



D2.2

**Legal and Ethical
Requirements**

Project number:	833683
Project acronym:	CyberSANE
Project title:	Cyber Security Incident Handling, Warning and Response System for the European Critical Infrastructures
Start date of the project:	1 st September, 2019
Duration:	36 months
Programme:	H2020-SU-ICT-2018

Deliverable type:	Report
Deliverable reference number:	DS-01-833683 / D2.2/ Final N.1.1 2020_CSN_RP_06_Deliverable 2.2_Legal and Ethical Requirements_v1
Work package contributing to the deliverable:	WP 2
Due date:	31 March 2020 – M7
Actual submission date:	01/04/2020

Responsible organisation:	KUL
----------------------------------	-----

Editor:	Daphné Van der Eycken, Ilaria Buri, Plixavra Vogiatzoglou, Anton Vedder
Contributors	Diarmuid O Connor, Mark Burkley
Dissemination level:	PU
Revision:	DRAFT N.1.1

Abstract:	This report outlines the main legal frameworks applicable to the CyberSANE solution and its end-users. Following a security and data protection by design approach, the report concludes with a set of requirements that the CyberSANE partners must take into account when designing and developing the CyberSANE solution.
Keywords:	Data protection, Cybersecurity, Critical Infrastructures, Fundamental Rights, Evidence
	The project CyberSANE has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833683.

Editor

Daphné Van der Eycken (KUL)

Ilaria Buri (KUL)

Plixavra Vogiatzoglou (KUL)

Anton Vedder (KUL)

Contributors (ordered according to beneficiary numbers)

Diarmuid O Connor (LSE)

Mark Burkley (LSE)

Disclaimer

The information in this document is provided “as is”, and no guarantee or warranty is given that the information is fit for any particular purpose. The content of this document reflects only the author’s view – the European Commission is not responsible for any use that may be made of the information it contains. The users use the information at their sole risk and liability.

Executive Summary

This deliverable informs the CyberSANE Consortium of the legal and ethical frameworks that are relevant to the development and the end-use of the CyberSANE solution. This report outlines the main definitions and obligations applicable to end-users of the CyberSANE system and the manner in which the developers of the CyberSANE system should take those into account. Significant focus is put on fundamental rights potentially impacted by the use of the CyberSANE system, and the European Union (EU) frameworks on data protection, network information system security, critical infrastructures, cybercrime and AI, relevant to CyberSANE. Throughout this deliverable, the overarching framework and the manner in which it may be applicable to CyberSANE is presented and specified. Requirements stemming from the applicable legal frameworks are also identified within this deliverable. These requirements must be taken into account and integrated where feasible, when designing the CyberSANE system (these requirements are compiled at the end of the deliverable in the *Summary Table of Requirements*). The requirements table will also serve as a means to oversee and evaluate the implementation of legal and ethical considerations in CyberSANE, as mandated by task T10.4 'Legal and ethical implementation, oversight and evaluation'.

Contents

Executive Summary	3
Contents	4
Chapter 1 Introduction	1
Chapter 2 Fundamental Rights	2
2.1 Privacy and Data Protection	3
2.1.1 Council of Europe	3
2.1.1.1 Privacy	5
2.1.1.2 Data Protection.....	6
2.1.2 European Union	7
2.1.2.1 Privacy	8
2.1.2.2 Data Protection.....	8
2.1.3 Application to the CyberSANE system	8
2.1.3.1 Interference with private life.....	9
2.1.3.2 Legal basis	9
2.1.3.3 Legitimate aim.....	10
2.1.3.4 Proportionality	10
2.2 Freedom of Expression	12
Chapter 3 EU Data Protection Framework	14
3.1 The General Data Protection Regulation	15
3.1.1 Scope, concepts and main definitions	15
3.1.1.1 Material scope	15
3.1.1.2 Personal data	17
3.1.1.2.1 Information	17
3.1.1.2.2 Natural person	18
3.1.1.2.3 Identifiability	18
3.1.1.2.4 Connecting link	19
3.1.1.3 Processing	20
3.1.1.4 Special categories of data	22

D2.2 – Legal and Ethical Requirements

3.1.1.5	<i>Data quality principles</i>	23
3.1.1.5.1	Lawfulness, fairness and transparency	24
3.1.1.5.2	Purpose limitation	25
3.1.1.5.3	Data minimisation	26
3.1.1.5.4	Accuracy	27
3.1.1.5.5	Storage limitation	27
3.1.1.5.6	Integrity and confidentiality	27
3.1.1.5.7	Example of web crawling	30
3.1.2	Data controller's obligations	31
3.1.2.1	<i>Legal basis</i>	31
3.1.2.2	<i>Data Protection Officer and Data Protection Impact Assessment</i>	35
3.1.2.2.1	Data Protection Officer	35
3.1.2.2.2	Data Protection Impact Assessment	35
3.1.2.3	<i>Data security and breach of personal data</i>	36
3.1.2.4	<i>Accountability, liability and overall responsibility</i>	36
3.1.3	Data subject's rights	37
3.1.3.1	<i>Automated decision-making</i>	38
3.2	E-Privacy Directive	41
3.3	Directive (EU) 2016/680	41
3.4	Regulation on the free flow of non-personal data	43
3.4.1	The Regulation	43
3.4.2	Mixed datasets	44
4	The EU legal framework on cybersecurity	47
4.1	Scope and objectives	47
4.2	The NIS Directive	47
4.2.1.	Overview and key definitions	47
4.2.2.	NIS Directive's obligations	49
4.2.2.1	<i>National frameworks on the security of network and information systems</i>	49
4.2.2.2	<i>Obligations for OES</i>	50
4.2.2.3	<i>Obligations for DSP</i>	52
4.3	The interplay between NIS Directive and GDPR	53

4.4	The Cybersecurity Act	53
5	Critical infrastructures in the EU	57
5.1	The notion of Critical Infrastructures	57
5.3	Information sharing	58
6	Evidence handling	60
6.1	Introduction	60
6.2	Cybercrime	60
6.2.2	The Budapest Convention	60
6.2.3	The Cybercrime Directive	61
6.3	Criminal and Criminal Procedural law	62
6.3.1	Fair trial principles	62
6.3.2	Admissibility of evidence	63
6.4	Data Protection law	64
6.5	Proposal for an e-Evidence Framework	65
7	Ethics Guidelines for Trustworthy AI	67
7.1	Introduction	67
7.2	Key principles and requirements	68
8	Summary Table of Requirements	71
9	List of Abbreviations	77
10	Bibliography	79

Chapter 1 Introduction

CyberSANE is a peer-to-peer solution for the detection, prevention and mitigation of cyber-threats and the exchange of valuable information regarding cybersecurity. In particular, CyberSANE seeks to enhance the cybersecurity of Critical Infrastructures' information systems through the collection, correlation and sharing of information by multiple sources. CyberSANE is based on a continuous monitoring of the end-users information systems. The design and implementation of the CyberSANE solution must provide for end-users to comply with various legal and regulatory obligations applicable to those systems and the data included. This deliverable will provide a number of requirements relevant for the development of the CyberSANE system. This report will also detail the field of (cyber) security, privacy and data protection following a security and data protection by design approach. The relevant legal instruments will be outlined and further described in the format of a preliminary analysis and on the basis of a certain degree of applicability or impact on the project or its end-users. Where possible and desirable, a visual summary and/or flowchart will be provided of said descriptions. The deliverable is structured as follows:

Chapter 2 provides an overview of the fundamental right to privacy and data protection, by looking in particular at the protection and safeguards offered to these fundamental rights at the international (Council of Europe) and EU level.

Chapter 3 illustrates the key concepts, definitions and obligations of the complex European Union (EU) Framework on Data Protection, which is composed by several legal and regulatory "layers": the discussion is in fact not limited to the General Data Protection Regulation (GDPR), but embraces the e-Privacy Directive, Directive 2016/680 on the processing of personal data for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties and the Regulation on the free flow of non-personal data.

The analysis follows with the discussion of the EU legal framework on cybersecurity (Chapter 4), with a focus on the most significant recent initiatives within the EU cybersecurity strategy: the NIS Directive (including in its interconnection with the GDPR) and the Cybersecurity Act.

Taking into account the goal of CyberSANE - which is to enhance the cyber-resilience of Critical information Infrastructures (CIIs) - Chapter 5 provides an overview of the EU legal framework on Critical Infrastructures and their protection, including on the sharing of information among Critical Infrastructures and between these and public authorities.

The multi-layered legal framework applicable to the formation and handling of evidences in cyberspace - composed of international, European and national rules - is described in Chapter 6, which also touches upon the recent proposal for an EU framework on e-Evidence.

Finally, chapter 7 discusses the ethics-related principles and constraints which must be taken into account when involving AI systems in the development of a cybersecurity solution. In particular, the discussion focuses on the ethical principles and requirements presented in the "Ethics Guidelines or Trustworthy Artificial Intelligence (AI)", published in April 2019 by the High Level Expert Group on AI appointed by the European Commission.

Chapter 2 Fundamental Rights

This chapter will outline the fundamental rights that are most relevant to the development and functioning of the CyberSANE system, specifically the right to privacy; the right to data protection and the right to freedom of expression.

Privacy and data protection strive to protect citizens' autonomy and human dignity via a personal space in which individuals can freely develop their personalities. In this sense, both privacy and data protection are considered essential prerequisites for the exercise of other freedoms. For example, citizens need to rely on a certain level of privacy and protection of their personal data in order to be enabled to freely express their opinions. This last statement explains why the right to freedom of expression should be discussed in this document. The CyberSANE system will need to avoid excessive interference in citizens' private life, but must also guarantee a certain level of privacy so that citizens still can express their opinions and ideas. Conversely, citizens need to be able to express themselves to develop their personality and a certain sense of self. Although they sometimes conflict with each other, privacy, data protection and freedom of expression are therefore essential prerequisites to the enjoyment of each other.

Aside from their co-dependent and - at times conflictual - relationship, the right to privacy, data protection and freedom of expression remain very distinct rights. This might come as obvious when comparing privacy to the freedom of expression. However, even if they are often mentioned in the same breath, privacy and data protection are very different too. Privacy and data protection cannot be perceived as equals as they differ in their formulation as well as in scope. Privacy comes into play whenever a private interest has been compromised and contains a general prohibition on interference unless an overriding interest legitimizes an exception. On the other hand, data protection is a more modern and flexible right. Data protection does not require a private interest to be compromised for data protection rights to apply, yet has a lot more attention for checks and balances.

Privacy	Data Protection	Freedom of expression
Fundamental right aiming to protect human dignity and autonomy		Fundamental right aiming to protect one's opinions without censorship, restraint or legal penalty
Requires the interference in the private life of individuals	Applies to all processing activities	
Contains a general prohibition	More flexible right with many checks and balances	

Figure 1 Similarities and differences between privacy and data protection

The applicability of the fundamental rights instruments to the CyberSANE solution will be discussed more in depth below, however, it should be noted from the outset that the fundamental rights instruments bind States and other governmental authorities. These instruments are not intended to regulate the relationships between private individuals and might, therefore, not have any direct impact on the CyberSANE solution as developed by the partners and/or employed by its end-users, insofar as they do not consist of public entities. Nevertheless, even in that case, their applicability is not completely excluded and, as will be demonstrated below, the fundamental rights of privacy, data protection and freedom of expression remain relevant within the assessment of the legal and ethical requirements for the development of this technology.

2.1 Privacy and Data Protection

Within the European continent, the fundamental rights to privacy and data protection are protected on roughly three different levels. The first one is at the level of the Council of Europe (CoE). In 1953, the CoE adopted the European Convention for the Protection of Human Rights (ECHR). Through its Article 8, the right to privacy came into effect for the first time in a binding manner. The second is at the level of the EU with its Charter of Fundamental Rights (Charter) that was adopted in 2000. Although originally only intended as a political document, the Charter gained its legally binding character when the Lisbon Treaty came into force in 2009. The *Charter* sets out the fundamental rights protected in the EU and includes the right to privacy and data protection. Finally, fundamental rights are granted protection within the constitutions of the national jurisdictions.

Because the ECHR and the Charter mainly reflect the constitutional traditions of the EU Member States, this document will not discuss this national perspective, but will focus on the legal instruments adopted by the CoE and by the EU.

2.1.1 Council of Europe

The CoE is an international organization whose aim is to uphold human rights, democracy and the rule of law in Europe. It was founded in 1949 and counts 47 Member States.¹ Note that, despite its name, the CoE is not an institution of the EU. Its membership is a lot more diversified and stretches far beyond the 27 Member States of the EU. However, all 27 Member States of the EU are Contracting Parties to the ECHR.

The fundamental rights conferred by the ECHR are to be enjoyed by the citizens of the Contracting Parties. Whenever citizens estimate that their right to privacy is violated, they may seek protection before the European Court of Human Rights (ECtHR). The ECtHR will then be burdened with the task of assessing whether a Contracting State failed to comply with its obligations under Article 8 ECHR. In this way, the ECtHR is the final arbiter and interpreter of the rights enshrined in the ECHR and, whenever it issues a judgment, their rulings are binding upon the 47 Contracting States.

As indicated before, the ECHR solely introduces obligations for the Contracting States and the respective governmental entities to follow, though it is to be noted that these obligations are two-

¹ The 47 Contracting Parties are the following: Albania, Andorra, Armenia, Austria, Azerbaijan, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Monaco, Montenegro, Netherlands, North Macedonia, Norway, Poland, Portugal, Republic of Moldova, Romania, Russian Federation, San Marino, Serbia, Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, Ukraine and the United Kingdom.

D2.2 – Legal and Ethical Requirements

fold: it confers upon them a positive and negative obligation. A negative obligation requires Contracting States to not interfere with the enjoyment and exercise of the fundamental right, unless the conditions provided by the ECHR are fulfilled. Alternatively, positive obligations require an active attitude of the Contracting States whenever omission would result in interference of citizen's right. These positive obligations may even go as far as to require states to intervene in the private sphere and relations of individuals themselves.

More concretely, the activities conducted by the end-users through the CyberSANE system may be caught by the ECHR if by their legal nature and status are considered subject to it or if it is deemed that the Contracting States need to intervene pursuant their positive obligations, in order to protect citizens' right to privacy. For this reason, the developers of the CyberSANE solution must pay attention to the ECHR when developing this new technology.

The exact boundary between the State's positive and negative obligations under Article 8 does not lend itself to precise definition. A case-by-case analysis imposes itself and a fair balance must be struck between the relevant competing interests.² In this regard, the more recent case-law on the scope of protection conferred by Article 8 ECHR confirms that it impacts the private sector by imposing on the Contracting States the positive obligation to create and enforce effective data protection rules.³ In addition to the obligation for government to ensure effective respect for private or family life even in the sphere of the relations of individuals between themselves, the ECtHR indicated that:

“The mere fact that the domestic legislation the domestic legislation provided the applicant with an opportunity to claim compensation for damages caused by an alleged unlawful disclosure of personal data was not sufficient to protect her private life. What is required in this connection is practical and effective protection to exclude any possibility of unauthorized access occurring in the first place.”⁴

The likelihood of the ECHR provisions to be invoked against the CyberSANE solution is rather marginal since the end-users will likely be active in the private sector. The judgment rendered by the ECtHR shows that it is not unthinkable that someone may initiate legal procedures if they estimate the intrusiveness of the CyberSANE solution to be excessive and safeguards offered by government to be insufficient in order to oppose against it. The national judge that will have to rule over this matter, could then potentially have to assess the positive State responsibility at stake. The above judgment, confirmed later in another case⁵, created a precedent in stating that States might need to prevent such intrusive actions undertaken by private individuals to take place. This does not mean that CyberSANE is to be considered in violation of the ECHR, rather it will need to abide by a few criteria and offer adequate guarantees to the citizens concerned.

² ECtHR Küchl v. Austria, 4 December 2012, no. 51151/06, paras 55-56.

³ ECtHR 07 July 1979, Gaskin v. UK, Application No. 10454/83; ECHR 06 September 1978, Klass and Others v. Germany, Application No. 5029/71; ECHR 13 August 1981, Young, James, and Webster v. UK Application No. 7601/76 ; 7806/77; and ECHR 26 March 1985, X. and Y. v. The Netherlands, Application no. 8978/80.

⁴ ECtHR 17 July 2008, I v. Finland, Application no. 20511/03. At issue was a dispute between a hospital and a former employee. The employee claimed a breach of Article 8 ECHR because the hospital's system for recording and retrieving patient information had been freely accessed and consulted by her colleagues which informed them of her HIV-positive diagnosis. In addition, the system did not allow her to obtain information on who had accessed her file due to a technical limitation. When all national procedures failed to obtain damages, she filed a complaint before the European Court of Human Rights.

⁵ ECtHR 2 December 2008, K.U. v. Finland, Application no. 2872/02.

2.1.1.1 Privacy

The right to respect for private and family life is enshrined in Article 8 ECHR. The concept of private life is a particularly broad one and includes any type of data processing activity (e.g. *collection, storage, pseudonymization, investigation, etc.*). In this sense, the case-law has elucidated a few matters that are relevant to the CyberSANE solution:

- The concept of private life “*extends to aspects relating to personal identity*”, such as a person’s name⁶
- Private life also includes other means of personal identification beyond a person’s name
- The interception of communications (mail and telephone) constitutes an interference with private life, family life and correspondence⁷
- The ECtHR also made clear that the intrusive nature of investigations will engage privacy rights and that access to metadata can be just as intrusive as access to content data.⁸

The CyberSANE solution will be able to crawl and index data and information on the Dark and Deep Web, exploit and incorporate multiple sources of social media streams and incorporate a neural network for face detection in digital images and videos. Considering the broad interpretation of the concept of ‘private life’, these three elements alone can potentially trigger the applicability of Article 8 ECHR as they constitute an interference of individuals’ private life.

The fact that CyberSANE might interfere with citizens’ private life, does not prohibit the deployment of the CyberSANE solution as the second paragraph of Article 8 ECHR reveals that the right to privacy is not an absolute right, which means that if the interference meets three requirements, it may be considered as valid.

Any interference must be *in accordance with the law*. This entails that individuals need to be able to access a legislative act that clearly sets out the rules for a privacy violation. As a second condition, the interference must *pursue a legitimate aim*. This includes public safety, public security, the economic well-being of the country, the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. Third, the interference must be *strictly necessary in a democratic society*. In other words, the interference must be (i) suitable, (ii) necessary and (iii) not go beyond to what is necessary to attain the pursued aim.

For sake of clarity, the following flowchart provides a visualization of the different steps to keep in mind when assessing the compliance criteria of Article 8 ECHR.

⁶ ECtHR Niemietz v. Germany, 16 December 1992, Application no. 13710/88.

⁷ Klass v. Germany, judgment of 22 September 1993, Series A no. 269, para. 41.

⁸ ECtHR 13 September 2018 Big Brother Watch v. UK, Application nos. 58170/13, 62322/14 and 24960/15.

D2.2 – Legal and Ethical Requirements

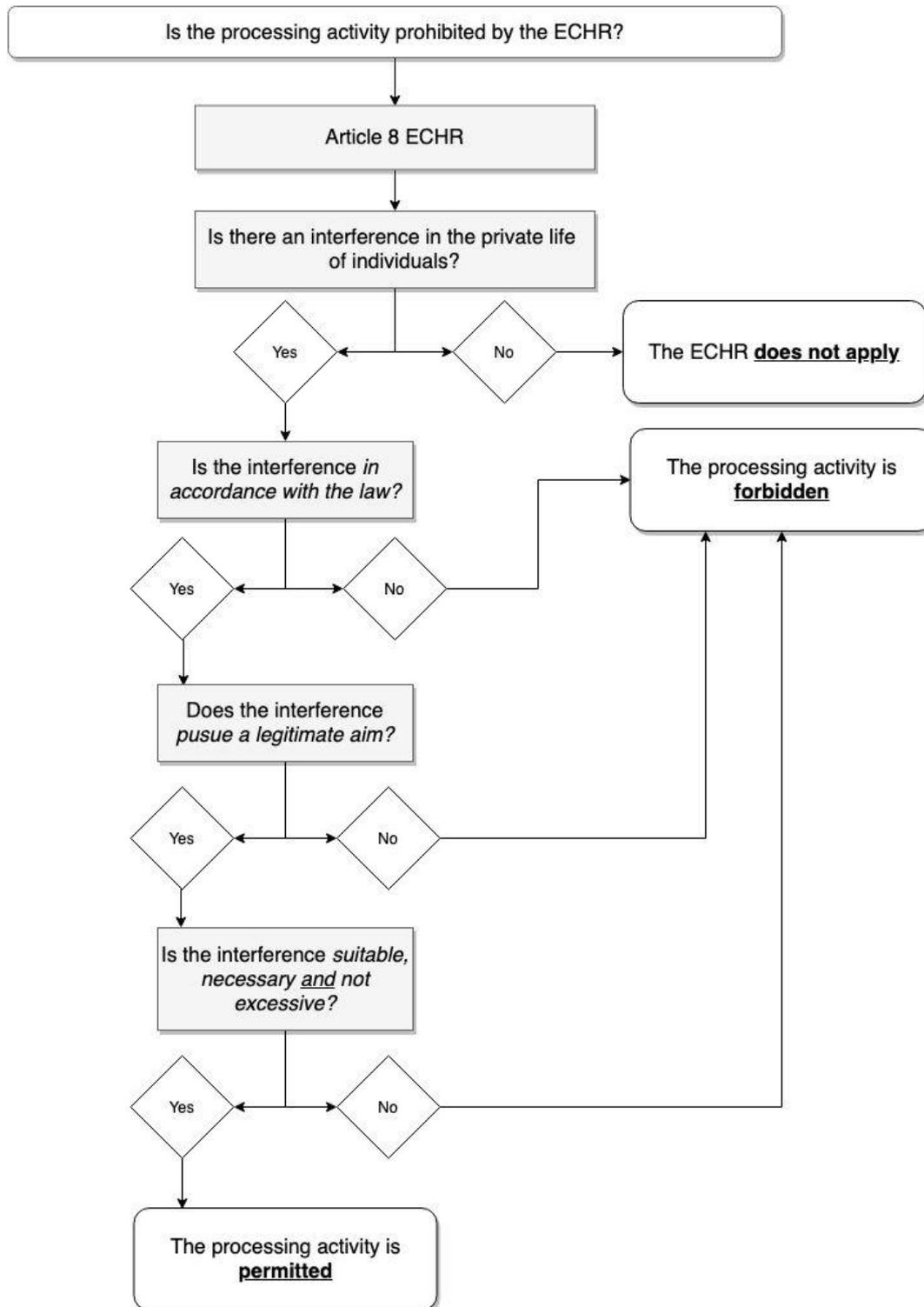


Figure 2 Flowchart on the applicability of Article 8 ECHR and the requirements for an interference to be considered lawful

2.1.1.2 Data Protection

The ECHR does not in itself contain a specific provision that guarantees the right to personal data protection. The CoE did adopt an international legally binding instrument dealing with data protection and is – to date – the only international organisation that has done so. In 1981 already, the Convention 108 was adopted to deal with the challenges that result particularly from the use of new information and communication technologies. Thirty years later this convention underwent a modernisation process that focused on reinforcing data protection in a digital age and on the reinforcement of the convention's follow-up mechanisms.

