is processed and stored outside the private environment of the office. The user only has the preliminary choice of accessing a Cloud. After this decision, the user’s data is registered and stored by a service. For that reason, users should be adequately informed of how the technology works. The benefits of cloud computing make it appealing to a wide range of customers. Despite the management and cost advantages, there are a number of information and privacy protection concerns, in particular when the cloud is used to process personal data.[103] These concerns result from organisational customer’s apparent lack of control and oversight of the way in which personal data is protected and managed therein.[104] Further legal guidance and practical advice to comply with the GDPR is provided by The European Data Protection Supervisor (EDSP) and the European Union Agency for Network and Information Security (ENISA).[105] Therefore, equipping ordinary users with knowledge and understanding of the Cloud is indispensable. In the worst-case scenario, users will lose their data due to software or hardware failure. In conclusion, it can be stated that the user should be informed about the potential risks associated with the processing of his or her data and the company’s attempts to reduce these kind of risks (for example built-in mechanisms such as Privacy by Design, data minimisation, erasure procedures).

In contrast, the term On Prem refers to local hardware, meaning data is stored on local servers. By hosting the infrastructure in the company’s environment and managing and administering policies, rules, and reports, the company itself has the total ownership and control over data protection. But it is also to be noted, that the On Prem deployments, disaster recovery and regularly scheduled and secure backup plans must be designed and implemented by the company.

After reviewing these possible configurations, the author suggests that On Prem is the most appropriate option with regard to data protection. The lack of transparency, loss of control over the data and the lack of information about cloud operations are three major risks associated with cloud use. On Prem, on the other hand, offers a level of security and control that's simply not possible in the cloud.[106] An On Prem solution provides businesses with control over all the data, managed and handled by their own dedicated IT staff. However, a cloud-based solution frees up processing and bandwidth on-site, which means that the network operates more efficiently and even securely. There are arguments for and against adopting On Prem or a cloud-based solution. The result is reported to be dependent on the size and the financial resources of the company.

5. Conclusion

Companies are collecting a growing amount of cyber security information internally and externally in order to better protect themselves from cyber threats and maintain a strong cyber security status. Sharing information about incidents has become a precious resource of information within the IT community. However, in some situations companies may not want to share internal information due to a lack of trust and legitimate need for confidentiality.[107] A suitable Incident Response, in particular a sharing system, would provide controls and safeguards, including provisions to ensure privacy and data protection. Incident Response routinely handles personal information, therefore in the distribution step appropriate measures must be put in place to ensure that the scope of data given to external organisations is strictly controlled. In conclusion, the author suggests removing personally identifiable information or using encryption wherever possible. Admittedly, Incident Response has limitations. According to the necessity of processing a mass of information to create a detailed overview of IT-Security by using a Ticketing System, some of these measures are technically impossible to implement. The information collected and exploited for classifying purposes can't be anonymous or encrypted when reporting security incidents. This data is secure only during transfer. With more accurate classification incorporating user knowledge, the system can better protect data. Data classification is a process to categorise different types of information. Defining classification and how the data is handled is critically important. Irrelevant data should be deleted as soon as possible.[108] In order to evaluate the large datasets that are generated, Data Mining techniques for structured data can be used to improve Incident Response. However, this is a task that will be resolved during the project. Another challenge will be the collaboration between peers. First, information should only be disclosed to trusted partners. Secondly, the recipient company should only know the full IP address of the threat source, not those of the corresponding system. These local addresses can either be removed, or anonymised, by hashing or removing trailing component(s) of the IP address.[109] This means that the disclosed information will only contain external identifiers. In case of the IP address of the threat source, processing of encrypted data raises many difficulties, in particular in case of the reuse of the data. The search for solutions within MISP will be done through a chain of trusted contacts within the affected organisations. Trust is the single most important feature of a successful cooperative relationship. As a result, an Incident Response should have a well-defined sharing policy to determine what types of information can be provided to different organisations. Sharing data shall take place after authentication. The authentication is done by using QR codes. Vulnerabilities and incidents are rarely specific to a single organisation, so knowing how an attack was conducted and discovered can help others detect or prevent the same happening to them. When the framework sends specific warnings to the companies by OSINT, as well as sharing what they learned from the incident with their peers, will have a positive outcome for all companies. This needs a secure system for reporting and collaboration. A wider sharing should be covered by a clear policy and information marked, for example using the Traffic Light Protocol (TLP), to indicate whether recipients may distribute it further.