Modernised Convention 108 introduced a few principles with regard to the processing of personal data, in particular the fair and lawful collection and automatic processing of data, for specified legitimate purposes.⁹ In other words, data cannot be used for a purpose that would be incompatible with the indicated original purpose and should not be kept longer than necessary. The Convention also introduced principles with regard to the quality of data, namely that they must be adequate, relevant, not excessive and accurate. Additionally, it introduced the concept of 'sensitive' data and prohibits the processing thereof as a principle unless proper legal safeguards can be provided.¹⁰

This Convention seeks to protect the individual against abuses which may accompany the collection and processing of personal data, while at the same time regulate the cross-border flow of personal data. Although not subject to the judicial supervision of the ECtHR, this Modernised Convention is used as a means to interpret the scope of protection afforded by the fundamental right of privacy in Article 8 ECHR which explains why it must be elaborated on in present document. Data protection is thus not specifically enunciated by the ECHR yet data protection forms part of the rights protected under the fundamental right to privacy. Note in this regard that, although Convention 108 entails the responsibility of the Contracting Parties that have ratified it, the instrument applies to all data processing carried out by both the public and private sector. According to Article 3 Convention 108, each Contracting Party shall commit to apply the content of this Convention to data processing subject to its jurisdiction. In an indirect way, Convention 108 will thus apply to the processing activities conducted by the end-users of CyberSANE, however they are not the ones that will be held accountable.

2.1.2 European Union

Initially envisaged as a regional organization focused on economic integration and the establishment of a common market, the original treaties of the EU did not contain any human rights provisions. However, as the Court of Justice of the EU (CJEU) was increasingly brought to rule over cases in which human rights violations were alleged, its case-law provided a first important source for EU fundamental rights by bringing them into the so-called principles of EU law. Today, the fundamental rights character of privacy and data protection in the EU is undeniable as they have been entrenched in the Charter, as well as in the Treaty on the Functioning of the European Union (TFEU), both acting as primary sources of EU law.

Similar to the ECHR, the *Charter* does not address the private, but rather the public EU institutions and bodies, as well as the Member States whenever they implement EU Law. Citizens of the European Union will therefore be able to rely on the Charter in their relations with the EU or their own national authorities. However, similar to the ECHR, this does not completely exempt the CyberSANE developers and end-users from taking the Charter into account since the CJEU

⁹ CoE, ECtHR, EU Data Protection Supervisor, EU Agency for Fundamental Rights, "Context and background of European data protection laws", in *Handbook on European data protection law*, Luxembourg, Imprimerie Centrale in Luxembourg, 2018, p. 24.

¹⁰ For more information on the concept of sensitive data, see section 3.1.1.4.

expressed in a handful of judgments that the Charter has a horizontal direct effect.¹¹ In other words, the CJEU clarified that fundamental rights, such as the right to privacy and to data protection, are capable of creating obligations between private parties and potentially scrutinized citizens.¹²

In the same way that the right to privacy is not elevated to an absolute right in the ECHR, the *Charter* provides for limitations on the exercise of the rights and freedoms. According to Article 52 of the *Charter*, limitations on fundamental rights are admissible only if they (i) are provided for by law, (ii) respect the essence of the right to data protection, (iii) are necessary and subject to the principle of proportionality and (iv) meet objectives of general interest recognized by the Union or the need to protect the rights and freedoms of others. The attentive reader is able to see a high level of similarity between these requirements and the ones set out in the ECHR.

2.1.2.1 Privacy

The right to respect for private and family life is protected in Article 7 of the Charter in an almost identical manner as the ECHR. Its broad concept and interpretation is equally applicable in the EU order.

2.1.2.2 Data Protection

As opposed to the ECHR, the Charter not only dedicates a provision to privacy, it also establishes the right to data protection as a distinct fundamental right in its Article 8. Article 8 not only recognizes the right to protection of personal data, it also enunciates the core principles of data protection. Data must be (i) processed fairly, (ii) for specified purposes and (iii) must be supported on a legitimate basis. The Charter recognizes citizens' right to access their data and rectify it in case an inaccuracy occurred. In addition, it makes the compliance of these rules subject to control by independent authorities. It is worthy to stress that, as opposed to privacy, the rules on personal data protection do not require an interference of the personal sphere. Data protection comes into play as soon as data is being processed which makes its scope a lot broader.

Besides the Charter, there is another primary source of EU law that dedicates a provision to the right to data protection. Indeed, in view of the crucial importance of the free movement of personal data in the EU internal market, the Union had to ensure that the use of personal data by the industry would comply with the fundamental right to data protection. It was in this vein important to have a legal basis to adopt legislation in order to strengthen citizens' rights, while at the same time simplify rules to which companies need to adhere. Article 16 of the TFEU thus confers upon the Parliament and the Council the competence to lay down rules relating to the protection of individuals when carrying out activities that fall within the scope of EU law.

2.1.3 Application to the CyberSANE system

This document will apply the previously expressed theoretical principles to the CyberSANE project and its deliverables. Although the right to data protection and privacy are two distinct rights, which are set out in two different legal frameworks, their assessment is very much conflated, which explains why the assessment below only needs to be executed once. The wording of the provisions under the ECHR and the Charter are rather similar and both legal frameworks require a legal basis, legitimate aim, necessity and proportionality for an interference to be lawful.

¹¹ Judgment of 22 November 2005, *Werner Mangold*, C-144/04, EU:C:2005:709 and Judgment of 19 January 2010, *Kükükdeveci*, C-555/07, EU:C:2010:21.

¹² Judgment of 15 January 2014, *Association de médiation sociale*, C-176/12, EU:C:2014:2.

Important differences between privacy and data protection or between the interpretation of the ECtHR as opposed to the CJEU will be outlined whenever relevant to the CyberSANE solution.

2.1.3.1 Interference with private life

The CyberSANE solution aims at improving the detection and analysis of cyber-attacks and threats on critical information infrastructures and increase the knowledge on the current cyber threat landscape by introducing a system comprising five different components. The relevant question here is whether the CyberSANE solution will cause an interference of citizens' private life. By collecting and processing data from internal (e.g. network traffic) as well as external sources (e.g. social networks and dark web), as well as using algorithms to detect anomalies, analyse incidents, facilitate the forensic analysis of cyber-attacks, employing facial recognition tools of individuals, profiling individuals as well as potentially monitoring employees' activities and patient data, the CyberSANE solution will undoubtedly pose a risk to the privacy rights of individuals concerned and process their personal data. Therefore, it will constitute an interference with their private lives. In this sense, the CyberSANE solution will be subject to the provisions laying out the right to privacy at the level of the CoE as well as the EU.

As outlined above, the fundamental rights to privacy and data protection are not absolute and the interference with citizens' private lives does not equate to a prohibition. The Courts supervising the correct application of fundamental rights instruments look negatively on the use of inadequate techniques rather than the reception of personal data and consequent monitoring activities as such.¹³ What is seen as problematic, is when a monitoring system exceeds what is necessary and does not come with sufficient safeguards and adequate oversight mechanisms. If found in accordance with the law and proportionate with regard to a legitimate aim, the CyberSANE system may be found lawful. This report outlines all necessary measures to be taken by the CyberSANE consortium.

2.1.3.2 Legal basis

Every interference of individuals' rights must be in accordance with the law. This requires that an interference stems from a national law and is foreseeable, in the sense that the individuals have the ability to access such law and foresee such interference. The relevant question is whether the activities conducted through the CyberSANE solution could be said to be in accordance with the law and could be foreseen by the individuals concerned. In this regard, the obligation to implement security measures to protect cyber security stems from various European as well as national legal frameworks. In particular, we mention indicatively the Network Information Systems Directive (NIS Directive)¹⁴ (which will need to be implemented in the different EU Member States through national legislative acts) and the GDPR¹⁵.

Various legal instruments impose the obligation to implement organizational and technical measures in order to ensure the security, integrity and confidentiality of personal data and of network and information systems. Furthermore, sector specific frameworks applicable to each CI foresee similar obligations (e.g. *transport, health, energy and finance*). As will be elaborated upon in the next chapter of this document, the NIS Directive requires the EU Member States to

¹³ *Big Brother Watch* and *Rattvisa*

¹⁴ Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

¹⁵ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

D2.2 – Legal and Ethical Requirements

implement the Directive in their national legislation so as to ensure the security of network information services.

The abovementioned instruments provide a legal basis for the obligation to secure one’s information systems. Therefore, the limitations to the individuals’ rights to privacy and data protection are in accordance with the law and meet the first condition.

CASE	REQUIREMENT
CyberSANE activities must be in accordance with the law	CyberSANE end-users must find a suitable national or European legislative act which describes the possibility to conduct the processing activities and the requirements to follow. CyberSANE activities must not exceed the boundaries of such legal basis.

2.1.3.3 Legitimate aim

The legitimate aims provided for by the ECHR and the Charter encompass broad notions such as national and public security, as well as the protection of the rights and freedoms of others. The CyberSANE system pursues such a legitimate aim as its purpose is to ensure the security of information infrastructures as well as to prevent and mitigate any cyber threats or attacks. The interference thus meets the second condition.

2.1.3.4 Proportionality

The CyberSANE system must limit its processing activities to what is necessary for the achievement of securing its information systems, so that its legitimate aim not to be questioned. It will need to strike a balance between its monitoring activities for cybersecurity purposes and protect human rights by insisting on a series of conditions and safeguards to limit abuse. The limitation of individuals’ privacy through the use of all kinds of security measures cannot go beyond what is necessary to attain the identified legitimate aim. This analysis is usually the most delicate. Proportionality is one of the conditions to assess whether an interference is lawful, but in its turn encompasses different notions. To be proportionate (*proportionality sensu lato*), any interfering measure must be suitable, necessary and be able to meet a balancing test to make sure a measure is not excessive (*proportionality sensu stricto*). The following illustration provides for a visualization of proportionality as part of the three-step analysis and as overarching concept for another three-step analysis.

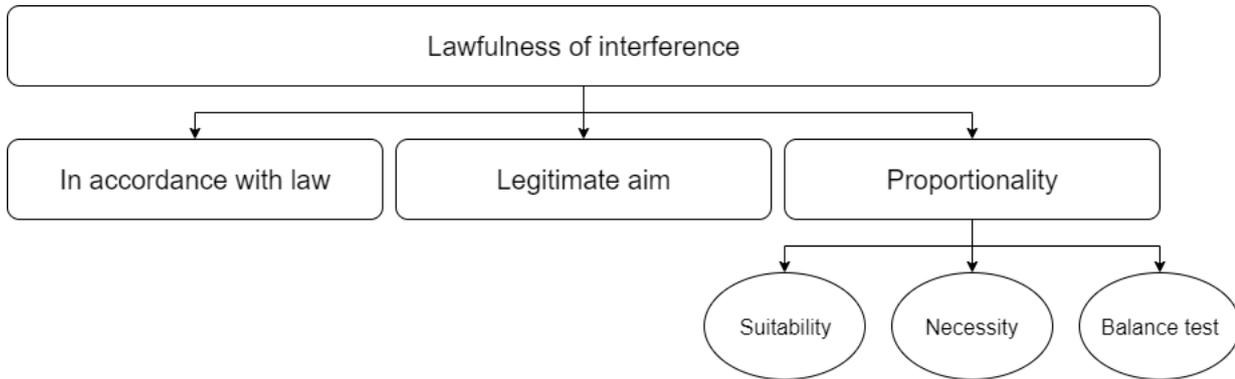


Figure 3 The relationship between proportionality *sensu lato* and proportionality *sensu stricto*

Starting with the suitability requirement, the appropriateness and effectiveness of a security measure must be reviewed. The measures proposed by the CyberSANE solution will have to be able to respond to potential threats of hackers and prevent or mitigate risks and possible harms to the information systems.

Any interference must be necessary. For example:

- Is the use of facial recognition tools the only way to ensure a high level of security of information infrastructures?
- Is it really necessary to crawl through all the data and information available on social networks or can the CyberSANE solution find another way to retrieve the information it needs?
- Is all the information retrieved necessary to protect one's information system?

To meet this criterion, the CyberSANE solution must make sure that no other less intrusive methods are available to attain one's goal. CyberSANE developers will thus need to investigate if alternatives exist that can be equally effective to achieve the desired security objective.

The CyberSANE solution must allow to balance the benefits of the suitable and necessary security measures against the severity of the impact of these measures on individuals' private lives. Even though a measure can be found suitable and necessary, it might fail the proportionality test if its added value cannot compensate the harm done to individuals. In view of the impossibility to inform suspect internet users prior to the interception of their data, safeguards must be put so as to be even stronger and more effective against abuse of monitoring powers, especially since there is little no possibility to recourse against the processing of one's data.

It should be noted that within the EU legal framework, an interference with privacy or data protection must at all times respect the essence of the right to which they interfere. It is necessary that a minimum level of privacy and data protection is always respected.

In order for the CyberSANE end users and developers to be able to conduct this assessment, all the measures and combination of measures to be taken as well as the objectives they pursue should be sufficiently and clearly described.¹⁶

¹⁶ European Data Protection Supervisor, *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit*.

CASE	REQUIREMENT
<p>CyberSANE activities might be excessively intrusive, thereby entailing the risk of undermining democracy on the ground of defending it</p>	<p>CyberSANE must allow for data processing activities to be suitable to protect information systems and must allow only processing activities that are necessary to said purpose, cannot go beyond what is strictly necessary and must allow for the interests of the end-users to be reasonably balanced with the disadvantage endured by monitored citizens. It must allow to implement adequate and effective guarantees against abuse, taking into account all relevant circumstances, including the nature, the scope and duration of possible measures, the ground for ordering them, the competent persons to permit, carry out and supervise them and the remedies provided by law</p>

2.2 Freedom of Expression

One of the rights that interact most significantly with the right to privacy is the right to freedom of expression, which is protected by Article 10 ECHR and Article 11 Charter. Without a certain level of privacy, individuals lack the space to think and speak. Equally true, without a certain freedom of expression, one would not be able to develop the sense of self. Freedom of expression, data protection and privacy are essential prerequisites to each other's enjoyment. Therefore, every measure that interferes with citizens' privacy, is potentially interfering with citizens' right to freedom of expression which in turn explains why this section is dedicated to it.

United Nations ('UN') Special Rapporteur on freedom of opinion and expression, Frank La Rue confirmed this in its Report on the promotion and protection of the right to freedom of opinion and expression in 2013.¹⁷ Although focused on surveillance measures undertaken by the State and State authorities, this document does stress the roles and responsibilities of the private sector as well. Aside from facilitating the access to a massive amount of information to government seeking to monitor citizens' behaviour on the internet, Mr La Rue explains that the private sector has been complicit in developing technologies that enable mass or invasive surveillance in contravention of existing legal standards. He also stresses the facts that these industries are virtually unregulated as States fail to keep pace with technological developments.

A good illustration demonstrating how a privacy breach resulting from the use of technology can also cause the violation of one's freedom of speech can be found in the case-law of the ECtHR, namely *Big Brother Watch v. UK* judgment.¹⁸ Although this case dealt with the techniques of

¹⁷

https://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

¹⁸ At stake was the exploitation of surveillance and intelligence sharing programs between the USA and the UK. British government was able to tap into and store huge amounts of data that passes through fibre-optic

D2.2 – Legal and Ethical Requirements

massive interception of communications practiced by a public intelligence agency, the insights and reasoning found in this decision are of much relevance to the CyberSANE project, as the *Court* found freedom of expression of journalists to be violated. On the one hand, the *Court* found a violation of Article 10 ECHR because domestic law only provided that interception of communications involving confidential journalistic material was allowed when a warrant is being considered for the interception but not in the case of bulk surveillance. On the other hand, the *Court* concluded a violation of Article 10 ECHR because the surveillance program did not provide enhanced protection when the data was retrieved to identify journalists, nor did it contain special provisions to restrict access of journalists’ communication for the purpose of combatting serious crime.

One must stress the importance of said judgment because, similar to the activities undertaken by the UK intelligence services, the CyberSANE solution is not aimed specifically at uncovering journalists’ sources. However the surveillance program was still found to be in breach of the right to freedom of expression by not providing adequate safeguards against abuse.

CASE	REQUIREMENT
CyberSANE activities process data capable to retrieve information of journalists’ identity or sources	CyberSANE must allow to limit bulk interception of data originating from journalists and must ensure that, whenever journalists’ data are processed, enhanced protection measures can be installed, additionally, it must contain provisions that allow to restrict access of journalists’ communication data
The CyberSANE end-users are processing data originating from forums or social media	CyberSANE must allow to limit bulk interception of data coming from citizens expressing opinions and must guarantee that there are adequate and effective guarantees against abuse. Account must be taken of all relevant circumstances, including the nature, the scope and duration of possible measures, the grounds for ordering them, the competent persons to permit, carry out and supervise them and the remedies provided by national law

cables between the UK and the USA. Aside from using this bulk interception of communications for own intelligence surveillance purposes, the UK also gave access to the National Security Agency of the USA.

Chapter 3 EU Data Protection Framework

The EU data protection framework encompasses primary as well as secondary law. Data protection in primary law sets out the fundamental principle of data protection and is discussed above (See 2.1.1.2 and 2.1.2.2). Secondary EU data protection law was first created in 1995 with the adoption of Directive 95/46/EC.

Due to the digitalisation of products and services, an accruing need for modernisation of data protection legislation rose. The European Parliament, the European Commission (EC) and the European Council thus adopted the EU Data Protection Reform Package, with the Regulation on the protection of individuals with regard to the processing of personal data on the free movement of such data – GDPR, as its main instrument. When the GDPR entered into force and replaced the existing Directive, this gave rise to a lot of commotion. However, most of the obligations described in it are not new. The GDPR reinforces and extends the regulatory framework as was set by the Directive. It provides for the same concepts and analyses them further while also making new additions. Because the GDPR is very similar to its predecessor, the existing case-law on the Directive gives good guidance to answer how data protection principles and obligations should be interpreted under the GDPR.

The choice for a new Regulation instead of a new Directive is important though. While Directives are not directly applicable and require to be transposed into the national laws of the Member States, Regulations enjoy a general application and are directly binding in its entirety in all the EU Member States. However, despite its enhanced potential to harmonise the EU legal framework, the GDPR does provide a large margin of discretion for the Member States to diverge from the standard said forth in the GDPR. This is true, for example, with regard to the lower age applicable to a child's consent, the data protection officer, or the conditions applicable to data transfers.¹⁹

The following chapter will discuss the integration of the identified legal requirements to the CyberSANE solution according to the data protection by design (DPbD) principle. This principle was legally established in the GDPR for the first time and calls for the adoption of organisational and technical measures designed to implement data protection principles in order to meet the requirements of the data protection framework and respect the data subjects' rights.²⁰

To achieve this goal, the DPbD principle addresses the enhancement of personal data protection in a twofold manner. 1) It requires from data controllers²¹ to implement organizational and technical measures in order to ensure that all processing activities are performed in compliance with the data protection framework. 2) The DPbD principle derives from the 'privacy by design' principle and the 'privacy engineering' concept. It relates to the proactive integration of data protection rules to computer and software code and invites the developers of tools and technologies to take into account the data protection framework by which the end-users will have to abide.²² In particular, according to recital²³ 78 GDPR, **"when developing, designing, selecting**

¹⁹ Article 8(1), Article 37(1)(a), (b), Article 49(1)(d), (g), and (4) GDPR.

²⁰ Article 25 GDPR

²¹ More on the concept of data controllers and their obligations in section 3.1.2.

²² A. Cavoukian, Privacy by Design, Leading Edge, IEEE Technology and Society Magazine, 2012, 31/4

²³ Together, recitals constitute the preamble of a legal text and, as such, they precede the main text of a legislative act or a contract. Recitals are not legally binding, however, they usually provide for useful

and using applications, services and products that are based on the **processing of personal data** or process personal data to fulfil their task, **producers** of the products, services and applications should be encouraged to **take into account the right to data protection** when developing and designing such products, services and applications and, with **due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations.**"

CyberSANE will rely on the processing of personal data, the developers of the CyberSANE system must take into account the obligations with which the end-users will have to comply after the end of the project, so as to allow the end-users to fulfil their data protection obligations. In doing so, CyberSANE will facilitate the implementation of the DPbD principle by the users, since the developers will have already taken it into account when building the CyberSANE solution. The requirements described below will also provide a helpful guidance to end-users employing the CyberSANE solution so as to guarantee security of their information systems.

3.1 The General Data Protection Regulation

The GDPR entered into force on 25 May 2018. It was adopted to align data protection rules with the digital age and is meant to provide substance to the fundamental right to protection of personal data, as established by Article 8 of the *Charter* and Article 16 of the TFEU. It regulates the processing of personal data in a very wide manner. It applies in public, private and primarily commercial contexts.