Fundamentally, collecting and sharing personal data by Incident Response systems is part of a wider debate about what legal and ethical safeguards should protect the data subject. Furthermore, the debate is moving from being merely about collecting and sharing freely accessible personal data as the companies increasingly enter personal data about their employees into the internal ticketing systems. Incident Response raises legal, as well as ethical, concerns. The House of Commons, Science and Technology Committee warn: “Given the scale and pace of data gathering and sharing, however, distrust and concerns about privacy and security is often well founded and must be resolved by industry and Government if the full value of big data is to be realised.”[110] Legal and policy instruments should also be backed up by technical solutions in order to be effective.

Bridging the gap between law and technology design is the big challenge in this project. The author takes the position that the concept of Data Protection by Design and Default is key to meet this challenge. In this process, much work is to be done in reaching the goal of sharing data in a privacy preserving manner. Above all, standards must be developed and appropriate safeguards considered.

References

Anthonysamy, P., Rashid, A., & Chitchyan, R. Privacy Requirements: Present and Future.

Armbrust, M., Stoica, I., Zaharia, M., Fox, A., Griffith, R., Joseph, A. D., . . . Rabkin, A. (2010). A view of cloud computing. *Communications of the ACM*, *53*, 50.

Article 29 Data Protection Working Party. (2017). Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679: WP248.

Article 29 Data Protection Working Party. (2018a). Guidelines on transparency under Regulation 2016/679 WP 260.

Article 29 Data Protection Working Party. (2018b). WP251: Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679.

Article 29 Working Party. (2007). WP 136: Opinion 4/2007 on the concept of personal data.

Article 29 Working Party. (2009). WP 158: Working Document 1/2009 on pre-trial discovery for cross border civil litigation.

Article 29 Working Party. (2011). WP 187: Opinion 15/2011 on the definition of consent.

Article 29 Working Party. (2014). Opinion 05/2014 on Anonymisation Techniques WP216.

Artikel 29-Datenschutzgruppe. (2013). WP 203: Opinion 03/2013 on purpose limitation.

Berendt, B., Engel, T., Ikonomou, D., Le Métayer, D., & Schiffner, S. (Eds.). (2016). *Lecture Notes in computer science: Vol. 9484*. *Privacy technologies and policy: Third Annual Privacy Forum, APF 2015, Luxembourg, Luxembourg, October 7-8, 2015, revised selected papers*. Cham: Springer.

Bilton, N. (2010). Price of Facebook Privacy? Start Clicking. *New York Times*.

Bitkom e.V. (2017). *Wirtschaftsschutz in der digitalen Welt.*

Boschi, E., & Trammell, B. (2011). IP Flow Anonymization Support.

Brown, S., Gommers, J., & Serrano, O. (2015). From Cyber Security Information Sharing to Threat Management.

BSI. (2008). BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise.

Cavoukian, A. (2010). Privacy by Design The 7 Foundational Principles: Implementation and Mapping of Fair Information Practices.

Chen, D., & Zhao, H. (2012, March - 2012, March). Data Security and Privacy Protection Issues in Cloud Computing. In *2012 International Conference on Computer Science and Electronics Engineering* (pp. 647–651). IEEE.

Cormack, A. (2011). Incident Response and Data Protection.

Cormack, A. (2016). Incident Response: Protecting Individual Rights under the General Data Protection Regulation. *Scripted.*

Council of Europe. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data: European Treaty Series - No. 108.

Cusumano, M. (2010). Cloud computing and SaaS as new computing platforms. *Communications* *of the ACM*, *53*, 27.

Deutscher Bundestag. (2014). *Antwort der Bundesregierung auf die Kleine Anfrage des Abgeordneten Andrej Hunko, weiterer Abgeordneter, der Fraktion DIE LINKE – Drucksache 18/540 – sowie der schriftlichen Nachfrage* (Deutscher Bundestag No. Drucksache 18/707). Berlin. Retrieved from Deutscher Bundestag, 18. Wahlperiode website: https://dip21.bundestag.de/dip21/btd/18/007/1800707.pdf

Edwards, L., & Urquhart, L. (2015). Privacy in Public Spaces: What Expectations of Privacy Do We Have in Social Media Intelligence? *International Journal of Law and Information Technology*, 279–310.

Egelmann, S., Cranor, L. F., & Hong, J. (2008). You've Been Warned: An Empirical Study of the Effectiveness of Web Browser Phishing Warnings.

ENISA European Union Agency for Network and Information Security. (2013). Detect, Share, Protect: Solutions for Improving Threat Data Exchange among CERTs.

ENISA European Union Agency for Network and Information Security. (2014a). Privacy and Data Protection by Design – from policy to engineering.

ENISA European Union Agency for Network and Information Security. (2014b). Standards and tools for exchange and processing of actionable information.

ENISA European Union Agency for Network and Information Security. (2015a). Actionable Information for Security Incident Response.

ENISA European Union Agency for Network and Information Security. (2015b). Privacy by design in big data: An overview of privacy enhancing technologies in the era of big data analytics.

ENISA European Union Agency for Network and Information Security. (2016). Privacy and Security in Personal Data Clouds: Final Report.

ENISA European Union Agency for Network and Information Security. (2017a). Exploring the opportunities and limitations of current Threat Intelligence Platforms.

ENISA European Union Agency for Network and Information Security. (2017b). Guidelines for SMEs on the security of personal data processing.

European Data Protection Board. (2018). Guidelines 3/2018 on the territorial scope of the GDPR: Article 3.

European Data Protection Supervisor. (2018a). Guidelines on the use of cloud computing services: by the European institutions and bodies.

European Data Protection Supervisor. (2018b). Opinion 5/2018 Preliminary Opinion on privacy by design.

Fenz, S., Heurix, J., Neubauer, T., & Pechstein, F. (2013). Current challenges in information security risk management.

Fessenden, T. (2017). The Most Hated Online Advertising Techniques.

FIRST Forum of Incident Response and Security Teams. Traffic Light Protocol (TLP) FIRST Standards Definitions and Usage Guidance.

Gibson, H. (2016). Acquisition and Preparation of Data for OSINT Investigations. In B. Akhgar, P. S. Bayerl, & F. Sampson (Eds.), *Advanced Sciences and Technologies for Security Applications. Open Source Intelligence Investigation* (Vol. 58, pp. 69–93). Cham: Springer International Publishing.

Golla, S. J., Hofmann, H., & Bäcker, M. (2018). Connecting the Dots: Sozialwissenschaftliche Forschung in Sozialen Medien im Lichte von DS-GVO und BDSG neu. *Datenschutz Und Datensicherheit - DuD*, 89–100.

Hilber, M. (2014). *Handbuch Cloud Computing*: Verlag Dr. Otto Schmidt.

Hon, K., Millard, C., & Walden, I. (2011). The Problem of 'Personal Data' in Cloud Computing - What Information is Regulated?: The Cloud of Unknowing, Part 1. *International Data Privacy Law*, *1*, 211–228.

The House of Commons, Science and Technology, Committee. (2016). The big data dilemma: Fourth Report of Session 2015–16.

A Joint Report by The Information and Privacy Commissioner/Ontario and Deloitte & Touche. (2003). The Security-Privacy Paradox: Issues, Misconceptions, and Strategies.

Kühling, J., & Buchner, B. (2017). *DS-GVO: Datenschutzgrundverordnung Kommentar*: C.H. Beck.