3.1.1 Scope, concepts and main definitions

Before delving into the material scope of the GDPR, the essential concepts of ‘data controller’ and ‘data processor’ need to be described. The **data controller** is the person competent to make any **decisions, alone or jointly, relating to the purposes and means** of the processing activities.²⁴ The actual processing operations can lawfully be delegated to another party that will be qualified as data processor under the GDPR, however, the data controller remains responsible for the lawfulness of the processing. The data controller is the norm addressee of the GDPR. On the other hand, the **data processor** refers to the person processing personal data **on behalf of the controller.**²⁵ This last element is of crucial importance, since the delegation of processing activities by the controller will determine the qualification of a party as controller or processor. Thus, whereas the controller detains the control over the decisions regarding the purpose and means, the processor merely executes those decisions. If the processor is not involved in the decision-making process, he will only be responsible for compliance with the GDPR provisions that specifically address the processor.

3.1.1.1 Material scope

The GDPR applies to the **processing of personal data wholly or partly by automated means** and to the processing other than by automated means of personal data which form **part of a filing system** or are intended to form part of a filing system, as set out in its Article 2.

explanation to the main text of a legal text and should be taken into account when interpreting the actual legally binding provisions.

²⁴ Article 4 (7) GDPR.

²⁵ Article 4 (8) GDPR.

D2.2 – Legal and Ethical Requirements

As the scope of the GDPR is substantially wide, it is of paramount importance to delineate the key concepts that trigger its application. There are two different components to be identified in the phrasing of this Article 2. First, in order for the GDPR to be applicable, the data need to be personal data. Second, the personal data need to be processed either wholly or partly by automated means or, if the personal data are processed in another way than by automated means, they need to form part of a filing system or be intended to form part of a filing system. The flowchart below provides for a schematic overview:

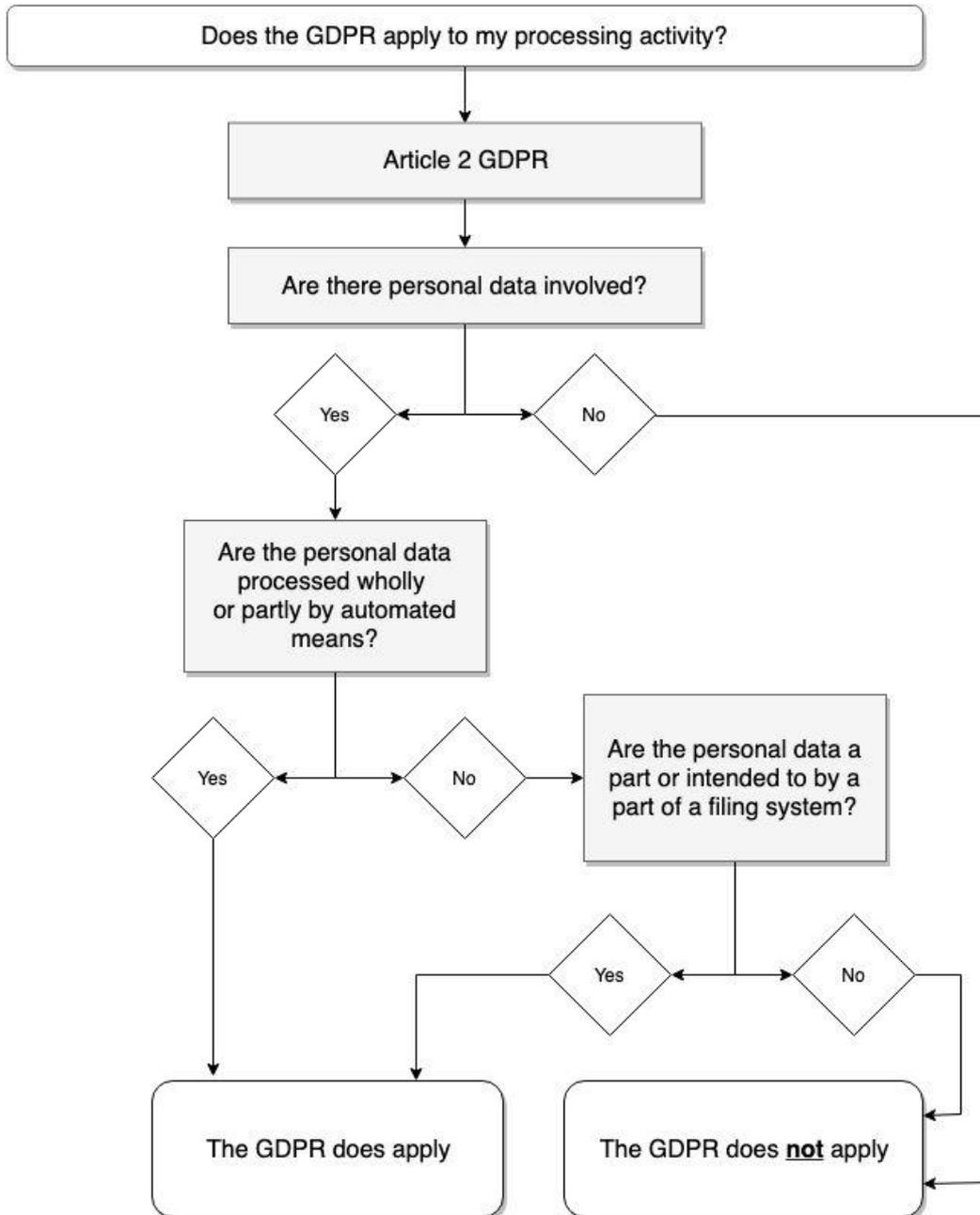


Figure 4 Flowchart on the applicability of the GDPR

Naturally, this broadly defined scope requires for several concepts to be explained. More specifically, one has to know (i) when data are to be considered ‘*personal data*’, (ii) when personal

data are ‘*processed by automated means*’ and (ii) when are they ‘*part of – or intended to be part of – a filing system*’.

3.1.1.2 Personal data

The concept of ‘personal’ data is explained by Article 4(1) GDPR:

‘personal data’ means **any information relating to an identified or identifiable natural person** (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, psychological, genetic, mental, economic, cultural or social identity of that natural person.

The GDPR contains a broad notion of personal data. It may consist of any sort of information, not only information concerning what is traditionally considered to be within the private sphere. This notion answers the need to be as general and technology-neutral as possible and to cover all information that may be linked to an individual (the data subject). It concerns information about a person that can be identified, directly or indirectly, by reference to a direct identifier or by a combination of indirect identifiers or other factors specific to his or her identity. There are thus four components to the notion of personal data: (i) information, (ii) a natural person, (iii) identifiability and (iv) a link connecting the information and the data subject.

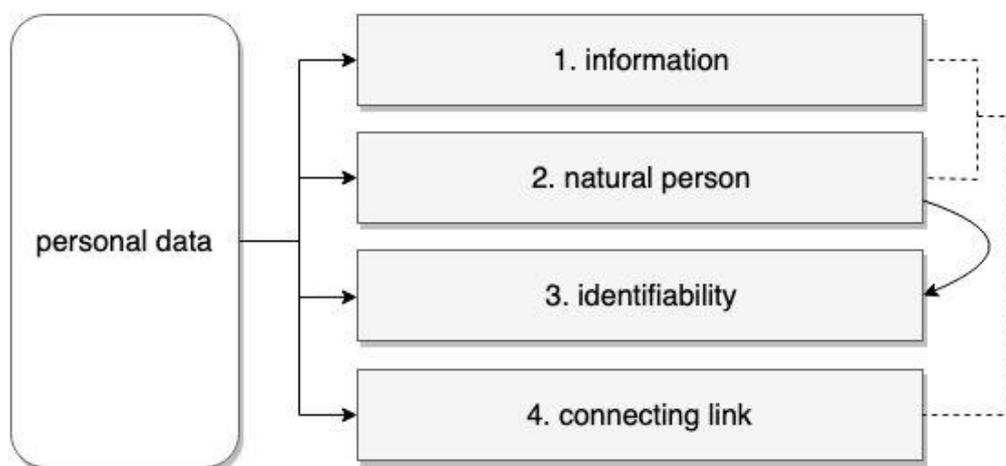


Figure 5 Cumulative requirements for data to be personal data

Those four building blocks are closely intertwined and feed on each other. Taking methodology and overall clarity into account, this document will elaborate on them separately. Although the range of data to be processed once the end-users will exploit the system will vary, this document will try to explain these main concepts with a focus on the potential caveats to take into account when processing data within the framework of CyberSANE.

3.1.1.2.1 Information

The term ‘**any information**’ contained in the GDPR reveals the ambition of the EU to catch as much data as possible. Personal data do not need to reveal information relating to the private life of a person though. Any kind of information can be personal data and the protection is not limited to matters of the private sphere of an individual. Information as basic as an IP address, therefore,

contains information. Think for example of smart grid data that allow for the monitoring of energy consumption and their adjustment capability. By collecting this information, smart grid processes personal data that is capable of revealing personal information, such as household habits and life patterns, as well as the number of hours spent at home.

The qualification as personal data is **not altered by any kind of format or medium** on which the information is contained. Data can be for example alphabetical, numerical, graphical or photographic. It includes information kept on paper as well as information stored in a computer, in particular, sound and image qualify as personal data.

3.1.1.2.2 *Natural person*

To be qualified as ‘personal data’, the data must disclose information of a **natural person, a living being**. Data relating to legal persons do not enjoy protection under the GDPR. However, note that this does not mean that every data related to a particular undertaking would be exempted from the scope of protection conferred by the GDPR. If, for example, data about an undertaking *de facto* equates to the revealing of information about a natural person, this data would be considered ‘personal data’. This, for example will be the case with sole proprietor businesses as the information of a firm’s solvability, inevitably discloses information about the financial situation of its proprietor.

3.1.1.2.3 *Identifiability*

To define the difference between, whether a natural person is identified or identifiable, a data controller or another person should take into account **all reasonable means that are likely to be used – such as singling out – to directly or indirectly identify the natural person**, which makes it possible to treat one person differently from another. Identification thus requires elements which describe a person in such a way that he or she is distinguishable from all other persons and recognizable as an individual. The name of a person is a prime example of this. However, other means may have a similar effect. Think for example of a telephone, social security number or vehicle registration number. These attributes are all able to make a person identifiable, at least indirectly.

More pertinent to the CyberSANE project, it should be noted that the European doctrine and case-law favour a rather broad interpretation of the concept of ‘personal data’ and therefore the threshold for data to be qualified as personal data, is very low. Possible attributes include computerized files, cookies and web traffic surveillance tools. It is not necessary to have the name or other explicit information such as the address of the individual disclosed. Electronic devices no longer require the disclosure of someone’s identity in the narrow sense, it is perfectly possible to categorise a person and link certain decisions to him or her, without specifically needing to know that person’s name. The qualification of data as personal data can, therefore, result from the content itself of the data, but also of its purpose or result. It is important that the CyberSANE developers and end-users are aware of this. Every possible type of data can potentially become personal data, for example, a simple traffic data within an information system that can be linked to the personal computer of an employee and this traffic data may become personal data.

There is **no need for actual identification of the data subject** for the GDPR to apply. As the definition of ‘personal data’ indicates, it is sufficient that the person concerned be identifiable. This is the case when there are enough elements available through which the person can be directly or indirectly identifiable. The benchmark for determining this, is whether it is likely that reasonable

D2.2 – Legal and Ethical Requirements

means for identification will be available and administered by the foreseeable users of the information, including information held by third-party recipients.

To ascertain whether means are reasonable likely to be used to identify the natural person, **account should be taken of all objective factors**, such as to cost of and the amount of time required for identification, taking into account consideration the available technology at the time of the processing and technological developments.

In *Breyer v Bundesrepublik Deutschland*, the CJEU considered that a dynamic IP address, which an online media services provider registers when a person accesses a website that the provider has made accessible to the public, constitutes personal data where only a third party – the internet service provider in this case – has the additional data necessary to identify the person.²⁶ It held that “it is not required that all information enabling the identification of the data subject must be held in the hands of one person” for information to constitute personal data. Users of a dynamic IP address registered by an internet service provider may be identified in certain situations, for instance within the framework of criminal proceedings in the event of cyber-attacks, with the assistance of other persons. According to the CJEU, when the provider “has the legal means which enable it to identify the data subject with additional data which the internet provider has about that person”, this constitutes “a means likely reasonable to be used to identify the data subject”. Therefore, such data are considered personal data.

CASE	REQUIREMENT
The CyberSANE system processes personal data	CyberSANE developers can minimize the applicability of the GDPR and the obligations imposed by it through anonymization techniques to the degree possible. CyberSANE must be developed taking into account that potentially the vast majority of data processed will be personal and hence protected by the EU Data Protection framework

3.1.1.2.4 Connecting link

Lastly, for data to constitute personal data, they must related to the individual in question, there must be a **connecting link between the information and the natural person, the information should be ‘about’ the individual**.²⁷ It is not necessary that the data focuses on someone before a connecting link can be found.

The flowchart below provides for a useful tool to assess whether data constitutes personal data or not:

²⁶ Judgement of 19 October 2016, Patrick Breyer v. Bundesrepublik Deutschland, C-582/14.

²⁷ Article 29 Working Party, Opinion 4/2007 on the concept of personal data, WP136, 20 June 2007.

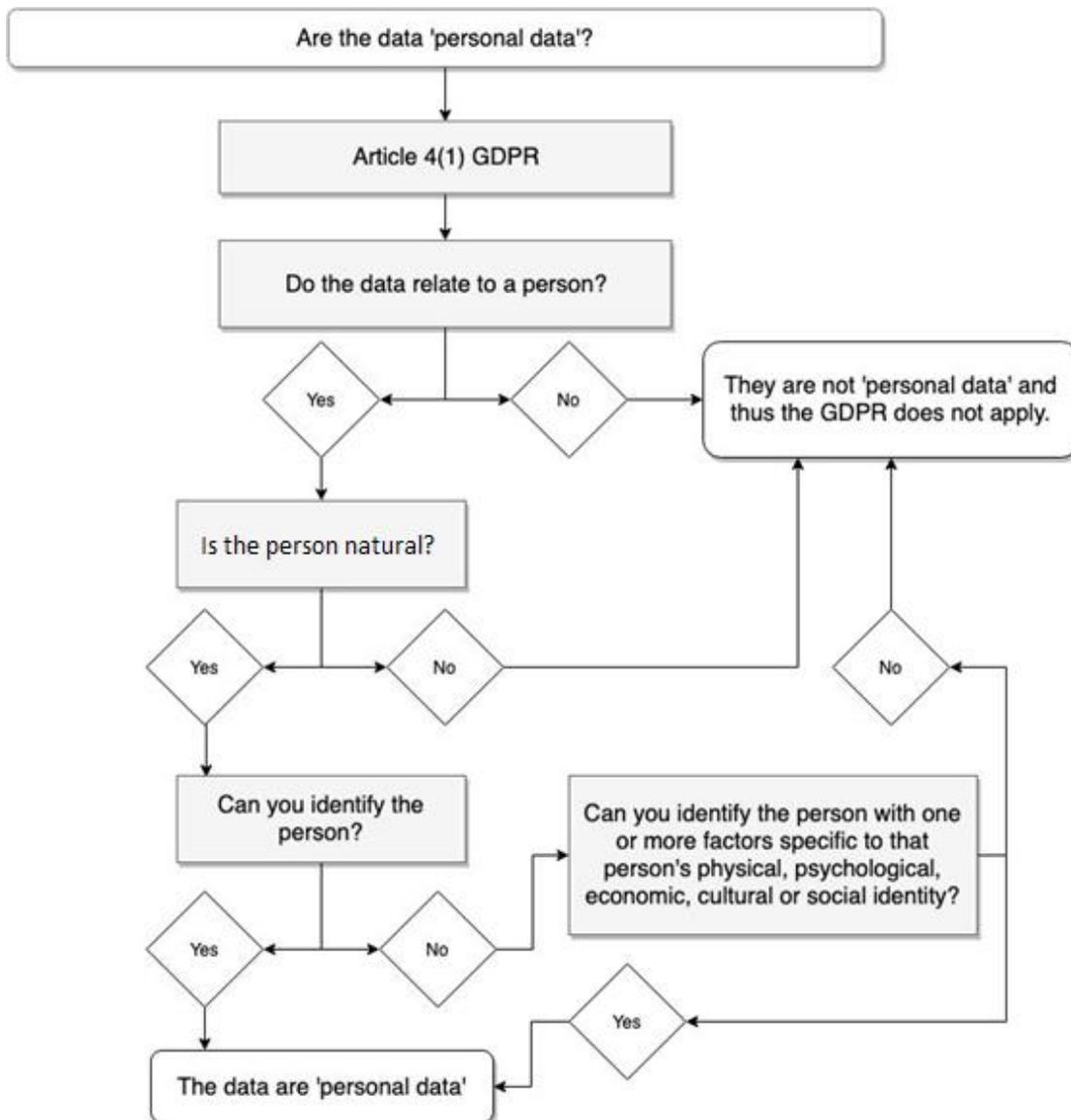


Figure 6 Flowchart on the concept of personal data

3.1.1.3 Processing

Data processing concerns any operation performed on personal data and is defined by Article 4(2) GDPR:

'processing' means **any operation or set of operations which is performed on personal data or on sets of personal data**, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

D2.2 – Legal and Ethical Requirements

It follows from the reading of this provision that the term ‘processing’ covers automated, as well as non-automated processing, so that the scope of the protection it confers on data subjects does not depend on the techniques used for processing and, thus, to avoid the risk of that protection being circumvented.²⁸ GDPR does make a difference between automated and non-automated processing in the sense that it only applies to the manual processing of personal data when it forms part of a filing system, or at least if it is intended.

If the personal data is being processed via **wholly or partly automated means**, the GDPR applies. In other words, the GDPR automatically applies to any processing of personal data as soon as this is partly done with the help of, for example, a computer, a mobile device or a router. In this regard, the CJEU stated that operations trigger the applicability of the GDPR if they result in *“exploring the internet automatically, constantly and systematically in search of the information which is published there, the operator of a search engine ‘collects’ such data which it subsequently ‘retrieves’, ‘records’ and ‘organises’ within the framework of its indexing programmes, ‘stores’ on its servers and, as the case may be, ‘discloses’ and ‘makes available’ to its users in the form of lists of search results”*.²⁹ Such actions thus fall under the scope of the GDPR, regardless of the fact that the operator of the search engine also carries out the same operations in respect of other types of information and does not distinguish between the latter and the personal data. Although the CyberSANE solution does not aim to provide for an internet search engine, the proposed techniques will provide the basis required for supporting the processing and storage of data gathered from various sources (e.g. structured data – logs and network traffic; unstructured data – data coming from social networks and dark web) in a unified structure in order to discover the relationships between devices and the evidence and produce a timeline of the incident, including a map of affected devices and a set of meaningful chains of evidence (linked evidence). In other words, the very low threshold for ‘automated data processing’ is easily reached.

If personal data is not processed via wholly or partly automated means, the GDPR will only apply provided that the data is comprised in a manual **filing system**, or is intended to form part of such system. The CJEU indicated that a filing system is *“any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis”*.³⁰ The applicability of the GDPR to a manual filing system is less relevant to the CyberSANE solution and does not require much more in-depth analysis since, in the framework of CyberSANE, all processing is intended to be conducted - at least partly - by automated means. However, it is useful to remember that the users of the CyberSANE solution will not be able to escape the applicability of the GDPR and its obligations by keeping hard copies of any suspicious navigator’s identity or by only exchanging paper versions of the CyberSANE solution’s findings.

The flowchart below provides for a visual of summary of what has been discussed in this section:

²⁸ Jehovan Todistajat, §52

²⁹ Google Spain, §28

³⁰ Jehovan Todistajat, §55

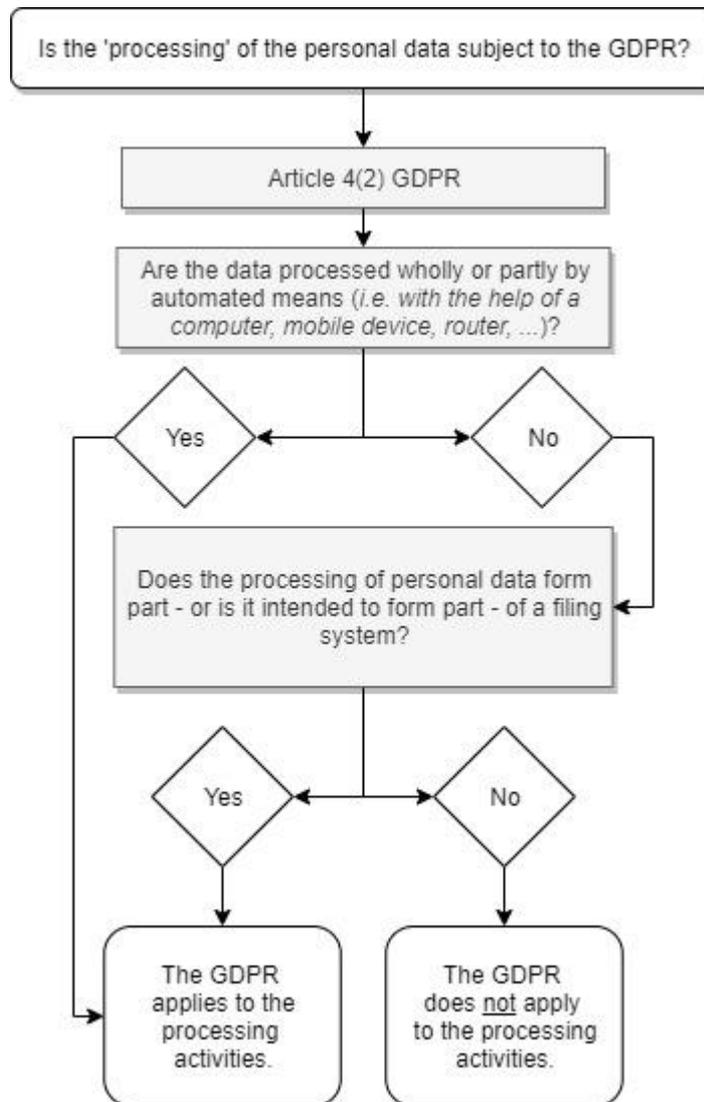


Figure 7 Flowchart on the concept of processing relevant to the material scope of the GDPR

3.1.1.4 Special categories of data

Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection because the context of their processing potentially creates a significant risk to the fundamental rights and freedoms. These personal data are indicated as **'special categories of data', so-called sensitive data**, and are listed in Article 9 GDPR.