Leenes, R., van Brakel, R., Gutwirth, S., & Hert, P. de. (2017). *Data Protection and Privacy: (In)visibilities and Infrastructures*: Springer International Publishing.

McCullagh, K. (2017). Brexit: potential trade and data implications for digital and ‘f intech’ industries. *International Data Privacy Law*, *7*, 3–21.

National Institute of Standards and Technology. (2012). Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology.

National Open Source Enterprise. (2006). Intelligence Community Directive 301.

Ohm, P. (2010). Broken Promises of Privacy: Responding to the surprising failure of anonymization.

Padhy, R. P., Patra, M. R., & Satapathy, S. C. (2011). Cloud Computing: Security Issues and Research Challenges.

Perera, C., McCormick, C., Bandara, A., Price, B., & Nuseibeh, B. (2016). Privacy-by-Design Framework for Assessing Internet of Things applications and Platforms. *Proceedings of the 6th International Conference on the Internet of Things*, 83–92.

Plath, K.-U., & Becker, T. (2016). *BDSG/DSGVO: Kommentar zum BDSG und zur DSGVO sowie den Datenschutzbestimmungen des TMG und TKG* (2. Auflage).

Ponemon Institute LLC and IBM Security. (2017). *2017 Cost of Data Breach Study*. Traverse City, Michigan, USA.

Popović, K., & Hocenski, Ž. (2010). Cloud computing security issues and challenges.

Seitz, N. (2005). Transborder Search: A new perspective in law enforcement? *Yale Journal of Law and Technology*.

Serrano, O., Dandurand, L., & Brown, S. (2014). On the Design of a Cyber Security Data Sharing System.

Sillaber, C., Sauerwein, C., Mussmann, A., & Breu, R. (2016). Data Quality Challenges and Future Research Directions in Threat Intelligence Sharing Practice.

Slagell, A., Wang, J., & Yurcik, W. (2004). Network Log Anonymization: Application of Crypto-PAn to Cisco Netflows.

Steele, R. D. Open Source Intelligence: What is it? Why is it important to the military?

Symantec Corporation. (2017a). *Internet Security Threat Report.*

Symantec Corporation. (2017b). *Internet Security Threat Report.*

Takabi, H., Joshi, J. B.D., & Ahn, G.-J. (2010). Security and Privacy Challenges in Cloud Computing Environments. *IEEE Security & Privacy Magazine*, *8*, 24–31.

TeleTrusT - Bundesverband IT-Sicherheit e.V. (2018). IT-Sicherheitsgesetz und Datenschutz-Grundverordnung: Handreichung zum Stand der Technik technischer und organisatorischer Maßnahmen.

Wagner, C., Dulaunoy, A., Wagener, G., & Iklody, A. (2016). MISP - The Design and Implementation of a Collaborative Threat Intelligence Sharing Platform.

Walden, I. (2007). *Computer crimes and digital investigations*. Oxford: Oxford Univ. Press.

Webster, W., Leleux, C., Sterbik-Lamina, J., Fischer, D., Hert, P. de, Fonio, C., . . . Galdon Clavell, G. (2013). Increasing Resilience in Surveillance Societies Deliverable D2.1: The Social Perspective: A report presenting a review of the key features raised by the social perspectives of surveillance and democracy.

Williams, H., & Blum, I. (2018). Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise.

[1] Researcher at the Center for Applied Legal Studies, Karlsruhe Institute for Technology.

[2] In cooperation with the University of Bonn Institute for Computer Science, HiSolutions AG, Comma Soft AG and the ASW Bundesverband - Allianz für Sicherheit in der Wirtschaft e.V., methods for better defence against IT attacks are being developed. Legal support and expert opinions are provided by Prof. Dr. Franziska Boehm, Karlsruhe Institute of Technology/Leibniz Institute for Information Infrastructure. Https://itsec.cs.uni-bonn.de/overview/

[3] Ponemon Institute LLC and IBM Security (2017); Symantec Corporation (2017a).