These special categories of personal data are personal data that are considered sensitive because they reveal:

- Racial or ethnic origin
- Political opinions, religious and other beliefs, including philosophical beliefs
- Trade union membership
- Genetic data and biometric data processed for the purpose of identifying a person
- Health-related information

D2.2 – Legal and Ethical Requirements

- Sexual life or sexual orientation.

There are different reasons to believe that the CyberSANE solution will process sensitive personal data.

1. The CyberSANE technology may engage in the processing of **health-related information**, especially when used as a solution to ensure the security of an information system within a hospital. One of the services that hospitals may offer is the remote monitoring and potentially emergency treatment of patients in real-time. As such, it could collect and process data coming from various medical devices and instruments connected, such as smart insertable cardiac monitoring devices to inform clinicians of data relating to their patients. The CyberSANE solution aims to accompany such health-related service to ensure security of the information it contains. To do so CyberSANE will correlate real-time information of the hospital with information about the latest mechanisms of cyber-attacks. This real-time information encompasses patient data and, thus, health-related data. By correlating this data to other datasets, the CyberSANE technology processes these patient data according to the definition in the GDPR.
2. CyberSANE may include the processing of **biometric data**, for instance if CyberSANE engages in facial recognition to identify potential threatening hackers. By incorporating a neural network for face detection, in digital images and videos, that supports facial landmark detection, head pose estimation, facial action unit recognition, facial features extraction and eye-gaze estimation, all these different types of data inevitably constitute biometric data.
3. CyberSANE might process data disclosing **sexual orientation, political opinion and religious or other beliefs**. Through its web crawling activities, the DarkNet component aims to provide an inclusive list of security related data which encompasses data coming from social networks, dark and deep web such as pictures, tweets and discussion on forums. Because the CyberSANE developers aim to set up a tool to ensure cybersecurity, they might create web crawlers that do not purely limit themselves to relevant cybersecurity-related data and, in doing so, they might process a lot of sensitive information.

3.1.1.5 Data quality principles

Data quality refers to several principles described in Article 5(1) GDPR. They serve as a starting point for more detailed provisions throughout the GDPR.

Personal data shall be:

- (a) Processed **lawfully, fairly and in a transparent** manner in relation to the data subject ('lawfulness, fairness and transparency')
- (b) Collected for **specified, explicit and legitimate purposes** and **not further processed in a manner that is incompatible** with those purposes; further processing for achieving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');
- (c) **Adequate, relevant and limited** to what is necessary in relation to the purposes for which they are processed ('data minimisation');

D2.2 – Legal and Ethical Requirements

- (d) **Accurate** and, where necessary, **kept up to date**; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
- (e) Kept in a form which permits identification of data subjects for **no longer than is necessary** for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');
- (f) Processed in a manner that ensures **appropriate security** of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ('integrity and confidentiality').

In the following part, these data quality principles will be discussed more in depth:

3.1.1.5.1 *Lawfulness, fairness and transparency*

Article 5(1) GDPR really describes three different principles. The first one relates to the lawfulness principle. To be considered compliant with the principle of lawfulness, the end-users of CyberSANE system, who will be considered as controllers of the personal data processed through CyberSANE, must establish a legal basis on which its processing activities will rely. The different legal grounds are exhaustively enumerated by Article 6 GDPR and will be further discussed below (see section 3.1.2.1).

In addition to lawful processing, EU data protection law demands that personal data are processed fairly. This requirement of fair processing governs primarily the relationship between a data controller and the data subject and entails a few obligations for whoever decides to process personal data. According to the principle of fair processing, the CyberSANE must make sure that data subjects and the general public are aware of the processing conducted on their data and understand what exactly is happening to it. It should not be performed in secret and data subjects should be aware of the risks that accompany such processing. However, the fairness principle goes beyond transparency obligations and should more be understood as an obligation for the CyberSANE end-users to process personal data in an ethical manner.

This principle sets out an obligation for the CyberSANE end-users to take all appropriate measures so as to keep the data subjects informed. CyberSANE must be developed and exploited in a manner that allows for complete transparency, in order for end-users and data subjects to be informed on the processing activities. Data subjects should ideally be given all necessary information before the processing of their data starts, information should be readily available to them, but the transparency principle also requires that additional information be offered to the data subjects whenever they formulate a request of access to their own data.

CASE	REQUIREMENT
The CyberSANE system processes personal data for security reasons and requires for a	The CyberSANE developers must ensure that the technology allows for the end-users to

D2.2 – Legal and Ethical Requirements

<p>certain level of secrecy while its use must remain transparent</p>	<p>inform all individuals concerned of their secret data processing activities on their websites via a privacy policy and that all processing activities are conducted fairly.</p> <p>CyberSANE developers must further ensure that clear comprehensive and accurate information is provided to end-users in a human-readable format that explains the functions, sources and risks associated.</p>
---	---

3.1.1.5.2 Purpose limitation

The principle of purpose limitation prescribes that the purpose of processing must be established before the processing starts and prohibits further processing of data in a way that is incompatible within the original purpose, though the GDPR foresees exceptions to principle. These include processing for archiving purposes in the public interest, scientific and historical research purposes and statistical purposes.³¹ Purpose specification is an essential condition and a prerequisite for applying the other data quality principles.³² The data controller must define, in advance of every processing activity, the purpose for which processing will take place. Any processing following the initial collection of the data must be restricted to the predefined purpose or to a purpose compatible to the initial one. Compatibility may only be assessed on a case-by-case basis, depending inter alia on the context, the nature of the data, the impact of the further processing on the data subjects and the safeguards implemented by the controller.³³

This principle ensures that CyberSANE end-users process personal data only for a specific and well-defined purpose and to only engage in additional processing if the purposes thereof are compatible with the original one. CyberSANE should allow for the purpose limitation principle to be implemented through controls on uses that go beyond the purpose of each processing activity to the extent that is technically possible.

CASE	REQUIREMENT
<p>The CyberSANE end-users process vast amounts of data for different purpose</p>	<p>CyberSANE developers should design the system so that only relevant data are processed. The relevance shall be determined by the link of the data processing with the specific purpose for which CyberSANE is used. CyberSANE should allow for different datasets to be processed differently, in accordance to their different purposes</p>

³¹ Article 5 (1)(b)§2 Regulation (EU) 2016/679.

³² Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, WP 203, 02 April 2013, available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf Last accessed on 24.08.2017.

³³ Article 6 (4) Regulation (EU) 2016/679.

D2.2 – Legal and Ethical Requirements

The CyberSANE system processes personal data beyond their original purpose	CyberSANE should ensure that further processing is performed only to the extent that is strictly necessary for the purpose of security.
--	---

3.1.1.5.3 Data minimisation

Data processing must be limited to what is necessary to fulfil a legitimate purpose and should only take place in case the purpose of the processing cannot be reasonably fulfilled by other means. It should not disproportionately interfere with the interests, rights and freedoms of the individuals concerned. A practical problem that may arise with regard to this principle occurs when CyberSANE deploys its data mining activities. Because data mining is the process finding correlations and patterns in large relational databases, it requires the analysis of large amounts of collected data in order to be effective.

Measures to minimise the processing of personal data must be applied in particular with respect to:

- **Proportionate collection:** It is important that the principle of proportionality is observed in the data collection phase. In order to do so, online sources should be pre-selected in advance and must have a clear and demonstrable link with the purpose of CyberSANE. For instance, the crawlers shall be designed and used in a ‘focused’ way so as to limit the unnecessary collection of personal data that may not be relevant for the detection of cyber security-related content. The system developers shall be proactive in determining a metric system for the criteria used for crawling and collecting online content.
- **Deletion of unnecessary data:** Once information has been indexed, it is very likely that personal data remain stored although not necessary anymore for the specific purpose for which they were collected. Such data must be identified and made subject to technical measures that will mitigate data protection risks, such as deletion or anonymisation.
- **Storage and retention:** The storage of personal data shall follow specific and pre-defined rules on storage and retention, with particular reference to the determination of a retention period. Different time periods for each category of data subjects shall be in place. Personal data processed by the CyberSANE system shall be therefore securely disposed after its processing unless relevant for the investigation, where alerts are automated.
- **Aggregation:** The processing of personal information in a big data context is often beneficial to determine trends, patterns and correlations. When data is redundant and excessive with respect to the purpose of the data collection, data must be separated from other data. Filtering relevant personal data in an aggregated form results in the minimization of processing excessive personal information and makes it significantly less sensitive.

CASE	REQUIREMENT
------	-------------

D2.2 – Legal and Ethical Requirements

<p>Vast amounts of data are being processed by the CyberSANE system</p>	<p>CyberSANE should function on restricted access controls, according to the function and capacity of the use. The data-controller shall make sure the process takes place under the principle of proportionality: access of users to the system shall be foreseen only insofar as it is necessary by the purpose for processing, respectful of the separation of duties with a need-to-know principle approach.</p>
---	--

3.1.1.5.4 Accuracy

The accuracy principle requires from anyone processing personal data to take reasonable measures to ensure with reasonable certainty that the data are accurate and up to date. Inaccurate data must be erased or rectified without undue delay. Data may need to be checked regularly and kept up to date to guarantee accuracy.

CASE	REQUIREMENT
<p>Personal data processed by CyberSANE must be accurate and up to date</p>	<p>CyberSANE must allow for continuous checks and the rectification of inaccurate data</p>

3.1.1.5.5 Storage limitation

According to the storage limitation principle, personal data must be deleted or anonymised as soon as they are no longer needed for the purposes for which they were collected.

CASE	REQUIREMENT
<p>The CyberSANE system must store personal data for restricted periods of time</p>	<p>CyberSANE developers must ensure that adequate technical and organizational measures are adopted to make sure that personal data can be deleted or anonymised whenever they lose their necessity to achieve cyber security.</p>

3.1.1.5.6 Integrity and confidentiality

Integrity and confidentiality are commonly also referred to as the 'data security principle'. This principle requires that appropriate technical or organisational measures are implemented when processing personal data to protect the data against accidental, unauthorised or unlawful access, use, modification, disclosure, loss, destruction or damage. The security and confidentiality of personal data are key to prevent any adverse effects for the individual concerned, and, include technical as well as organisational measures. Following the DPbD principle, the developers of CyberSANE should design the technology to help ensuring integrity and confidentiality of the data.

D2.2 – Legal and Ethical Requirements

Depending on the circumstances at hand, security of data can include measures such as **encryption, pseudonymisation or anonymisation**. Security can also encompass a regular testing and evaluating of the adopted measures and their effectiveness to secure data. In what will follow, these security methods are discussed further.

The pseudonymisation, anonymisation, encryption and splitting of personal data provide for tools to enhance the protection of individuals’ personal data. Their aim is to prevent – or at least hamper – re-identification of individuals, each to a different extent, so that security and confidentiality can be guaranteed, these will be referred to as ‘privacy enhancing techniques’. In order to assess the requirements stemming from the data protection regulatory regime, one needs to first analyse the legal effect that the main function of the privacy enhancing techniques of PrivacyNet component of the CyberSANE system will have on the application of said regulatory regime. These privacy enhancing techniques aim to de-identify individuals to a certain extent, the identifiability component of the notion of ‘personal data’ is attacked, which might influence the applicability of the GDPR’s material scope. When personal data are being pseudonymized, anonymized, encrypted or split, this has an impact on whether or not they will maintain their personal nature and, thus, whether their processing still needs to comply with the different obligations enumerated by the GDPR.

The GDPR does not apply to data rendered anonymous in such a way that the data is no longer identifiable.³⁴ **Anonymisation** requires that all identifying elements are eliminated from a set of personal data so that the data subject is no longer identifiable. Whenever it is not possible to identify an individual, directly or indirectly, in particular by reference to an identifier (*i.e. a name, an ID number, location data or online identifier*), the data does not amount to personal data. In order to assess whether the data used on which privacy enhancing or de-identification techniques have been performed amount to anonymized data, one should use and interpret these criteria.

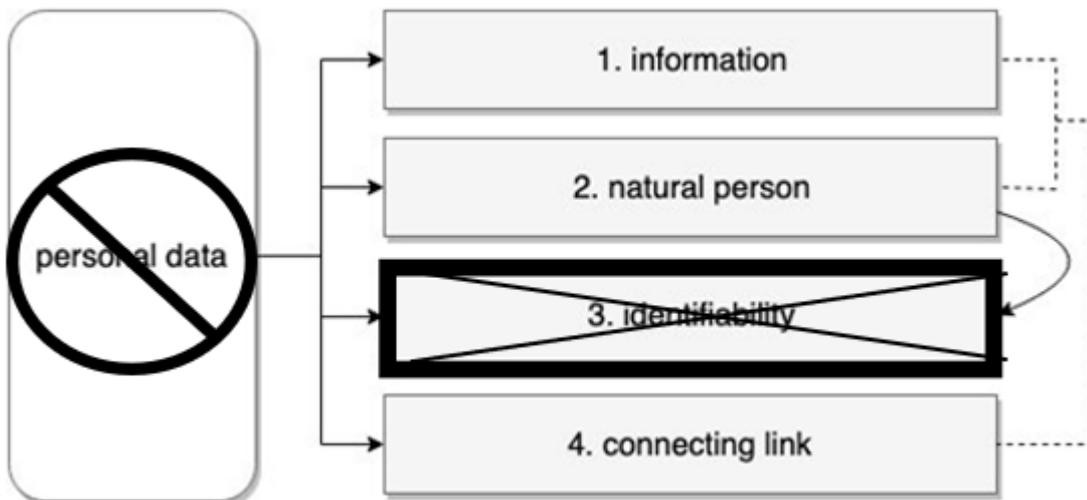


Figure 8 De-identifying individuals takes away the personal character of data

The recitals of the GDPR clarify that *to determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain*

³⁴ Recital 26 GDPR

D2.2 – Legal and Ethical Requirements

*whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.*³⁵

It must be stressed that there is currently no consensus on what constitutes the ‘means reasonably likely to be used’ to identify a natural person. Two main streams of thoughts can be identified. On the one hand, the absolute approach supports that personal data that have undergone privacy enhancing techniques will almost always remain personal as long as anyone in the world is able to identify the individual whom the information relates to. This approach claims that no technique is ‘perfect’ and cannot offer a waterproof solution against future technological developments. On the other hand, the relative approach stands for a more risk-based solution and builds further on the criterion of ‘means reasonably likely to be used’. According to this relative approach, privacy enhancing techniques provide for different degrees of de-identification taking into account contextual elements, such as the technical progress, the safeguards restricting access to the data and the overall realistic risk of re-identification. In other words, identification may not be considered as likely if excessive efforts, in technical, organizational and financial terms are required to reverse the privacy enhancing techniques. The Working Party 29 (WP29)³⁶, recitals from the GDPR and the CJEU seem to support the relative approach rather than the absolute approach.

The WP29 indicated that even if there is a hypothetical possibility to single out the individual, this is not enough to consider a person ‘identifiable’. It should be noted that **anonymising personal data is a challenging thing** to do. There is a shallow threshold for data to be considered personal data, yet the benchmark for anonymisation to be a suitable protection mechanism is very high and criticised. After a number of re-identification attacks were conducted on anonymised datasets, the effectiveness of anonymisation as a protective measure has been put into question.³⁷ In its Opinion 05/2014, the WP29 analyses the effectiveness and limits of different anonymisation techniques. It acknowledged the potential value of such techniques but underlined that they do not necessarily offer a ‘one fits all’ solution. In other words, **the appropriateness of anonymisation needs to be assessed on a case-by-case basis**. Irrespective of the technique used, identification must be prevented, irreversibly. This means that for data to be anonymised, no element can allow, by exercising reasonable effort, to re-identify the person(s) concerned. The risk of re-identification can be assessed by taking into account “the time, effort or resources needed in light of the nature of the data, the context of their use, the available re-identification technologies and related costs”.

As opposed to anonymised data, **pseudonymised data remain subject to the scope of the GDPR**. Article 4(5) GDPR defines pseudonymisation as the processing of personal data in such a manner that the data can no longer be attributed to a specific subject without the use of additional information. To be pseudonymised, this additional information should be kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable person.

Within the framework of CyberSANE, it is important to remember the anonymisation of personal data is possible and can help the end-users to conduct their project in a privacy-friendly way. Indeed, anonymisation is not required to be completely risk-free. It must be possible to mitigate

³⁵ Recital 26 GDPR.

³⁶ The WP29 was an independent European working party that dealt with data protection and privacy issues until the entry into force of the GDPR. Since the GDPR, the WP29 has been replaced with the European Data Protection Board (EDPB).

³⁷ See also section 3.4.

D2.2 – Legal and Ethical Requirements

the risk of identification until the risk is remote. Anonymisation is not equal to pseudonymisation and that the latter is more easily accomplished than the former.

Aside from anonymisation, pseudonymisation and encryption, CyberSANE developers may also help enhance data security by hiding information. In principle, personal data shall be processed in plain view only insofar as it is strictly necessary and justified. By using hiding techniques and limit view to some external actors or third parties, CyberSANE end-users may restrict the view of personal information to those players with a grounded interest.

Access rights can provide for an extremely valuable functionality when setting up the privacy features of an IT system. They reflect the user profile as well as play a key role in establishing the stakeholders that can process personal information. CyberSANE end-users shall be given access to the system according to the purposes for which the infrastructure is used, the capacity of the user and its entitlements within the internal structure. This will ensure separation of duties based on a need-to-know principle. For example, administrative workers should not be granted the same access to a patient's file as that patient's doctor.

CASE	REQUIREMENT
<p>The CyberSANE system must keep personal data in a secure manner, preventing unauthorised access or unwarranted loss of data.</p>	<p>The CyberSANE system must be designed taking into account confidentiality and secrecy requirements, with limitations as to access and management of the system. CyberSANE developers and end users must take into account the implementation of security measures (equipment access control, data media control, storage control, user control, data access control, communication control, input control, transport control, recovery, reliability, integrity) based on an assessment of risks for the protection of individuals' data against the nature and scope of processing. CyberSANE developers shall ensure that access rights are calibrated so as to limit the plain view of personal data processed by CyberSANE only to those competent subjects. Limitations on access and use of CyberSANE to third parties shall be designed and implemented before the system becomes fully functional to the end-user</p>

3.1.1.5.7 *Example of web crawling*

In order to demonstrate the application of these principles to the CyberSANE envisaged processing activities, the example of web crawling and the DarkNet component will be used. Crawled personal data should be retained only insofar as a retention period is established and frequently reviewed, possibly in a systematic way. Different time limits must be set out according the different categories of data subjects. Alerts for deletion and review shall be set up in an automated manner. Unnecessary personal data should be deleted as soon as possible or at the very least made anonymous. Where possible, crawled personal data shall be further processed

in an aggregated form to maximise the efficiency of trends and patterns discovery whilst ensuring a minimised data processing operation. Crawlers should be coded in a way that minimize websites revisits, its velocity and the irrelevant duplication of crawled webpages in order to avoid the risk of causing denial of service while operating.

3.1.2 Data controller's obligations

The data controller is the person responsible for the processing activities and the normal addressee of the GDPR. The data controller is the person competent to make any decisions, alone or jointly, relating to the purposes and means of the processing activities and is responsible for the lawfulness of the processing.

3.1.2.1 Legal basis

One of the obligations of the data controller is to make sure that personal data is lawfully processed by basing all processing activities with the same distinct purpose on a legal ground and to restrict the processing to that defined purpose. This obligation stems from the principle of lawfulness and is further described by Article 6(1) GDPR, which provides an exhaustive list of six potential legal grounds:

Processing shall be lawful only if and to the extent that at least one of the following applies:

- (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- (c) processing is necessary for compliance with a legal obligation to which the controller is subject;
- (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interest are overridden by the interest or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

The processing of personal data by the CyberSANE solution is aimed at securing the information systems of the end-users of CyberSANE and, all data processing activities need to rely on a legal base to be considered lawful. Depending on the nature of each processing activity, the specific purpose and the dataset involved, the legal basis might differ.

The initial collection of data which will form part of the network information system the CyberSANE solution will seek to protect, might be based on **consent**, for instance in the case of clients of the end-users. Consent must be freely given, specific and informed, it must constitute an unambiguous indication of that data subject's wishes by which he or she, by a statement or by a clear affirmative action indicates an agreement to the processing of personal data relating to him or her.³⁸ It clearly follows from these exigent requirements that end-users will need to invest

³⁸ Article 4(11) GDPR.

D2.2 – Legal and Ethical Requirements

enough time and resources to make sure their patients are well informed before they can give such consent.

In many cases, however, the individuals concerned will not always be aware of the processing activities of CyberSANE for the overarching purpose of cybersecurity. The reliance on consent as a legal basis is for example very unlikely to meet the aforementioned criteria when the data subject is an employee of the data controller. Because the relationship between employees and employers typically shows some hierarchy, power asymmetry or, at the very least, a form of dependency from the employee towards their employer, consent cannot be said to be entirely and truly freely given.³⁹

Furthermore, because of the covert nature of the employed techniques to attain the purpose of cybersecurity, end-users will need to rely on either (i) a **legal obligation** to which the data controller is subject or (ii) **legitimate interests** to ensure network and information security.

- To rely on the necessity to comply with a legal obligation, CyberSANE end-users will be able to rely on, for instance, the NIS-Directive, which will be further discussed below (See Chapter 4), as well as any other sector specific national legal instrument on the (cyber)security of critical infrastructures.
- To rely on legitimate interests as a legal ground, the data controller must ensure that the processing does not override the interests or fundamental rights and freedoms of the data subject.

The difficulty for end-users to rely on their legitimate interest lies in the fact that they need to make a balancing exercise for each and every different processing context against the interests of each actor involved. In other words, the processing of patient data for example, for the securing hospitals' information systems will be assessed completely different than in the energy industry.

Recital 49 of the GDPR indicates that the **processing of personal data to the extent that it is strictly necessary and proportionate for the purposes of ensuring network and information security** (*i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), by providers of electronic communications networks and services and by providers of security technologies and services*) constitutes a legitimate interest of the data controller concerned. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems.

CASE	REQUIREMENT
The CyberSANE system processes personal data	The legal basis for using the CyberSANE system should be established in advance. CyberSANE developers should take into account that each processing activity might

³⁹ Article 4(11) and Article 7(4) GDPR

D2.2 – Legal and Ethical Requirements

	rely on a different legal basis, and might be thus subject to different limitations.
--	--

Note that there is an extra layer of complexity within the CyberSANE solution when it comes to establishing the adequate legal basis. When personal data relates to a **special category of personal data**, Article 9(1) GDPR states that the processing of such data is, in principle, prohibited. This principal prohibition can be explained by their sensitive character. However, Article 9(2) GDPR indicates that such processing may be considered lawful if it meets certain conditions which are exhaustively listed. In addition to the general principles of data protection, sensitive data must, thus, adhere to a particular regime. In other words, it is not sufficient to rely on one of the legal bases enumerated in Article 6 GDPR when sensitive personal data are being processed, but one of the grounds listed in Article 9(2) should also cumulatively apply. Here, the grounds under Article 9(2) that are relevant for the CyberSANE system are presented:

- | |
|--|
| <ul style="list-style-type: none">(a) the data subject has given <u>explicit consent</u> to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;(b) [...](c) [...](d) [...](e) processing relates to personal data which are <u>manifestly made public by the data subject</u>;(f) [...](g) processing is necessary for reasons of <u>substantial public interest</u>, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;(h) [...](i) processing is necessary for reasons of <u>public interest in the area of public health</u>, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;(j) [...] |
|--|

In the specific case of CyberSANE, being a system aimed at identifying situations that can become a threat for the CIs, one pathway that can be considered to not be hindered by the prohibition principle, is by relying on Article 9(2)(g) GDPR. This provision describes the necessity to process sensitive data for reasons of **substantial public interest on the basis of Union or Member State law**. To protect the information system of critical infrastructures against cyber-attacks can indeed be argued to be a reason of substantial public interest according to the NIS Directive. It is not sufficient for the data controller to refer to the existence of NIS Directive. They will additionally need to (i) demonstrate the necessity of such processing to guarantee the security of his or her information system, (ii) assure the proportionality of the processing of data, (iii) respect the essence of the right to data protection and (iv) safeguard the fundamental rights and interests of the data subject. Note that 'legitimate interests' do not appear in the legitimisation ground described by Article 9(2) GDPR. The securing of CIs can thus still be a ground on which end-users can rely on through their legal obligations, yet they cannot merely invoke their legitimate interest at protection their information systems in case they process sensitive data, even unintentionally.

D2.2 – Legal and Ethical Requirements

Another possible ground to process sensitive personal data can be found in the **explicit consent** in the case of patient or health management. When wanting to make use of services that offer remote monitoring and emergency treatment in real-time, the processing of sensitive data is inevitable and the CyberSANE end-users can rely on Article 9(2)(a) GDPR. Note that the threshold for explicit consent is higher than for consent of Article 6(1)(a) GDPR. Where such explicit consent is required, a ‘statement or clear affirmative action’ is not sufficient. The question then raises what extra efforts a controller should undertake. The WP29 indicates that the term ‘explicit’ refers to the way consent is expressed by the data subject.⁴⁰ One way the end-users could meet this requirement, is by asking the data subjects for a written statement, a filing in an electronic form, the sending of an email, or perhaps by using an electronic signature.

The reference to ‘**personal data manifestly made public**’ as a legal ground for the processing of sensitive data raises questions for its potential relevance to web crawling. This reference may seem to imply that the larger set of personal data manifestly made public, for example in the context of social networks openly accessible, are exempted from the requirements of a legal ground for processing under the GDPR and that the sensitive data found within may be processed insofar as they have been manifestly made public by the data subject.⁴¹ The public nature of such data does not exempt the controller from the obligation of securing a legitimate basis for the processing in the first place.⁴² It should be noted that while data may have been manifestly made public to a social network by one individual, they may include information on third parties, other individuals, who may or may not be users of the said social network and for whom this legal ground does not apply, since it is not the latter who have manifestly made public the information relating to them. To assess whether data have been manifestly made public by the individual, their reasonable expectations of privacy should be assessed. Article 29 Working Party has made clear that insofar as a user does *not actively take notice and is in fact aware of the fact that her or his data are available to competent authorities* in the sense of Directive (EU) 2016/680 (see section 3.3) the processing of said data is not allowed.⁴³

CASE	REQUIREMENT
The CyberSANE system processes biometric data, patient data or other sensitive data	CyberSANE developers need to consider technical means in which the controller/end-user will be restricted in using CyberSANE only within the boundaries of a certain purpose and legal basis

⁴⁰ Article 29 Data Protection Working Party, ‘Guidelines on consent under Regulation 2016/679’, 10 April 2018, p.18.

⁴¹ L. Edwards, L. Urquhart, *Privacy in public spaces: what expectations of privacy do we have in social media intelligence?*, International Journal of Law and Information Technology, 2016, 24, p. 293.

⁴² B. Van Alsenoy, *SPION D6.1 - Legal requirements for privacy friendly model privacy policies*, Report – Conference Level Paper, 30.06.2012, Article 29 Data Protection Working Party, *Opinion 5/2009 on online social networking*, 01189/09/EN, WP 163, 12 June 2009.

⁴³ Article 29 Data Protection Working Party, *Opinion on some key issues of the Law Enforcement Directive (EU 2016/680)*.

3.1.2.2 Data Protection Officer and Data Protection Impact Assessment

3.1.2.2.1 Data Protection Officer

In some situations, the data controller must designate a data protection officer (DPO) in order to comply with the GDPR. This is the case where the core activities of the controller consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale. It is rather easy to state that this will most likely be the case for the CyberSANE system.

The DPO should be an expert on data protection law and practices and be in a position to operate independently within the organisation. Their main tasks as described by Article 39 GDPR include to inform the data controller on their obligations and provide assistance in complying with the GDPR obligations. The DPO must assist the data controller in its task to ensure the correct application of the GDPR and that the rights and freedoms of the data subjects are not likely to be adversely affected by the processing operations. The DPO must have sufficient access to the CyberSANE system and must be able to evaluate whether the processing activities are in conformity with the GDPR:

CASE	REQUIREMENT
The CyberSANE system performs processing activities which require the presence of a DPO	CyberSANE must allow proper and easily understandable access to the DPO

3.1.2.2.2 Data Protection Impact Assessment

A data protection impact assessment (DPIA) is a process described in Article 35 GDPR aimed to evaluate risks to the rights and freedoms of individuals, in particular the risks' origin, nature, particularity and severity. In accordance with Article 35 GDPR, 'where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a **high risk to the rights and freedoms** of natural persons, the controller shall, prior to the processing, carry out an **assessment of the impact of the envisaged processing operations on the protection of personal data**. A single assessment shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment. A DPIA must be performed in the cases below:

- (a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
- (b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or
- (c) a systematic monitoring of a publicly accessible area on a large scale.

Data controllers need to undertake a data protection impact assessment (DPIA) whenever processing results in a high risk to the rights and freedoms of data subjects, which applies to the CyberSANE due to the processing of personal data at a very large scale via data crawling and

D2.2 – Legal and Ethical Requirements

mining techniques.⁴⁴ This DPIA must be conducted prior to the processing and is necessary to evaluate the origin, nature, particularity and severity of the risk. On the basis of this DPIA, the data controller should be able to determine the appropriate measures to be taken to demonstrate that he complies with the GDPR. In the scenario where the adoption of adequate technical or organizational measures is not possible, the data controller needs to consult the national data protection authority prior to the processing.

CASE	REQUIREMENT
CyberSANE processing activities result in high risk for the rights and freedoms of individuals	CyberSANE must be designed in a way that allows the continuous evaluation of the system and implementation of measures for the protection of the personal data

3.1.2.3 Data security and breach of personal data

A personal data breach occurs whenever there is a breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. Whenever such a data security breach happens, the GDPR prescribes that this must be brought to the attention of the competent national supervisory authority within a delay of 72 hours, or, if this would be unfeasible, without undue delay after the controller became aware of the breach and accompanied by the reasons for this delay.

If the data breach is unlikely to result in a risk to the rights and freedoms of natural persons, the controller may choose not to notify the supervisory authority. If the contrary is true, and, the personal data breach is likely to result in a high risk to the rights and freedoms of the data subjects involved, the data controller should notify the individuals concerned too, in addition to notifying the supervisory authority.⁴⁵

CASE	REQUIREMENT
There is a breach of personal data to the CyberSANE system	CyberSANE must implement techniques for notifications to the DPA and/or the data subject within the strict time limits

3.1.2.4 Accountability, liability and overall responsibility

The data controller is the norm addressee of the GDPR and, in addition to being responsible for compliance with the GDPR, the data controller must, at all times, be able to demonstrate compliance. This is referred to as the accountability principle.⁴⁶ Article 24 GDPR describes the general responsibility of the data controller:

⁴⁴ Article 35 GDPR

⁴⁵ Article 34 GDPR.

⁴⁶ Article 5(2) GDPR.

1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation.

It should be noted that even if the controller is assisted by a DPO, the controller is the sole responsible of the processing. To help ensure accountability in the processing of personal data, CyberSANE end-users will have to maintain records of the processing activities carried out under their responsibility and be ready to grant access to supervisory authorities whenever so requested (Article 30 GDPR)

Whenever an end-user fails to fulfil his or her obligations as a data controller, his or her liability is at stake and administrative fines may be imposed by the Data Protection Authorities based on Article 83 GDPR:

1. Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 in each individual case be effective, proportionate and dissuasive.

2. [...]

3. [...]

4. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(a) the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43;

(b) the obligations of the certification body pursuant to Articles 42 and 43;

(c) the obligation of the monitoring body pursuant to Article 41(4).

5. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;

(b) the data subjects' rights pursuant to Articles 12 to 22;

(c) the transfer of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49;

(d) any obligations pursuant to Member State law adopted under Chapter IX;

(e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1).

3.1.3 Data subject's rights

The data subjects are entitled to a few specific rights vis-à-vis the data controller, listed below:

Data subject rights	Relevant provisions in the GDPR
Right to information and access	Articles 12, 13 and 14
Right of access	Article 15
Right to rectification	Article 16
Right to erasure ('right to be forgotten')	Article 17
Right to restriction of processing	Article 18
Right to data portability	Article 20
Right to object	Article 21
Right not to be subject to automated decision making	Article 22

Conversely, they reflect in corresponding responsibilities and obligations of data controllers (or the data processor on the behalf of the controller). In light of this, one of the practical consequences of the catalogue of data subject rights is that the controller has to be organisationally prepared for them, for example by providing the contact point, portal or access to information and data subject requests. In line with the DPbD approach, CyberSANE developers should design the solution in a way that allows for responding to these data subject requests.

If data subject thinks his or her data has been processed unlawfully or has any other complaints or requests, he or she can send a request to the data controller and ask for the data to be accessed, corrected, erased or blocked or demand that the data controller notify third parties who have already received or seen the data. If the data subject does not receive an (adequate) answer or handling by the controller, it can file a complaint to the national supervisory data protection authority.

CASE	REQUIREMENT
Data subjects file in a request to exercise their rights	The CyberSANE system must be prepared to abide by the request, and provide proper information and/or access regarding the processing activities, rectify or delete data, or block the processing

3.1.3.1 Automated decision-making

In view of the large potential for automated decision-making processing activities in CyberSANE, particular focus will be allocated to it.

The risks that accompany automation have been one of the key drivers behind the development of European data protection generally.⁴⁷ Data subjects have been granted a right to obtain human intervention in **automated decision-making, including profiling, resulting in adverse legal effects or similarly significant effect**. Therefore, in principle, there is a **general prohibition** of automated decision making, unless one the following conditions apply.⁴⁸ Automated processing

⁴⁷ See Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Ets No 108) and Recommendation CM/Rec(2010)13, 16.

⁴⁸ Idem.

D2.2 – Legal and Ethical Requirements

can be used **exceptionally** (1) where the decision is **necessary for the entry into or the performance of a contract**, (2) when it is **authorised by EU or Member State** law applicable to the controller or (3) when it is based on the individual's **explicit consent**. However, **appropriate measures to protect the individual's interests** must still be in place.

This right aims at striking a balance between human and machine judgment. However, it is to be noted that Article 22 GDPR confers upon data subjects such a right to not be subject to automated processing producing significant effects only where the decision is based *solely* on automated processing. This raises the question of *when* a human operator must exert judgement or influence over an automated process. For instance, the first stage of profiling, i.e. the collection and warehousing of datasets, can be entirely manual, and the profiling could still fall under the GDPR if subsequent operations are automated. This means, for example, that it is not sufficient that a human operator merely enters keywords into a system like CyberSANE to exert influence over the retrieval of information. As long as the human operator does not intervene to control the profile construction as well as the final re-application of group profiles to individuals, the operations would still be classified as profiling in the meaning of the GDPR.

(4) 'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.

Profiling is undertaken to evaluate, analyse and predict certain personal characteristics and entails the creation or use of profiles on data subjects. However, it is unclear whether this has to be intentional to meet the threshold of profiling. Recital 71 GDPR indicates that data subjects should have the right not to be subject to a decision which may include a measure evaluating personal aspects to him or her which is based solely on automated processing and which produces effects concerning him or her in a similarly significant way as a legal effect. However, Recital 71 also states that profiling should be allowed where expressly authorized by Union or Member State law to which the data controller is subject. Important here are three elements.

- (i) First, Article 21 GDPR provides that a data subject has the right not to be subject to profiling based solely on automated processing. As a remedy hereto, any profiling generated from the CyberSANE system should be accompanied by non-fully automated cross-checks.
- (ii) Second, Article 20 GDPR provides that the individual concerned has the right to object against profiling if the processing activity at hand is based on the legal ground of legitimate interests. Thus, if the data-controller chooses to rely on his or her legitimate interests rather than on a legal obligation to protect the security of information systems, he or she can only use profiling techniques if he or she can demonstrate that the interest of securing his network overrides the interests, rights and freedoms of the individuals concerned.
- (iii) Third, Recital 71 GDPR indicates that profiling measures should not concern children. No children should ever be involved at any stage, including during field testing.

Big data do not necessarily imply the processing of personal information only. WP29 indicated that *"the retention and analysis of huge amounts of personal data in big data environments require*

D2.2 – Legal and Ethical Requirements

*particular attention and care. Patterns relating to specific individuals may be identified, also by means of the increased availability of computer processing power and data mining capabilities.*⁴⁹

Such mining capabilities can easily be linked with the CyberSANE solution, for instance where the DarkNet component detects and analyses online user-generated content derived from social media, the dark and deep web through machine learning technologies. Although it is often presumed that all information posted on social networks is public information, processing of said information can constitute an intrusion into someone's private life. Individuals posting personal information may still have a legitimate expectation of privacy. This legitimate expectation might be infringed by collection and storage of individual's personal data.

Contemporary profiling of online data frequently relies on Big Data to draw correlations and patterns regarding data subjects. This is also the case in CyberSANE, using social media heterogeneous online sources to profile potential hackers. The processing of Big Data raises concerns for the principles of data minimization, necessity and proportionality.

In any attempt of profiling there is a risk of discrimination, and this is also the case with regard to algorithmic profiling. This is because profiling algorithms identify correlations and make predictions about behaviour at a group-level, then the individual is categorised based on connections with others identified by the algorithm, rather than actual behaviour. Profiling can inadvertently create an evidence base that leads to discrimination.⁵⁰ Discrimination can arise inadvertently in algorithmic systems, such as profiling technology. The primary cause for possible discrimination is that 'data mining algorithms may "learn" to discriminate on the basis of biased data used to train the algorithm.' Moreover, 'discriminatory analytics can contribute to self-fulfilling prophecies and stigmatisation in targeted groups, undermining their autonomy and participation in society.'

Transparency is a key pillar in data protection law.⁵¹ Personal data needs to be processed lawfully, fairly and in a transparent manner in relation to the data subject. Article 13(2)(f) and 14(1)(h) GDPR both provide that data subjects shall have the right to obtain information on the existence of automated decision-making, including profiling, and meaningful information about the logic involved. In addition, these two provisions confer upon data subjects the right to obtain information of the significance and the envisaged consequences of such processing.

One way in which the CyberSANE system might result in automated decision-making is by entering personal data in a register of suspicious internet users which may have a negative impact on internet users. This may block access to services or even trigger further investigative measures against the data subject. Moreover, it should be noted that the definition of profiling does not presume that decisions are taken with respect to the data subject. Evaluation and prediction of behaviours could potentially give rise of adverse legal effects or significant effects. Moreover, in his report Jan Albrecht suggested that the effects "for the rights and freedoms" of the data subject were of particular interest to profiling and that for any effects to be *significant*, they should be "comparable in intensity to legal effects."

In order for automated decision-making to take place within the context of the CyberSANE solution, nonetheless, one of the conditions foreseen in the GDPR should apply. It is not likely that

⁴⁹ Article 29 Data Protection Working Party (2014) *Statement on Statement of the WP29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU* (14/EN WP 221), Adopted on 16 September 2014)

⁵⁰ de Vries K (2010) Identity, profiling algorithms and a world of ambient intelligence. *Ethics and Information Technology* 12(1): 71– 85

⁵¹ Article 5(1)(a) GDPR

D2.2 – Legal and Ethical Requirements

the data subject will have given an explicit consent for such processing. Therefore, the end-user should examine to what extent automated decision-making may be allowed on the basis of EU or national law or is necessary for the provision of services and/or conclusion of the contract with the end-user clients for instance.

CASE	REQUIREMENT
The CyberSANE system allows for automated decision making	<p>The CyberSANE system should include checks and balances, by keeping a human in the loop</p> <p>The CyberSANE user must ensure that one of the three exhaustively enumerated conditions under which automated decision-making is allowed, applies</p>

3.2 E-Privacy Directive

The e-Privacy Directive 2002/58/EC regulates the use of electronic communication services. A revision of this instrument was announced and the new e-privacy Regulation was intended to apply from 25 May 2018 together with the GDPR. However, due to a lack of political compromise, there is, to date, still no replacement of the e-Privacy Directive.

This uncertainty could potentially play an important factor in case of the application of the CyberSANE solution within Telecom industry. In that case, additional requirements may have to be met and end-users should take into account the uncertainty regarding the adoption of new e-privacy regulation.

3.3 Directive (EU) 2016/680

Directive (EU) 2016/680 ('DPLED') on 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 accompanies and complements the GDPR.⁵² It entered into force on 5 May 2016 and was due to be transposed by the Member States by 6 May 2018.⁵³ Currently, only Spain has failed to meet to transpose the DPLED. While the GDPR regulates the processing of personal data in a general context, the processing of personal data within the sector of law enforcement and criminal justice has been considered to require a separate legal instrument, due to the special nature of security-related data and activities.⁵⁴ It should be noted that the relation between these two legal

⁵² Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on 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, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, p. 89–131.

⁵³ Art. 63-64 Directive (EU) 2016/680.

⁵⁴ P. De Hert and V. Papakonstantinou, The Police and Criminal Justice Data Protection Directive: Comment and Analysis, *Computers & Law Magazine of SCL*, Vol. 22 Issue 6, 2012, p. 1-2.

D2.2 – Legal and Ethical Requirements

instruments, i.e. the GDPR and the DPLED, is exclusionary, in the sense that, depending on the purpose and context of the processing of personal data, either one or the other will apply.⁵⁵

The DPLED applies 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, including the safeguarding against and the prevention of threats to public security.**⁵⁶ A competent authority is further defined as either any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security or any other body or entity entrusted by Member State law to exercise public authority and public powers for the same abovementioned purposes.⁵⁷ A competent authority is considered as data controller when alone or jointly with others, it determines the purposes and means of the processing of personal data. In addition, a processor may be a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. Processing on behalf of competent authorities should be governed by contract or legal obligation.⁵⁸

Insofar as CyberSANE is concerned, it is considered that end-users will most likely not fall under the definition of competent authority, which however further depends on the national transposition of the DPLED in each Member States. CyberSANE end-users, however, might be considered as processors. More specifically, when dealing with criminal and evidentiary data, the issue of the applicability of the DPLED on entities outside law enforcement and judicial evidence is raised. Given the nature of the issue, it will be further addressed in Chapter 6 Evidence Handling.

In the case where CyberSANE end-users are subject to the DPLED, however, as controller or more likely as processor, the regime, principles and definitions of the DPLED, which are similar to the GDPR, should be followed. It should be noted, nevertheless, that the DPLED rules are more lenient than the GDPR. For instance, the legal basis for processing personal data is much broader⁵⁹, and there is no direct prohibition on the processing of special categories of data⁶⁰. Moreover, the DPLED introduces a few novelties, such as the obligation to distinguish between different categories of data, depending on the capacity of the individual in relation to a criminal case⁶¹, and depending on whether data are based on facts or personal assessments⁶². Storage of such data should be strictly and periodically reviewed⁶³, while specific logs of consultation and disclosure of the data in question should be kept⁶⁴.

CASE	REQUIREMENT
------	-------------

⁵⁵ Recital 19 Regulation (EU) 2016/679, Recital 12 Directive (EU) 2016/680.

⁵⁶ Art. 1(1) Directive (EU) 2016/680.

⁵⁷ Art. 3(7) Directive (EU) 2016/680.

⁵⁸ Art. 22 Directive (EU) 2016/680.

⁵⁹ Art. 8 Directive (EU) 2016/680.

⁶⁰ Art. 10 Directive (EU) 2016/680.

⁶¹ Art. 6 Directive (EU) 2016/680.

⁶² Art. 7 Directive (EU) 2016/680.

⁶³ Art. 5 Directive (EU) 2016/680.

⁶⁴ Art. 25 Directive (EU) 2016/680.

The CyberSANE end-user might be subject to the DPLED	CyberSANE must allow for compliance with the DPLED-specific obligations, such as the distinction of data and separate storage rules
--	---

3.4 Regulation on the free flow of non-personal data

3.4.1 The Regulation

There is a plethora of national laws across the EU imposing technical and legal barriers to the free movement of non-personal data. **Non-personal data** consist of data not relating to an identifiable natural person such as environmental, industrial or machine generated data. Data localisation restrictions derive from administrative rules or practices which provide the obligation that certain categories of data or datasets must be collected, processed and/or stored within a specifically defined geographical area. In other words, Member States often prefer that data are processed within their own territory.