[4] See for instance Bitkom e.V. (2017).

[5] See National Institute of Standards and Technology (2012) 15

[6] See Brown, Gommers, and Serrano (2015); Fenz, Heurix, Neubauer, and Pechstein (2013) 421.

[7] http://www.misp-project.org/

[8] The term “Privacy” has a bearing not only on the data protection principles but also on, e.g., Art. 8 ECHR. This paper refers to the term in accordance with GDPR.

[9] Cormack (2011) 3.

[10] See for instance Symantec Corporation (2017b); ENISA European Union Agency for Network and Information Security (2015a); ENISA European Union Agency for Network and Information Security (2017a).

[11] The term “privacy enhancing technologies” is often used by computer scientists and engineers.

[12] With practical advices and more background information see European Data Protection Board (2018) and on the context of Brexit and Fintechs see McCullagh (2017).

[13] Recital 26 GDPR.

[14] With practical examples Article 29 Working Party (2007).

[15] See The Federal Constitutional Court of Germany, BVerfGE 65,1.

[16] Article 29 Working Party (2011).

[17] Each controller needs to precisely define what personal data are actually needed for the purpose of the processing, including also the relevant data retention periods

[18] See for instance Cormack (2016) 273, 276.

[19] BSI (2008).

[20] See for instance Fessenden (2017).

[21] See Sillaber, Sauerwein, Mussmann, and Breu (2016).

[22] http://stixproject.github.io/getting-started/whitepaper/

[23] https://taxiiproject.github.io/

[24] See ENISA European Union Agency for Network and Information Security (2013).

[25] Gibson (2016).

[26] See for instance Webster et al. (2013).

[27] Edwards and Urquhart (2015), 285.

[28] See Williams and Blum (2018); Steele 22.

[29] National Open Source Enterprise (2006) 8. A legal basis is needed for further use.

[30] See Kühling and Buchner (2017) 1498.

[31] Council of Europe.

[32] Deutscher Bundestag (2014).

[33] Seitz (2005); Walden (2007).

[34] See for instance Bilton (2010); Egelmann, Cranor, and Hong (2008).

[35] Google Spain v Costeja Gonzales, ECJ, Case C-131/12, para 80.

[36] Data that is freely accessible to everyone.

[37] See Golla, Hofmann, and Bäcker (2018) 97

[38] It could also be necessary to include the case that decisions are made solely on the basis of an automated procedure. These are inadmissible if they have legal consequences for the data subject.

[39] See Kühling and Buchner (2017) 98.

[40] Kühling and Buchner (2017), 336; The Federal Constitutional Court of Germany 1 BvR 370/07

[41] Explained by ENISA European Union Agency for Network and Information Security (2014a) 14, 15.

[42] ENISA European Union Agency for Network and Information Security (2014b) 38.

[43] Overview of MISP: Wagner, Dulaunoy, Wagener, and Iklody (2016); Serrano, Dandurand, and Brown (2014).

[44] See Artikel 29-Datenschutzgruppe (2013) 23.

[45] See recital 50.

[46] Plath and Becker (2016); Kühling and Buchner (2017) 278.

[47] The Article 29 Working Party was an advisory body made up of a representative from the data protection authority of each EU Member State, the European Data Protection Supervisor and the European Commission. The European Data Protection Board has replaced the Art. 29 Working Party. The previously issued opinions are still valid.

[48] Artikel 29-Datenschutzgruppe (2013).

[49] Kühling and Buchner (2017) 281.

[50] See ENISA European Union Agency for Network and Information Security (2015a).

[51] Article 29 Data Protection Working Party (2017).

[52] ENISA European Union Agency for Network and Information Security (2015b), 44. Under the GDPR, in addition to the requirements that data must be processed lawfully and fairly, transparency is included as a fundamental aspect of these principles.

[53] With references and examples Article 29 Data Protection Working Party (2018a).

[54] Article 29 Working Party (2011) 19.

[55] Article 29 Data Protection Working Party (2018a), 25.