Such restrictions have been identified by the European Commission (EC) as obstacles hampering the free flow of non-personal data within the EU, and the competitive data economy within the Digital Single Market overall. Data localisation restrictions have become financially and practically cumbersome for businesses as well as public and governmental entities in hold of data, subject to these restrictions.⁶⁵ According to the EC's report, data localisation restrictions are particularly problematic for cloud computing services, as the providers often employ data centres spread in many different states, while outsourced data are constantly transferred amongst these data centres. Entities bound by such restrictions are deterred from using cloud computing services. To mediate these issues, the EC proposed in 2017 a legal instrument aiming to abolish data localisation restrictions imposed on a national level. The Regulation on the Free Flow of Non-Personal Data ('Regulation 2018/1807') became applicable as of 28 May 2019.⁶⁶

The Regulation 2018/1807 applies to electronic data that are not personal, and thus not subject to the GDPR⁶⁷, and it seeks to enhance their free movement within the EU, namely by abolishing national data localisation requirements on non-personal data stored by a natural or a legal person in the EU⁶⁸. Exceptions are provided for Member States when they invoke reasons of public security.⁶⁹ Moreover, the Regulation 2018/1807 seeks to implement the principle of data availability for regulatory control.⁷⁰ In other words, competent authorities will be facilitated in exercising their rights of access to the non-personal data stored or processed in the EU. In that respect, the Regulation 2018/1807 provides the possibility for Member States to '*impose effective,*

⁶⁵ European Commission, EC Communication, *Building a European Data Economy*, COM(2017) 9, 10.01.2017, available at <https://ec.europa.eu/digital-single-market/en/news/communication-building-european-data-economy>; EC Staff Working Document on the free flow of data and emerging issues of the European data economy Accompanying the document Communication Building a European data economy, 10.1.2017 SWD(2017) 2 final, available at <https://ec.europa.eu/digital-single-market/en/news/staff-working-document-free-flow-data-and-emerging-issues-european-data-economy>

⁶⁶ Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, OJ L 303, 28.11.2018, p. 59–68.

⁶⁷ Art. 3(1) Regulation (EU) 2018/1807.

⁶⁸ Art. 4 Regulation (EU) 2018/1807.

⁶⁹ *ibid.*

⁷⁰ Art. 5 Regulation (EU) 2018/1807.

proportionate and dissuasive penalties for failure to comply with an obligation to provide data, in accordance with Union and national law.⁷¹

Furthermore, self-regulatory solutions via the development of **codes of conduct** are encouraged for the facilitation of data portability and switching of providers, as for example cloud service providers. More specifically, the codes of conduct in question should be *'based on the principles of transparency and interoperability and taking due account of open standards, covering, inter alia, the following aspects:*

- (a) Best practices for facilitating the switching of service providers and the porting of data in a structured, commonly used and machine-readable format including open standard formats where required or requested by the service provider receiving the data;*
- (b) Minimum information requirements to ensure that professional users are provided, before a contract for data processing is concluded, with sufficiently detailed, clear and transparent information regarding the processes, technical requirements, timeframes and charges that apply in case a professional user wants to switch to another service provider or port data back to its own IT systems;*
- (c) Approaches to certification schemes that facilitate the comparison of data processing products and services for professional users, taking into account established national or international norms, to facilitate the comparability of those products and services. Such approaches may include, inter alia, quality management, information security management, business continuity management and environmental management;*
- (d) Communication roadmaps taking a multi-disciplinary approach to raise awareness of the codes of conduct among relevant stakeholders.*⁷²

It is finally affirmed that any (cyber)security requirements already applicable to storing and processing data will continue to apply when they store or process data across borders in the EU or in the cloud.⁷³

3.4.2 Mixed datasets

In reality most **datasets are mixed, comprising of both personal and non-personal data**, the applicability of rules becomes less clear. The EC published a guidance on the applicable framework for mixed datasets and on the interaction between the Regulation 2018/1807 and the GDPR.⁷⁴ The Guidance aims to clarify the scope of the two legal instruments by juxtaposing personal and non-personal data. The latter, according to the Guidance, may be categorised by origin as data initially and by nature non-personal, for instance machine generated data, and as data rendered non-personal, through techniques such as anonymization. It should be noted that numerous studies contest the efficiency of anonymization techniques and the extent in which anonymized data should be considered as non-personal, since the continuous rapid evolvement of technology more than often allows for their re-identification. It is therefore recommended that a

⁷¹ *ibid.*

⁷² Art. 6 Regulation (EU) 2018/1807.

⁷³ Rec 33-34 Regulation (EU) 2018/1807.

⁷⁴ European Commission, Communication, Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union, COM(2019) 250, 29.05.2019, available at: <https://ec.europa.eu/digital-single-market/en/news/practical-guidance-businesses-how-process-mixed-datasets>

D2.2 – Legal and Ethical Requirements

great deal of attention is paid on datasets that are anonymized.⁷⁵ Anonymized datasets should not be considered as non-personal data, or in any case should be subject to enhanced security measures and revision controls, protecting them from the risk of re-identification.

In accordance with the above, it may already be challenging to identify whether a dataset consists of personal data, of non-personal data, or is mixed. The Guidance provides for the following examples of mixed datasets⁷⁶:

- *A company’s tax record, mentioning the name and telephone number of the managing director of the company*
- *Datasets in a bank, particularly those with client information and transaction details, such as payment services (credit and debit cards), partner relationship management (PRM) applications and loan agreements, documents mixing data concerning natural and legal persons*
- *Research institution’s anonymised statistical data and the raw data initially collected, such as the replies of individual respondents to statistical survey questions*
- *Company’s knowledge database of IT problems and their solutions based on individual IT incident reports*
- *Data related to the Internet of Things, where some of the data allow assumptions to be made about identifiable individuals (e.g. presence at a particular address and usage patterns)*
- *Analysis of operational log data of manufacturing equipment in the manufacturing industry.*

According to Regulation 2018/1807, the latter should apply only to the non-personal data of a mixed dataset while the GDPR continues to apply to the personal data of the mixed dataset.⁷⁷ **If, however, the non-personal data part and the personal data parts are ‘inextricably linked’, ‘the data protection rights and obligations stemming from the GDPR fully apply to the whole mixed dataset, also when personal data represent only a small part of the dataset’.**⁷⁸ The condition where data parts are inextricably linked within the meaning of the above, may refer to a situation whereby a dataset contains personal data as well as non-personal data and separating the two would either be impossible or considered by the controller to be economically inefficient or not technically feasible.⁷⁹ As the Guidance further points out, *‘neither of the two Regulations obliges businesses to separate the datasets they are controlling or processing. Consequently, a mixed dataset will generally be subject to the obligations of data controllers and processors and respect the rights of data subjects established by the GDPR.’*

⁷⁵ See for example Finck, Michèle, and Frank Pallas. “They Who Must Not Be Identified - Distinguishing Personal from Non-Personal Data Under the GDPR.” SSRN Electronic Journal, 2019. Rocher, Luc, Julien M. Hendrickx, and Yves-Alexandre de Montjoye. “Estimating the Success of Re-Identifications in Incomplete Datasets Using Generative Models.” *Nature Communications* 10, no. 1 (December 2019): 3069.

⁷⁶ European Commission, Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union.

⁷⁷ Art 2(2) Regulation 2018/1807.

⁷⁸ European Commission, Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union.

⁷⁹ *ibid.*

D2.2 – Legal and Ethical Requirements

In regard to non-personal data portability, the Guidance clarifies that it differs from the right to data portability as established in the GDPR. In practice, data portability within the meaning of Regulation 2018/1807 concerns business-to-business interactions between a professional user and a service provider. More specifically, it *'targets a situation where a professional user has outsourced the processing of its data to a third party offering a data processing service'*.⁸⁰ To the extent that the CyberSANE solution could be exploited as a cloud computing service, the requirement of allowing an end-user to easily switch providers should be taken into account, as explained above.

CASE	REQUIREMENT
The CyberSANE system consists of a cloud computing service	CyberSANE must allow for data portability
The CyberSANE system processes non-personal data	CyberSANE must allow for controls by regulatory authorities and must have strong security measures in place
The CyberSANE system processes mixed datasets	CyberSANE must make clear to what extent the non-personal data and the personal data parts are inextricably linked. If not, CyberSANE must allow for separate privacy and confidentiality policies to apply for the non-personal and the personal data

⁸⁰ *ibid.*

4 The EU legal framework on cybersecurity

This chapter provides an overview of the EU legal framework on cybersecurity, focusing on the most significant initiatives within the EU cybersecurity strategy: the NIS Directive (including in its interconnection with the GDPR) and the Cybersecurity Act.

4.1 Scope and objectives

Digital technologies have become the cornerstone of all the most critical sectors of our economy, which rely on the continuous availability and performance of Information Communication Technologies (ICT) resources. Cybersecurity incidents - independently from their origin (criminal or terrorist activity, natural disasters or involuntary mistake) - have the potential to hugely impact our societies and economy, particularly when affecting the provision of essential services.

Against this background, the security of network and information systems has become a key objective of the EU, which, in the last decade, has significantly intensified its efforts to promote cyber-resilience at the EU level.

In 2013, the EC launched the EU Cybersecurity Strategy "An Open, Safe and Secure Cyberspace"⁸¹, which includes the only comprehensive definition of cyber-security at EU level⁸² as the *"safeguard, and the actions that can be used to protect the cyber-domain, both in the civilian and military fields, from those threats that are associated with or that, may harm its interdependent networks and information infrastructure"*. The 2013 Strategy was accompanied by a Proposal for a Directive on the Security of Network and Information Systems (the "NIS Directive"); this Directive (which is discussed in the following paragraph) was finally approved in July 2016 and entered into force in August 2016.

In September 2017, the EC adopted a Cybersecurity Package, which encompassed a wide range of measures to enhance cybersecurity, including a proposal for a EU Cybersecurity agency and a EU-wide certification scheme. Such measures and innovations are envisaged in the so-called "Cybersecurity Act", adopted in 2019 and illustrated under par. 4.3.

4.2 The NIS Directive

4.2.1. Overview and key definitions

The NIS Directive⁸³ is the first piece of EU legislation on cybersecurity and represents the main output of the "2013 EU Security Strategy". It introduces a set of legal measures aimed at *"achieving*

⁸¹ European Commission, High Representative of the EU for Foreign Affairs and Security policy, Joint Communication, *Cybersecurity Strategy of the European Union: an Open, Safe and Secure Cyberspace*, Brussels, 7.2.2013, JOIN (2013).

⁸² Alessandro Bruni, Promoting Coherence in the EU Cybersecurity Strategy, in Anton Vedder, Jessica Schroers, Charlotte Ducuing and Peggy Valcke (eds.), *Security and Law, Legal and Ethical Aspects of public Security, Cyber Security and Critical Infrastructure Security*, Intersentia, 2019.

⁸³ Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union ("NIS Directive"), OJ L 194, 19.7.2016.

a high common level of security of network and information systems within the Union so as to improve the functioning of the internal market".⁸⁴ In particular, the NIS Directive aims at:⁸⁵

- Obliging the Member States to adopt a *national strategy* on the security of networks and information systems
- Creating a *Cooperation Group* and a *security incident response team network* (“CSIRT” network) to facilitate trust, collaboration and information exchange among Member States
- Introducing *security and notification obligations* for operators of essential services (hereinafter also referred as “OES”) and *digital service providers* (hereinafter also referred as “DSP”)
- Imposing obligations on the Member States regarding the appointment of national authorities, single point of contact and CSIRTs.

The goal of the NIS Directive is to introduce a minimum harmonisation in the area of NIS security, allowing for stricter rules to be adopted at the national level. Its provisions should have been transposed by the Member States by 9 May 2018 (with six additional months for the identification of the OES).

The obligations of the NIS Directive are addressed at two categories of entities, for which the NIS Directive establishes a different regime: the operators of essential services and the digital service providers. The CyberSANE system is primarily addressed to CI which are likely to be identified by the Member States as operators of essential services or digital service providers, subject to the obligations of the NIS Directive. CyberSANE itself might be considered a digital service. It is therefore convenient to present the main definitions of the NIS directive before illustrating the key obligations posed by the Directive, which are discussed in the next paragraph.

A **network and information system** is defined as follows by the NIS Directive:

- a) *Electronic communications network within the meaning of point (a) of Article 2 of Directive 2002/21/EC*⁸⁶
- b) *Any device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data*
- c) *Digital data stored, processed, retrieved or transmitted by elements covered under points (a) and (b) for the purposes of their operation, use, protection and maintenance.*⁸⁷

Another key definition of the NIS Directive is that of **security of network and information systems**, which is understood as *“the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or*

⁸⁴ Art. 1 NIS Directive.

⁸⁵ Ibidem.

⁸⁶ Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive), OJ L 108, 24.4.2002, p. 33–50, according to article 2 (a): *electronic communications network means transmission systems and, where applicable, switching or routing equipment and other resources which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed.*

⁸⁷ Article 4 (1) NIS Directive. It can be noted that the letter b) and c) correspond to the definition of the term information system as set out in the aforementioned Directive 2013/40/EU

D2.2 – Legal and Ethical Requirements

*confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems”.*⁸⁸

Operators of essential services (OES) are defined by the NIS Directive as public or private entities active in the sector listed under Annex II (such as energy, transport, banking, financial market infrastructure, health) which also fulfil the criteria set out by art. 5(2) Directive:

- a) *An entity provides a service which is essential for the maintenance of **critical societal and/or economic activities***
- b) *The provision of that service **depends on network and information systems***
- c) *An incident would have **significant disruptive effects** on the provision of that service.*⁸⁹

Member States had to identify by 9 November 2018 the operators of essential services established on their territory for each of the sectors and subsectors in Annex II.⁹⁰

What constitutes a ‘**significant disruptive effect**’ will also be determined on a national level, taking into account the criteria listed under art. 6:

- Number of users relying on the service
- Dependency of other essential services on the service
- Possible impact of incidents in degree and duration on economic and societal activities or public safety
- Market share of the entity
- Area that could be affected by an incident
- Importance of the entity for maintaining a sufficient level of the essential service, taking into account the availability of alternative means for the provision of that service.

Digital service providers (DSP) are defined as legal entities which provide a digital service, in particular in the context of an online marketplace, and online search engine, or a cloud computing service.⁹¹

4.2.2. NIS Directive’s obligations

4.2.2.1 National frameworks on the security of network and information systems

Member States must adopt a **national strategy** and designate **one or more national competent authorities** on the security of network and information systems, covering at least the sectors and the services listed under Annex II and III.⁹²

Member States are also required to appoint a **single point of contact** (this may coincide with the competent authority) which exercises a liaison function to ensure cross-border cooperation among authorities and one or more **Computer Security Incident Response Teams (CSIRTs)** that are responsible for risk and incident handling.⁹³ This national framework is relevant to the operators of essential services, as it defines their obligations.

⁸⁸ Article 4 (2) NIS Directive.

⁸⁹ Article 5(2) NIS Directive.

⁹⁰ Art. 5(1) NIS Directive.

⁹¹ Art. 4(5) and Annex III NIS Directive.

⁹² Art. 7 and 8 NIS Directive.

⁹³ Articles 8 and 9 NIS Directive.

4.2.2.2 Obligations for OES

All the entities that are identified as OES must comply with the security and notification requirements listed under art. 14 NIS Directive.

OES must adopt the **technical and organizational measures** which are appropriate to **manage the risks posed to the security of their network and information systems**⁹⁴. In order to guarantee the continuity of the services, such measures must be able to prevent and minimise the impact of incidents concerning the network and information systems on which the OES rely.⁹⁵

The Cooperation Group established under art. 11 of the NIS Directive - composed of representatives of the Member States, the Commission and the European Union Agency for Network and Information Security (ENISA) to facilitate strategic cooperation between the Member States on NIS-related matters - has published a series non-binding guidelines to support the Member States in the effective and coherent implementation of the NIS Directive across the EU. In this regard, the first publication of the Cooperation Group (01/2018) has addressed the adoption of appropriate measures by the OES.⁹⁶

Art. 14(3) and (4) of the NIS Directive further impose on the OES the obligation to **notify the incidents** having a **significant impact on the continuity of the essential services** to the competent authorities or the CSIRT without undue delay.⁹⁷ When assessing the significance of the impact of an accident, the OES should take into account the elements listed under art. 14(4):

- a) Number of users affected
- b) Duration of the incident
- c) Geographical spread of the area concerned by the incident.

The second report (02/2018) published by the Cooperation Group, “Reference Document on Incident Notification for Operators of Essential Services (Circumstances of Notification)”,⁹⁸ aims specifically at assisting the Member States in the transposition of art. 14 par. 3 and 4.

The Reference Document 02/2018 observes the following with regard to the parameters listed under art. 14 par. 4:

- **Number of the users affected** by the disruption of the essential service (art. 14 par. 4 lett. a): this parameter is understood as “the number of affected natural persons and legal entities with whom a contract for the provision of the services has been concluded”. The way of determining the number of users, however, affected may vary depending on the type of industry involved
- **Duration** of the incident (art. 14 par. 4 lett. b): it is the period of time during which the service is not properly available, starting from the first moment in which the provision of the service is affected up until the time of full recovery
- **Geographical spread** with regard to the area affected by the incident (art. 14 par. 4 lett. c): this indicator has to be adapted to the specifics of the sector affected. Especially in

⁹⁴ Art. 14(1) NIS Directive.

⁹⁵ Art. 14(2) NIS Directive.

⁹⁶ Cooperation Group, *Reference document on security measures to be adopted by Operators of Essential Services*, 01/2018, available at <https://ec.europa.eu/digital-single-market/en/nis-cooperation-group>

⁹⁷ Article 14 NIS Directive.

⁹⁸ Cooperation Group, *Reference Document on Incident Notification for Operators of Essential Services*, 02/2018, available at <https://ec.europa.eu/digital-single-market/en/nis-cooperation-group>

D2.2 – Legal and Ethical Requirements

certain sectors, such as Transport, Energy, Banking, a specific reporting procedure must be defined and implemented.

The Reference Document points out that the parameters to be taken into consideration for assessing the significance of an incident are not limited to the ones referred to under art. 14 par. 4, as further criteria - such as the additional ones listed under art. 6 - can be included in such assessment.

Therefore the OES, when accomplishing their reporting obligations, could take into consideration the following additional parameters:

- **Dependency of other OES sectors** on the service provided by the affected entity (art. 6, letter b): for instance, a fallout in energy may cause significant disruptions in a variety of other OES, such as transports, healthcare, emergency services and banking. Interdependencies among OES should be described during the identification process required by art. 5 par. 1 NIS Directive and reported during the notification process (in this regard, it is advisable that interdependent OES impose on each other notification obligations under their commercial contracts);
- Impact that incidents could have, in terms of degree and duration, on **economic and societal activities or public safety** (art. 6, letter c): this indicator can only be measured by governments, as it relates to the possible damages to the EU single market and to public safety (beyond the economic impact for OES);
- **Market shares** of that entity (art. 6, letter d): the market share of an entity can also be interpreted as an indicator that the entity at issue acts as EOS (in this regard, an indicator such as the number of users should be preferred to a unit of measure such as the revenues);
- Geographic spread with regard to the area that could be affected by an incident (art. 6, letter e): see comment under art. 14 par. 4 lett. c;
- Importance of the entity for **maintaining a sufficient level of the service**, taking into account the availability of **alternative means** for the provision of that service (art. 6, letter f): this indicator looks at the availability of alternative means for the provision of the service, which may come from outside or from inside the OES. When alternative means are available for the provision of the service, the incident might not reach the threshold of “significance”.

CASE	REQUIREMENT
A CyberSANE end-user qualifies as OES under the NIS Directive.	<p>The technical partners developing the CyberSANE system must consider that the end-users must adopt, as required under the NIS Directive, technical and organizational measures appropriate to manage the risks posed to the security of their network and information systems.</p> <p>The CyberSANE system must enable the prompt detection of an incident having a significant impact on the continuity of the</p>

	essential service, as the OES end-users are subject to a duty to notify such incident without undue delay.
--	--

4.2.2.3 Obligations for DSP

The NIS Directive does not require Member States to identify the digital service providers subject to NIS obligations. Therefore, contrary to OES, all DSP - which can be online market place providers, online search engine providers and cloud service providers - fall under the scope of application of the NIS Directive provisions.

As set out by art. 16(1) NIS Directive, DSP must implement the **technical and organizational measure** which are required under national law to **manage the risks posed to the security of network and information systems** and to prevent and minimize the impact of possible incidents. Such measures must be aligned with the state of the art and take into consideration the series of elements listed under art. 16, i.e.: security of systems and facilities; incident handling; business continuity and management; monitoring, auditing and testing; compliance with international standards.

Art. 16(3) NIS Directive require DSP to **notify, without undue delay, the competent authority or the CSIRT of any incident having a substantial impact on the provision of a service**. The elements that the competent authority or CSIRT will consider when assessing the substantial character of an incident are the ones listed under art. 16(4) NIS Directive:

- Number of users affected
- Duration of the incident
- Geographical spread
- Extent of the disruption of the service
- Extent of the incident’s impact on the economy and society.

The notification must also include reference to the **possible impact of the incident on the provision of an essential service**. This obligation can be relevant in the context of the adoption of CyberSANE, where the end user is a provider of essential services which relies on a third-party digital service provider.

Both the elements that need to be considered for the security measures, and the parameters to be taken into account for the evaluation of the significance of an incident are further specified in a Commission’s Implementing Regulation issued in January 2018.⁹⁹

CASE	REQUIREMENT
Where CyberSANE is to be offered as a cloud-based solution, the CyberSANE provider qualifies as DSP under the NIS Directive.	The development of CyberSANE must take into account the obligations to which a CyberSANE provider will be subject under the NIS Directive (art. 16), concerning security

⁹⁹ Commission implementing Regulation (EU) 2018/151, of 30 January 2018, laying down rules for the application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact.

	measures and notification requirements. The notification of an incident with substantial impact on the provision of a CyberSANE cloud service must refer to the possible impact on the provision of a service by an OES.
--	--

4.3 The interplay between NIS Directive and GDPR

While the provisions of the NIS Directive and the GDPR do not contain an explicit reference to each other, the two legal frameworks are undoubtedly inter-related on a number of levels.¹⁰⁰

In particular, to the extent that personal data are processed through network and information systems, the two legal frameworks will apply at the same time. As the obligations posed by the NIS directive and GDPR aim at different purposes, and compliance with these is posed under the scrutiny of different authorities, it seems advisable to address compliance with each of these sets of obligations separately.¹⁰¹ In practice, this translates in the need to list the adopted security measures in distinct documents and to assess these separately and through the lens of two different regulatory frameworks.¹⁰² According to the same rationale, a security incident which requires notification both under NIS and GDPR, should be addressed to the competent authority through both notification procedures.

Possible conflict between the NIS Directive and GDPR should be framed in the context of a *lex specialis/lex generalis* type of relationship, where the fundamental right to data protection prevails in principle over the interests pursued through cybersecurity initiatives. Possible conflicts between the GDPR, on the one hand, and the Member State law implementing the NIS, on the other hand, could arise where a certain type of processing operation, prohibited or subject to strict safeguards under GDPR, is allowed by national law in the context of its cybersecurity policy.¹⁰³

CASE	REQUIREMENT
The CyberSANE end-user is subject to the NIS Directive's obligations processes personal data.	GDPR and NIS Directive obligations apply cumulatively. Compliance with each of these legal frameworks, in any case, should be addressed separately (for instance by keeping two distinct lists of the measures taken under GDPR and the NIS Directive respectively).

4.4 The Cybersecurity Act

¹⁰⁰ Dimitra Markopoulou, Vagelis Papakonstantinou, Paul de Hert, *The EU Cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation*, Computer Law and Security Law Review 35 (2019).

¹⁰¹ Markopoulou, p. 10.

¹⁰² *ibidem*.

¹⁰³ Markopoulou, p. 11, "For example, a Member State could decide to permit personal data processing operations otherwise prohibited or strictly regulated under the GDPR as part of its cybersecurity strategy, e.g. profiling on the basis of special categories of data (IP addresses coming from regions with high concentrations of ethnic and religious populations) without the safeguards of article 22 of the GDPR. Or, an essential services provider could decide to store personal data for the purposes of cybersecurity for much longer than needed under the GDPR's principle of data minimization".

D2.2 – Legal and Ethical Requirements

In June 2019, the EU passed another important piece of legislation aimed at strengthening the security of the EU cyber-space: Regulation (EU) 2019/881 on ENISA (the European Union Agency for Network and Information Security) and on information and communications technology cybersecurity certification, also known as the “Cybersecurity Act”.¹⁰⁴

The Cybersecurity Act innovates in particular on two levels:¹⁰⁵

- a) Defines the objectives, tasks and organization (administrative and management structure) of the European Union Agency for Cybersecurity (ENISA), granting the Agency a permanent mandate and more resources
- b) Establishes a “European cybersecurity certification schemes for the purpose of ensuring an adequate level of cybersecurity for ICT products, ICT services and ICT processes in the Union”.

The first part of the Cybersecurity Act (art. 3 through 45) is dedicated to **redefining and expanding the role of ENISA**. The Act mandates ENISA to contribute to the development and implementation of the EU cybersecurity policy and legislation through a variety of actions, including by¹⁰⁶: providing its independent opinion; assisting Member States in the consistent implement of EU policy and law on cybersecurity, particularly with regard to the NIS directive; assisting Member States and EU institutions in the preservation of the integrity of the open internet; contributing to the work of the Cooperation Group provided for under art. 11 NIS Directive; supporting the development of EU policies in the field of electronic identity and trust services and the promotion of electronic communications security; preparing an annual report on the state of the implementation of the legal frameworks regarding incident notification.

Furthermore, the Cybersecurity Act granted ENISA a very significant role in a variety of key areas:

- Capacity-building towards Member States, EU institutions and the Cooperation Group (art. 6)
- Operational cooperation at the EU level, as detailed under art. 7
- Promotion of EU policy on cybersecurity certifications of ICT products, services and processes (art. 8)
- Knowledge and information (art. 9)
- Awareness-raising and education (art. 10)
- Research and innovation (art. 11)
- International cooperation (art. 12).

The second part of the Cybersecurity Act (art. 46 through 65) lays down a framework for the introduction of the first **EU-wide harmonized cybersecurity certification framework for ICT products, services and processes**. The certification scheme aims at attesting that the certain products, services and processes, which must be duly identified in the EU work rolling programme, comply with specific security requirements. The security objectives pursued by the certification scheme are, among others, the protection of the data stored, transmitted or otherwise processed, against accidental or unauthorised storage, processing, access, disclosure, destruction, loss or

¹⁰⁴ Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (“Cybersecurity Act”), *OJ L 151, 7.6.2019, p. 15–69*.

¹⁰⁵ Art. 1 Cybersecurity Act.

¹⁰⁶ Art. 5 Cybersecurity Act.

D2.2 – Legal and Ethical Requirements

alteration; the identification of vulnerabilities; the monitoring of the access, use and processing of data and functions.¹⁰⁷

Unless otherwise provided by EU or Member State law, the cybersecurity certification is voluntary. The first EU rolling programme will be published by 28 June 2020 and updated at least every three years.¹⁰⁸ In this regard, ENISA may be requested by the Commission to prepare a candidate scheme or to review an existing certification scheme in light of the rolling work programme.¹⁰⁹

An EU cybersecurity certification mechanism will include at least the elements detailed under art. 54: among others, subject matter and scope of the certification scheme; purpose of the scheme and of the operativity of selected standards (including international, European or national), evaluation methods and assurance levels; reference to the possibility of self-assess conformity; specific evaluation criteria; possible marks and labels and specific or additional requirements. Moreover, the manufacturer or provider of certified ICT products, services and processes must make available the supplementary information listed under art. 55 (guidance and recommendations; the period during which assistance is guaranteed; their contact information and reference to online repositories reporting publicly disclosed vulnerabilities).

The Cybersecurity Act mandates Member States to designate one or more national cybersecurity certification authorities, which - among other tasks - (i) will supervise and enforce the rules included in the EU cybersecurity certification schemes to monitor the compliance of ICT products, service and processes (and of their manufacturers and providers) with the requirements set out under such schemes, (ii) support the national accreditation bodies in monitoring the conformity assessment bodies and (iii) report annually their activities to ENISA and the ECCG established under art. 62 of the Act.

While the NIS Directive applies only to operators of essential services and digital service providers, the **Cybersecurity Act encourages all businesses to invest more in cybersecurity to raise the trust of consumers and industry players in the cyber-resilience of ICT solutions.**

In particular, each European scheme will attest that the certified products and services comply with specific requirements, specifying in particular the following:¹¹⁰

- a) Categories of products and services covered
- b) Cybersecurity requirements, in technical terms and/or referring to standards
- c) Type of evaluation (e.g. self-assessment or third-party evaluation)
- d) Intended level of assurance (e.g. basic, substantial and/or high) compared with the risk - in terms of the probability and impact of an incident - associated with the envisaged use of the product, service or process.

The cybersecurity certificate issued under an EU scheme will be valid in all EU Member States, fostering the growth of the digital economy and supporting customers in understand the security features of the product or service they are purchasing.¹¹¹

¹⁰⁷ Art. 51 Cybersecurity Act.

¹⁰⁸ Art. 47(2) Cybersecurity Act.

¹⁰⁹ Art. 48 Cybersecurity Act.

¹¹⁰ <https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework>

¹¹¹ Ibidem

D2.2 – Legal and Ethical Requirements

CASE	REQUIREMENT
A CyberSANE-related product, service or process will be offered on the market	The CyberSANE partners involved in the development of the product, service or process at issue, and in any case the entity that will manufacture or market those, must monitor the rules of the EU cybersecurity certification scheme that will be introduced, in order to ensure compliance with such rules and possibly achieve a certification.

5 Critical infrastructures in the EU

This section is aimed at providing a general overview of the EU legal framework concerning the protection of CIs, which is relevant to CyberSANE in light of its focus on the protection of critical infrastructures and critical information infrastructures.

5.1 The notion of Critical Infrastructures

Following an EC Communication of October 2004, concerning the protection of critical infrastructures in the fight against terrorism, in December 2008 the EU adopted Directive 2008/114/EC on the protection of **European Critical Infrastructures**.¹¹²

Directive 2008/114/EC is the most important piece of the European legislation concerning the physical protection of critical infrastructures in the EU. The primary goal of the Directive is the introduction of ‘a procedure for the **identification and designation of European Critical Infrastructures (ECI)** and a common approach to the assessment of the need to improve the protection of such infrastructures’¹¹³.

The Directive provides for two essential definitions: those of “critical infrastructures” and “European Critical Infrastructures”.

Art. 2 lett. a) Directive 2008/114/EC defines “critical infrastructure” as “an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions.”¹¹⁴

European Critical Infrastructures (“ECI”), on the other hand, are defined by Article 2 (b) of Directive 2008/114/EC as critical infrastructure located in Member States the disruption or destruction of which *would have a significant impact on at least two Member States*. The significance of the impact shall be assessed in terms of cross-cutting criteria, including with regard to the effects resulting from cross-sector dependencies on other types of infrastructure.’

The ECI Directive focuses on protection of *European* Critical Infrastructures, meaning the identification and protection of national CIs that only affects one Member State remain outside the scope of the Directive. The Directive takes a sector-specific approach and focuses on two main sectors and their subsectors: **energy** (electricity, oil and gas) and **transport** (road, rail, air, inland waterways, ocean, short-sea shipping and ports).¹¹⁵

5.2 The protection of Critical Infrastructures

¹¹² Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

¹¹³ ECI Directive, art 1.

¹¹⁴ Council Directive 2008/114/EC, Article 2.

¹¹⁵ Council Directive 2008/114/EC, Annex 1.

D2.2 – Legal and Ethical Requirements

The ECI Directive provides minimum common standards for EU Member States as the matter is regulated at national level.

The key points foreseen by the ECI Directive are as follows:

The Directive mandates ECI operators to have in place an **Operator Security Plan (OSP)** or equivalent measures.¹¹⁶ The goal of an OSP procedure is the identification of the critical infrastructure assets and existing security solutions. Furthermore, each ECI operator must appoint a Security Liaison Officer,¹¹⁷ tasked with the coordination of security-related issues between ECI operators and the Member State's contact points. Member States must implement appropriate communication mechanisms to facilitate information exchange. Additionally, the Directive specifies ECI related **information handling and reporting requirements**.¹¹⁸

The ECI Directive represents an important step for the protection of critical infrastructures in Europe. However, it does not impose on the Member States specific and substantive measures for the protection of critical infrastructures, as:

- According to the subsidiarity principle, every Member States has the competence to autonomously regulates on national CIs
- The 'primary and ultimate responsibility for protecting ECI falls on the Member States and owners/operators of such infrastructures'.¹¹⁹

Similarly, the ECI Directive does not provide detailed provisions on **confidentiality for security-related information**, as it is under the competence of Member States to regulate on these. Nevertheless, it requires that 'Member States, the EC and relevant supervisory bodies shall ensure that sensitive European critical infrastructure protection-related information [...] is not used for any purpose other than the protection of critical infrastructures'.¹²⁰

5.3 Information sharing

Information sharing can concern a wide variety of valuable data, ranging from security practices, risks, threats and so on, to personal data as well as intellectual property and confidential or business related information.¹²¹ Beyond the notification requirements mentioned in the previous sections, the **sharing of security-related information amongst critical infrastructures and with public authorities** is not comprehensively regulated at the EU level.

As will be discussed more thoroughly in the following chapter, cyber-attacks are criminalised on a national, European and international level. CIs progressively need to cooperate, either on a voluntary or a mandatory basis, with national competent or law enforcement authorities for the prevention, detection, investigation and prosecution of cybercrimes constituted by cyber-attacks. Cooperation among CI with regard to potential threats, incidents, prevention and responses

¹¹⁶ Directive on European Critical Infrastructures, Article 5.

¹¹⁷ Directive on European Critical Infrastructures, Article 6.

¹¹⁸ Directive on European Critical Infrastructures, Article 7.

¹¹⁹ Directive on European Critical Infrastructures, recital 6.

¹²⁰ Directive on European Critical Infrastructures, Article 9.

¹²¹ Recitals 40, 41 and 63 Directive (EU) 2016/1148.

D2.2 – Legal and Ethical Requirements

initiatives is encouraged and promoted, as well as collaboration with other European bodies and agencies, inter alia Europol¹²², its European Cyber Crime Centre (EC3) and ENISA¹²³.

CyberSANE end-users, in their capacity of critical infrastructures, may voluntarily participate in platforms such as the Critical Infrastructure Warning Information Network (CIWIN) and the European Public Private Partnership for Resilience (EP3R) in order to share information related to prevention and distribution of best practice documentation. The key objective of the CIWIN is to enable coordination and co-operation via information sharing on the protection of critical infrastructure at an EU level, ensuring secure and structured exchange of information and allowing its users to efficiently learn about best practices in other EU Member States. On the other hand, EP3R is managed by ENISA and it mainly encourages the exchange of information between the public and the private sector.

¹²² European Union Agency for Law Enforcement Cooperation.

¹²³ European Union Agency for Network and Information Security, <https://www.enisa.europa.eu/>.

6 Evidence handling

6.1 Introduction

In the aftermath of a cyber-attack or attempted attack, information relating to the attack may consist part of potential valuable evidence which can assist in answering investigative questions.¹²⁴ The role of a CI, or any non-law enforcement entity, is not to perform an investigatory process and define which data constitute relevant digital evidence for an investigation. Nonetheless, either on an obligatory basis, or upon own initiative, the entity may provide access and/or share data with investigatory authorities. The ShareNet component of CyberSANE aims at facilitating this process. The rules that apply on handling of digital evidence will be reviewed within this section.

6.2 Cybercrime

6.2.2 *The Budapest Convention*

As technology advances, computer related crimes have grown to include many new types of crimes, which are encompassed by the umbrella term '**cybercrime**', adopted by scholars, policymakers, and the general public. Cybercrime, like all types of crime, is regulated by criminal law which has already been widely sensitive and primarily within the realm of the national legal order. As this newly founded form of crime emerged, it was clear that the transnational nature of cybercrime called for international cooperation and legislative harmonisation.¹²⁵ The CoE initiated the first legislative process in fighting cybercrime within Europe already in 1989, which led to the signing of the Budapest Convention on Cybercrime in 2001.¹²⁶

The Budapest Convention is the only binding international instrument providing for substantive and procedural rules on cybercrime and it has been ratified by 55 States, including all the Contracting Parties of the CoE and EU Member States, except Ireland and Sweden that have only signed it, and other States inter alia the United States of America (U.S.A.).¹²⁷ It has influenced both the European and the **national legislative procedures in criminalising attacks against computer and information systems**. However, even though the Budapest Convention achieved a major step towards harmonisation and cooperation in the international field of cybercrime, its broad scope and nature allows an ample discretion in its implementation by States. Its provisions on international cooperation are considerably bounded and insufficient to meet the threshold of cooperation for the investigation of cybercrime. What remains important, nonetheless, is its provisions on law enforcement powers to order **production, real-time collection and**

¹²⁴ Marcus Rogers, Forensic Evidence and Cybercrime in T. Holt, A. M. Bossels (eds.) The Palgrave Handbook of International Cybercrime and Cybercrime, Springer Nautre (Switzerland 2019).

¹²⁵ P. M. F. Freitas and N. Gonçalves, *Illegal access to information systems and the Directive 2013/40/EU*, International Review of Law, Computers & Technology, Vol. 29, No 1, 2015, p.56-57.

¹²⁶ Council of Europe, Convention on Cybercrime, 23.11.2001, European Treaty Series No 185, available at: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf.

¹²⁷ According to the status as of 20.02.2020, available at: http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=I5RQNY0D

interception of data, that should be implemented by States within their national criminal and criminal procedural laws.

6.2.3 The Cybercrime Directive

The EU actions on cybercrime include several Communications from 2001 onwards, the Council Framework Decision 2005/222/JHA and finally the Directive 2013/40/EU on attacks against information systems ('Cybercrime Directive') replacing the aforementioned Framework Decision.¹²⁸ In its turn, the Cybercrime Directive seeks to harmonise to the extent possible criminal law provisions regarding computer related criminal offences at an EU level, by providing for a minimum **set of rules on computer related offences and respective sanctions as well as to improve cooperation between national authorities and EU bodies and agencies**. It has been transposed by all the Member States but Denmark¹²⁹ and it builds on the Budapest Convention, as it provides for an aligned definition of criminal offences. Its added value stems from its more cogent approach on penalties as well as its provisions improving the field of cooperation.

The Cybercrime Directive **criminalises acts compromising the confidentiality, integrity and availability of information systems**. In particular, an information system refers to:

*'a device or group of inter-connected or related devices, one or more of which, pursuant to a programme, automatically processes computer data, as well as computer data stored, processed, retrieved or transmitted by that device or group of devices for the purposes of its or their operation, use, protection and maintenance.'*¹³⁰

The term covers a wide range of computing devices, ranging from traditional computers to new electronic communication devices as well as it applies to computer data to networks supporting the communication of data between devices. Criminal offences underlined by the Directive include the illegal access to information systems, the illegal system and data interference and the illegal interception.¹³¹ Access to confidential information by an unauthorized person, personification, interception, modification or reproduction of data streams are examples of the numerous types of acts that fit into the legal definitions of these cyber-crimes.¹³² The Cybercrime Directive **further encourages the Member States to punish incitement, aiding and abetting and attempt to commit a cybercrime** offence in the same manner as the criminal offence itself. Finally, Member States must *'take the necessary measures to ensure that appropriate reporting channels are made available in order to facilitate the reporting of the [cybercrime] offences'*. An operational national point of contact should be established within each Member State in order to facilitate the exchange of information and provide assistance where possible.¹³³

¹²⁸ Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, OJ L 218, 14.8.2013, p. 8–14.

¹²⁹ National transposition measures communicated by the Member States concerning: Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, available at: <http://eur-lex.europa.eu/legal-content/EN/NIM/?uri=CELEX:32013L0040&qid=1504174899685>.

¹³⁰ Art. 2(a) Directive 2013/40/EU.

¹³¹ Art. 3-6 Directive 2013/40/EU respectively.

¹³² Pedro Miguel F. Freitas and Nuno Gonçalves, *Illegal access to information systems and the Directive 2013/40/EU*, p. 54.

¹³³ Art 13 Directive 2013/40/EU.

D2.2 – Legal and Ethical Requirements

It should be pointed out that the risks stemming from attacks against the information systems of Critical Infrastructures are mentioned explicitly in the recitals of the Cybercrime Directive. In particular, it notes that the framework and stringent criminal penalties provided for by the Directive will, by extension, enhance and complement the protection of Critical Infrastructures and their information systems.¹³⁴ In this way, it is important for CIs to note that a cyber-attack, whether committed or attempted, will most probably constitute a criminal offence and as such further cooperation with law enforcement authorities would be either obligatory or advisable. The national laws transposing the Directive should then also be taken into account.

For the development of CyberSANE, it should be noted that data relating to attacks, including attempted attacks, constitute data on a criminal offence and thus part of potential evidence, should a criminal investigation be initiated. Sharing of the data in question might take place either on a voluntary basis, or in compliance with a legal obligation under which the end-user is subject, like for instance, the aforementioned breach of data under the GDPR, incident notification under the NIS Directive or criminal procedural law under the Cybercrime Directive and national criminal law.

CASE	REQUIREMENT
The CyberSANE system processes data that may constitute digital evidence, after a cyber-attack or attempted attack has taken place	CyberSANE must allow for an criminal investigatory process by law enforcement to take place

6.3 Criminal and Criminal Procedural law

6.3.1 Fair trial principles

Criminal law is primarily nation-based, which means that rules and obligations are not harmonised on a European level. Nonetheless, several principles derive from European human rights law and are enshrined into national criminal law. The right to fair trial and effective remedy is established in Article 6 ECHR and Article 47 Charter, in combination with Article 48 Charter on the presumption of innocence. As discussed in Chapter 2 Fundamental Rights, the ECHR and the Charter provide obligations for the State, which has to protect its citizens rights and freedoms. In that regard, CyberSANE end-users will not be under the obligation to adhere to these principles. Nevertheless, as cybercrime evolves outside the boundaries of physical crime, and private entities are increasingly involved in the investigatory process, it may be good to envisage a potential applicability of some of these principles. Therefore, the principles in question are briefly presented here.

The right to fair trial ¹³⁵	The guarantees stemming from the right to fair trial apply in advance of formal charges, throughout the entire process of investigation.
--	--

¹³⁴ Recital 4 Directive 2013/40/EU.

¹³⁵ Art 6(1) ECHR, 'In the determination of any criminal charge against him, everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law'.

D2.2 – Legal and Ethical Requirements

A fair hearing	A fair hearing provides the individual with the right of access to court, a hearing in the presence of the accused, freedom from self-incrimination, equality of arms, the right to adversarial proceedings and a reasoned judgement.
The freedom from self-incrimination	The accused has the right to silence and the right not to incriminate themselves. The prosecution carries the burden of proof and must, thus, seek to prove their case against the accused. Any doubt should benefit the accused until a final conviction in accordance with the law.
The principle of equality of arms and the right to adversarial proceedings	All parties to proceedings must have knowledge of all evidence adduced or observations filed. This right implies that prosecuting and investigatory authorities must disclose any material in their possession, or to which they could gain access, which may assist the accused in exonerating themselves or in obtaining a reduction in sentence.
Witness attendance and examination	The accused is allowed to call and examine any witness whose testimony they consider relevant to their case, and must be able to examine any witness who is called, or whose evidence is relied on, by the prosecutor. Moreover, all evidence relied on by the prosecution should be produced in the presence of the accused at a public hearing with a view to adversarial argument.