[56] Article 29 Data Protection Working Party (2018a), 28.

[57] Article 29 Data Protection Working Party (2018b).

[58] Legitimate interest is to be understood widely according to recital 47.

[59] See Article 29 Working Party (2009) 9.

[60] See Cavoukian (2010).

[61] Cormack (2011) 7.

[62] See FIRST Forum of Incident Response and Security Teams.

[63] See for instance Cormack (2016) 258, 263.

[64] Article 29 Working Party (2007).

[65] See CJEU C-582/14.

[66] Cormack (2011) 15.

[67] For example in Belgium or Italy.

[68] ENISA European Union Agency for Network and Information Security (2013).

[69] The term “Data Protection by Design and Default” is used to designate the special legal obligations established by Art. 25 GDPR. Whilst “Privacy by Design and Default” means the measures taken under the obligations. See also European Data Protection Supervisor (2018b).

[70] The relationship between data protection and data security is not always free of conflicts and described as a "security-privacy paradox: A Joint Report by The Information and Privacy Commissioner/Ontario and Deloitte & Touche (2003).

[71] Key criteria are given by ENISA European Union Agency for Network and Information Security

(2014a).

[72] See Art. 25 GDPR, recital 78.

[73] Leenes, van Brakel, Gutwirth, and Hert (2017) 108.

[74] See in general ENISA European Union Agency for Network and Information Security (2017b); Berendt, Engel, Ikonomou, Le Métayer, and Schiffner (2016).

[75] See ENISA European Union Agency for Network and Information Security (2015b); Article 29 Working Party (2014) 20.

[76] See ENISA European Union Agency for Network and Information Security (2014a); Article 29 Working Party (2014).

[77] The company could create and manage groups with other companies and share information with those particular groups.

[78] See FIRST Forum of Incident Response and Security Teams.

[79] With references and examples ENISA European Union Agency for Network and Information Security (2013), 31-33.

[80] ENISA European Union Agency for Network and Information Security (2013), 28.

[81] ENISA European Union Agency for Network and Information Security (2015b), 18.

[82] See ENISA European Union Agency for Network and Information Security (2015b) 9, 30, 36.

[83] Further information see Hon, Millard, and Walden (2011) 15, 16.

[84] Article 29 Working Party (2014) 5.

[85] Recital 26.

[86] Article 29 Working Party (2007) 21.

[87] See Ohm (2010) 1743, 1744.

[88] Article 29 Working Party (2007) 18.

[89] Article 29 Working Party (2007) 18.

[90] Article 29 Working Party (2007) 18.

[91] See ENISA European Union Agency for Network and Information Security (2015b) 38, 39.

[92] See Hon et al. (2011) 1744.

[93] Anthonysamy, Rashid, and Chitchyan 1.

[94] For example, MISP can be used as a platform to support information sharing implementing the ISO/IEC 27010 standard.

[95] TeleTrusT - Bundesverband IT-Sicherheit e.V. (2018) 11.

[96] ENISA European Union Agency for Network and Information Security (2014a) 6.

[97] ENISA European Union Agency for Network and Information Security (2017b), 16.

[98] Hilber (2014).

[99] ENISA European Union Agency for Network and Information Security (2017b), 5.

[100] ENISA European Union Agency for Network and Information Security (2017b), 48.

[101] Armbrust et al. (2010). 57.

[102] Cusumano (2010).

[103] See for instance Takabi, Joshi, and Ahn (2010); Chen and Zhao (2012 - 2012).

[104] See for instance Popović and Hocenski (2010).

[105] European Data Protection Supervisor (2018a); ENISA European Union Agency for Network and Information Security (2016).

[106] See Padhy, Patra, and Satapathy (2011).

[107] Serrano et al. (2014) 62.

[108] Perera, McCormick, Bandara, Price, and Nuseibeh (2016) 85.

[109] See for instance Slagell, Wang, and Yurcik (2004); Boschi and Trammell (2011).

[110] The House of Commons, Science and Technology, Committee (2016).