6.3.2 Admissibility of evidence

The rules on the admissibility of evidence, as part of criminal procedural law, are principally established at a national level. In particular, for most States, the question of **admissibility of evidence is strongly related to the lawfulness of gathering and obtaining evidence**, in the sense that unlawfully obtained evidence may be excluded from admission. This is referred to as the exclusionary principle of illegally or improperly obtained evidence, to which, however, exceptions are also often established. The unlawfulness may be born from the violation of fundamental rights, such as the right to fair trial or the rights to privacy and to data protection, or from the violation of legal rules, such as criminal procedural rules or data protection rules. Depending on the legal regime of each State, judges enjoy a wide margin of discretion in deciding the admissibility of unlawfully obtained evidence. Furthermore, several national legal orders accept the admissibility of unlawfully obtained evidence when there is no other evidence to support the conviction of the accused.¹³⁶ Finally, from a technical point of view, digital evidence must be relevant, reliable and authentic in order to be admissible before a criminal court.¹³⁷

¹³⁶ F. Coudert, M. Gemo, L. Beslay, F. Andritsos, 'Pervasive Monitoring: Appreciating Citizen's Surveillance as Digital Evidence in Legal Proceedings, 4th International Conference on Imaging for Crime Detection and Prevention 2011 (ICDP 2011).

¹³⁷ O. Leroux 'Legal admissibility of electronic evidence', *International Review of Law, Computers & Technology*, 18:2, (2004)

Regarding handling of evidence, it is law enforcement authorities that are responsible for presenting lawfully obtained and admissible evidence before the court. Nonetheless, given that, upon a cybercrime attack, all the evidence will first be located within the information system of the victim, i.e. the CI, the latter will by default also handle to a degree evidence. All information relating to an attack should thus be handled with outmost care, not allowing for any access beyond necessary in order to prevent any alteration of the evidence and to ensure that no rule is broken on behalf of the CI.

CASE	REQUIREMENT
The CyberSANE system processes data that may constitute digital evidence, after a cyber-attack or attempted attack has taken place	CyberSANE must keep all information relevant to the cyber-criminal offence in question, which could be used for the investigatory process. CyberSANE must separate digital evidence from rest datasets. CyberSANE must preserve the digital evidence in a manner that does not allow any alteration or unauthorised access.

6.4 Data Protection law

As mentioned in Chapter 3 EU Data Protection Framework, the DPLED might be applicable on end-users who are competent authorities within the meaning of the directive or who **process personal data on behalf of law enforcement authorities for the purpose of prevention, investigation, detection or prosecution of criminal offences**. According to the DPLED, *‘the activities [...] are focused mainly on the prevention, investigation, detection or prosecution of criminal offences, including police activities without prior knowledge if an incident is a criminal offence or not. [...] They also include maintaining law and order [...] where necessary to safeguard against and prevent threats to public security and to fundamental interests of the society protected by law which may lead to a criminal offence.’*¹³⁸

The DPLED provides clarification as regards potential processors: *‘[F]or example, for the purposes of investigation detection or prosecution of criminal offences financial institutions retain certain personal data which are processed by them, and provide those personal data only to the competent national authorities in specific cases and in accordance with Member State law. A body or entity which processes personal data on behalf of such authorities within the scope of this Directive should be bound by a contract or other legal act and by the provisions applicable to processors pursuant to this Directive, while the application of [the GDPR] remains unaffected for the processing of personal data by the processor outside the scope of this Directive’*¹³⁹

Given the nature of CIs, the critical role they play for safeguarding fundamental interests of society, and the criminal aspect of cybercrime, a **CI might be considered as a competent authority, and thus a controller, under the DPLED, insofar as its activities fall within the above described context, and is entrusted by national law to exercise public powers in performing the activities in question**. Otherwise, a CI might be considered as a **processor under the DPLED**,

¹³⁸ Recital 12 Directive (EU) 2016/680.

¹³⁹ Recital 11 Directive (EU) 2016/680. Similarly, recital 19 Regulation (EU) 2016/679 is dedicated to the interaction between the Regulation and the Directive (EU) 2016/680.

insofar as it performs these activities on behalf of the controller, i.e. law enforcement authorities, either on the basis of contract or on the basis of a legal obligation. The latter may include any legal obligation deriving from EU or national law, for instance criminal procedural law, cybersecurity or cybercrime law, or CI/sector specific law, as discussed in this and previous Chapters. The NIS Directive puts any data processing pursuant to its provisions into the scope of Directive 95/46/EC which was repealed by the GDPR. Given that both NIS Directive and DPLED have to be transposed into national law, their exact application will depend on the national implementation in each Member State.¹⁴⁰

As the landscape between the two data protection instruments, DPLED and GDPR, is unclear, a degree of legal uncertainty is present.¹⁴¹ This uncertainty should, nonetheless, not lead to a situation where personal data remain unprotected. Furthermore, as the DPLED is more lenient and allows for a more wide application of exceptions and restrictions to data subjects rights, its application should be strictly restricted to the processing activities for law enforcement purposes. It should be noted that one of the cornerstone principles of data protection, the purpose limitation principle, enshrined in both the GDPR and the DPLED, provides for a strict framework as regards personal data collected for one purpose and further processed for another.¹⁴² In the case of CyberSANE, it may not always be clear from the start what data are relevant for cybersecurity purposes. Therefore, it may be the case that personal data initially processed for business and economic purposes, are further processed for law enforcement purposes. In that case, the purpose limitation principles requires an assessment of necessity and proportionality. In other words, any further processing should not be excessive or ill-suited to achieve the law enforcement purpose.

CASE	REQUIREMENT
The CyberSANE end-user might be also subject to the DPLED	CyberSANE must allow for different data protection rules/policies to be applicable but in any case make sure that at least one of the two regimes (DPLED or GDPR) applies. CyberSANE should allow for the purpose limitation to be applicable in cases of data initially processed for a purpose different than cybersecurity and cybercrime.

6.5 Proposal for an e-Evidence Framework

In April 2018, the EC presented its proposal for law enforcement cross-border direct access to electronic evidence ('e-evidence') held by service providers. The proposed framework consists of a Regulation and a Directive, which will allow, if they enter into force, for law enforcement authorities in one Member State to ask for user information directly from service providers in another Member State.¹⁴³ The services in question include electronic communications services,

¹⁴⁰ Art. 2 NIS Directive

¹⁴¹ Purtova, Nadezhda. "Between the GDPR and the Police Directive: Navigating through the Maze of Information Sharing in Public–Private Partnerships." *International Data Privacy Law* 8, no. 1 (February 1, 2018).

¹⁴² See also Chapter 3 EU Data Protection Framework.

¹⁴³ https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en

D2.2 – Legal and Ethical Requirements

information society services, and internet domain name and Internet Protocol (IP) numbering services. E-evidence may include subscriber data, access data, transactional data and content data of the users of the abovementioned services. Some categories of data may be requested for all criminal offences, while others may only be requested for cybercrimes as well as for criminal offences with a sentence of maximum 3 years. In accordance with this system, the law enforcement authority may request that the e-evidence being held by the service provider be preserved in their database, until further notice.

The proposed framework is still going through the legislative procedure of negotiations amongst the competent EU Institutions and, as such, it is still subject to changes. Nonetheless, it has raised much concern and criticism, and its future seems precarious. Furthermore, should the proposal be accepted and enter into force, it will only affect CyberSANE end-users that provide the aforementioned services. In that regard, it would be useful to keep in mind that an end-user receiving such request on the basis of the e-evidence framework, will have to easily process the data in question separately from the rest.

CASE	REQUIREMENT
The CyberSANE end-user is subject to the E-Evidence framework, upon its entry into force	CyberSANE must allow for the processing of production and preservation orders

7 Ethics Guidelines for Trustworthy AI

7.1 Introduction

In April 2019, the High Level Expert Group on Artificial Intelligence (HLEG) - set up by the EC in June 2018 - published a document concerning the development of a general framework to support trustworthy AI, the “Ethics Guidelines for Trustworthy AI”.¹⁴⁴

The Guidelines point out that three main components underpin a trustworthy approach to AI, i.e.:

- i) **Lawful**, therefore in compliance with the relevant legal and regulatory framework
- ii) **Ethical**, adhering with ethical principles and values
- iii) **Robust**, from a technical as well as from a social point of view, to avoid unintentional harm.¹⁴⁵

The first element (lawful AI) is not directly dealt with in the Guidelines, where the focus is placed in particular on the second and third component (ethical and robust AI). The latter components cannot be based solely on the existing legal provisions, as the full realization of an ethical and robust AI may require the implementation of principles and elements that exceed the current legal obligations. Against this background, the “*Guidelines proceed on the assumption that all legal rights and obligations that apply to the processes and activities involved in developing, deploying and using AI systems remain mandatory and must be duly observed*”.¹⁴⁶

The Guidelines are structured around three chapters, which will be briefly illustrated, in their key conclusions and guidance, in the next paragraph. The first chapter (“Foundations of Trustworthy AI”) discusses fundamental rights as the foundational basis for Trustworthy AI and particularly of four key ethical principles. The second chapter (“Realisation of Trustworthy AI”) presents seven key requirements, which must be addressed during the entire AI life-cycle via technical and non-technical methods. These requirements are tackled again, in a more practical perspective, by the third chapter (“Assessment of Trustworthy AI”), which explains how to operationalize them and ensure they are complied with through an assessment list.

It is appropriate to add that the publication of the Guidelines had been accompanied by a rather heated debate concerning the alleged vagueness of what has been defined as a strongly industry-driven compromise document. One of the Member of the HLEG, prof. Thomas Metzinger, has defined the Guidelines as a case of “ethics washing” centred on a “Trustworthy AI” marketing narrative, pointing in particular at the scarce involvement of ethicist and at the removal from the final document of “Red Lines”, intended as non-negotiable ethical principles determining what should not be done with AI in Europe.¹⁴⁷

¹⁴⁴ High Level Expert Group on Artificial Intelligence, Ethics Guidelines for Trustworthy AI (hereinafter, “the Ethics Guidelines”), 2019, available at: <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai>.

¹⁴⁵ Pag. 5 of the Ethics Guidelines.

¹⁴⁶ Pag. 6 of the Ethics Guidelines.

¹⁴⁷ Thomas Metzinger, Ethik-Waschmaschinen made in Europe, Tagespiegel, 8 April 2019, available at: <https://background.tagesspiegel.de/ethik-waschmaschinen-made-in-europe> (English)

7.2 Key principles and requirements

The Guidelines promote an **ethics-approach to AI based on the fundamental rights** set out in the EU Treaties, the EU Charter of Fundamental Rights of the EU and international law. Building upon these fundamental rights, the Guidelines (Chapter I) formulate four ethical principles, which must be adhered to in the development of any AI technology. These are:

- Principle of respect for human autonomy
- Principle of prevention of harm
- Principle of fairness
- Principle of explicability.¹⁴⁸

Possible tensions between these principles must be addressed through democratic and open deliberative methods, which allow to identify and avoid those situations where an ethically-acceptable trade-off is not possible.

With a view to translate the principles discussed in chapter I into practical requirements, chapter II illustrates a non-exhaustive list of seven requirements, which must be taken into consideration and implemented throughout the entire AI life-cycle by the whole variety of stakeholders involved in it (developers, end-users and society at large).

These interrelated requirements are the following:

1. Human agency and oversight (linked with the principle of respect for human autonomy)¹⁴⁹
2. Technical robustness and safety (linked to the principle of prevention of harm)¹⁵⁰
3. Privacy and data governance (linked to the principle of prevention of harm)¹⁵¹
4. Transparency (linked with the principle of explicability)¹⁵²
5. Diversity, non-discrimination and fairness (linked with the principle of fairness)¹⁵³
6. Societal and environmental wellbeing (linked with the principles of fairness and prevention of harm)¹⁵⁴
7. Accountability (linked to the principle of fairness).¹⁵⁵

The implementation of these requirements can be achieved by a combination of measures, both of a technical and non-technical nature. On the one hand, technical measures that can be included in AI systems, starting from the outset, include the following¹⁵⁶:

version: <https://www.tagesspiegel.de/politik/eu-guidelines-ethics-washing-made-in-europe/24195496.html>)

¹⁴⁸ Pag. 12 and 13 of the Ethics Guidelines.

¹⁴⁹ Pa. 15 of the Ethics Guidelines.

¹⁵⁰ Pag. 16 of the Ethics Guidelines.

¹⁵¹ Pag. 17 of the Ethics Guidelines.

¹⁵² Pag. 18 of the Ethics Guidelines.

¹⁵³ Ibidem.

¹⁵⁴ Pag. 19 of the Ethics Guidelines.

¹⁵⁵ Ibidem

¹⁵⁶ Pag. 21-22 of the Ethics Guidelines.

D2.2 – Legal and Ethical Requirements

- Architectures for trustworthy AI
- Ethics and rule of law by design
- Explanation methods
- Testing and validating and quality of service indicator.

On the other hand, non-technical methods that can play a key role in ensuring Trustworthy AI include the following elements:¹⁵⁷

- Regulation
- Codes of conduct
- Standardization
- Certification
- Accountability via governance framework
- Education and awareness to foster an ethical mind-set;
- Stakeholder participation and social dialogue
- Diversity and inclusive teams.

Chapter III of the Guidelines presents the pilot-version of a Trustworthy AI assessment checklist,¹⁵⁸ which is mainly addressed at developers and deployers and refers to AI systems directly interacting with users.

The assessment list which addresses seven thematic areas: human agency and oversight; technical robustness and safety; privacy and data governance; transparency; diversity, non-discrimination and fairness; societal and environmental well-being and accountability. The list is not intended to be exhaustive and must be adapted to the specific AI system, which has to be continuously checked against the principles and values (discussed in the Guidelines) as underpinning a fully Trustworthy AI.

Case	Requirement
<p>The CyberSANE system (product, process or service) includes components based on AI-systems.</p>	<p>The technical partners involved in the development of AI systems within CyberSANE, as well as the end-users of the CyberSANE system involving AI components, should follow the Ethics Guidelines for Trustworthy AI, with a view to assess and tackle - through the lens of the principles and requirements outlined therein - possible risks entailed by the incorporation of AI systems.</p> <p>The same entities should consider how the assessment list included in the Guidelines can be adapted and implemented in their organization, taking in this regard the most appropriate measures - in terms of processes and governance - to address the risks posed</p>

¹⁵⁷ Pag. 22-23 of the Ethics Guidelines.

¹⁵⁸ Pag. 26 of the Ethics Guidelines.

D2.2 – Legal and Ethical Requirements

	<p>by the AI systems at issue. The entities involved in the development or deployment of an AI-based CyberSANE must also be aware that a new, revised version of the above-mentioned check-list will be proposed to the Commission in early 2020, based on the experience of the stakeholders engaging in the piloting of the list during the first months following the publication of the Guidelines.</p>
--	---

8 Summary Table of Requirements

CASE	REQUIREMENT
<p>CyberSANE activities are should be in accordance with the law</p>	<p>CyberSANE end-users must find a suitable national or European legislative act which describes the possibility to conduct the processing activities and the requirements to follow. CyberSANE activities must not exceed the boundaries of such legal basis.</p>
<p>CyberSANE activities might be excessively intrusive, thereby entailing the risk of undermining democracy on the ground of defending it</p>	<p>CyberSANE must allow for data processing activities to be suitable to protect information systems and must allow only processing activities that are necessary to said purpose, cannot go beyond what is strictly necessary and must allow for the interests of the end-users to be reasonably balanced with the disadvantage endured by monitored citizens. It must allow to implement adequate and effective guarantees against abuse, taking into account all relevant circumstances, including the nature, the scope and duration of possible measures, the ground for ordering them, the competent persons to permit, carry out and supervise them and the remedies provided by law</p>
<p>CyberSANE activities process data capable to retrieve information of journalists' identity or sources</p>	<p>CyberSANE must allow to limit bulk interception of data originating from journalists and must ensure that, whenever journalists' data are processed, enhanced protection measures can be installed, additionally, it must contain provisions that allow to restrict access of journalists' communication data</p>
<p>CyberSANE end-users are processing data originating from forums or social media</p>	<p>CyberSANE must allow to limit bulk interception of data coming from citizens expressing opinions and must guarantee that there are adequate and effective guarantees against abuse. Account must be taken of all relevant circumstances, including the nature, the scope and duration of possible measures, the grounds for ordering them, the competent persons to permit, carry out and supervise</p>

D2.2 – Legal and Ethical Requirements

	<p>them and the remedies provided by national law</p>
<p>CyberSANE system processes personal data</p>	<p>CyberSANE developers can minimize the applicability of the GDPR and the obligations imposed by it through anonymization techniques to the degree possible. CyberSANE must be developed taking into account that potentially the vast majority of data processed will be personal and hence protected by the EU Data Protection framework</p>
<p>The CyberSANE system processes personal data for security reasons and requires for a certain level of secrecy while its use must remain transparent</p>	<p>The CyberSANE developers must ensure that the technology allows for the end-users to inform all individuals concerned of their secret data processing activities on their websites via a privacy policy and that all processing activities are conducted fairly.</p> <p>CyberSANE developers must further ensure that clear comprehensive and accurate information is provided to end-users in a human-readable format that explains the functions, sources and risks associated.</p>
<p>CyberSANE end-users process vast amounts of data for different purpose</p>	<p>CyberSANE developers should design the system so that only relevant data are processed. The relevance shall be determined by the link of the data processing with the specific purpose for which CyberSANE is used. CyberSANE should allow for different datasets to be processed differently, in accordance to their different purposes</p>
<p>The CyberSANE system processes personal data beyond their original purpose</p>	<p>CyberSANE should ensure that further processing is performed only to the extent that is strictly necessary for the purpose of security.</p>
<p>Vast amounts of data are being processed by the CyberSANE system</p>	<p>CyberSANE should function on restricted access controls, according to the function and capacity of the use. The data-controller shall make sure the process takes place under the principle of proportionality: access of users to the system shall be foreseen only insofar as it is necessary by the purpose for processing,</p>

D2.2 – Legal and Ethical Requirements

	respectful of the separation of duties with a need-to-know principle approach.
Personal data processed by CyberSANE must be accurate and up to date	CyberSANE must allow for continuous checks and the rectification of inaccurate data
The CyberSANE system must store personal data for restricted periods of time	CyberSANE developers must ensure that adequate technical and organizational measures are adopted to make sure that personal data can be deleted or anonymised whenever they lose their necessity to achieve cyber security.
The CyberSANE system must keep personal data in a secure manner, preventing unauthorised access or unwarranted loss of data.	<p>The CyberSANE system must be designed taking into account confidentiality and secrecy requirements, with limitations as to access and management of the system.</p> <p>CyberSANE developers and end users must take into account the implementation of security measures (equipment access control, data media control, storage control, user control, data access control, communication control, input control, transport control, recovery, reliability, integrity) based on an assessment of risks for the protection of individuals' data against the nature and scope of processing. CyberSANE developers shall ensure that access rights are calibrated so as to limit the plain view of personal data processed by CyberSANE only to those competent subjects. Limitations on access and use of CyberSANE to third parties shall be designed and implemented before the system becomes fully functional to the end-user</p>
The CyberSANE system processes personal data	The legal basis for using the CyberSANE system should be established in advance. CyberSANE developers should take into account that each processing activity might rely on a different legal basis, and might be thus subject to different limitations.
The CyberSANE system processes biometric data, patient data or other sensitive data	CyberSANE developers need to consider technical means in which the controller/end-user will be restricted in using CyberSANE only within the boundaries of a certain purpose and legal basis

D2.2 – Legal and Ethical Requirements

The CyberSANE system performs processing activities which require the presence of a DPO	CyberSANE must allow proper and easily understandable access to the DPO
The CyberSANE processing activities result in high risk for the rights and freedoms of individuals	CyberSANE must be designed in a way that allows the continuous evaluation of the system and implementation of measures for the protection of the personal data
There is a breach of personal data to the CyberSANE system	CyberSANE must implement techniques for notifications to the DPA and/or the data subject within the strict time limits
Data subjects file in a request to exercise their rights	The CyberSANE system must be prepared to abide by the request, and provide proper information and/or access regarding the processing activities, rectify or delete data, or block the processing
The CyberSANE system allows for automated decision making	<p>The CyberSANE system should include checks and balances, by keeping a human in the loop</p> <p>The CyberSANE user must ensure that one of the three exhaustively enumerated conditions under which automated decision-making is allowed, applies</p>
The CyberSANE end-user might be subject to the DPLED	CyberSANE must allow for compliance with the DPLED-specific obligations, such as the distinction of data and separate storage rules
CyberSANE consists of a cloud computing service	CyberSANE must allow for data portability
The CyberSANE system processes non-personal data	CyberSANE must allow for controls by regulatory authorities and must have strong security measures in place
The CyberSANE system processes mixed datasets	CyberSANE must make clear to what extent the non-personal data and the personal data parts are inextricably linked. If not, CyberSANE must allow for separate privacy and confidentiality policies to apply for the non-personal and the personal data

D2.2 – Legal and Ethical Requirements

<p>A CyberSANE end-user qualifies as OES under the NIS Directive.</p>	<p>The technical partners developing the CyberSANE system must consider that the end-users must adopt, as required under the NIS Directive, technical and organizational measures appropriate to manage the risks posed to the security of their network and information systems.</p> <p>The CyberSANE system must enable the prompt detection of an incident having a significant impact on the continuity of the essential service, as the OES end-users are subject to a duty to notify such incident without undue delay.</p>
<p>Where CyberSANE is to be offered as a cloud-based solution, the CyberSANE provider qualifies as DSP under the NIS Directive.</p>	<p>The development of CyberSANE must take into account the obligations to which a CyberSANE provider will be subject under the NIS Directive (art. 16), concerning security measures and notification requirements. The notification of an incident with substantial impact on the provision of a CyberSANE cloud service must refer to the possible impact on the provision of a service by an OES.</p>
<p>The CyberSANE end-user is subject to the NIS Directive’s obligations processes personal data.</p>	<p>GDPR and NIS Directive obligations apply cumulatively. Compliance with each of these legal frameworks, in any case, should be addressed separately (for instance by keeping two distinct lists of the measures taken under GDPR and the NIS Directive respectively).</p>
<p>A CyberSANE-related product, service or process will be offered on the market</p>	<p>The CyberSANE partners involved in the development of the product, service or process at issue, and in any case the entity that will manufacture or market those, must monitor the rules of the EU cybersecurity certification scheme that will be introduced, in order to ensure compliance with such rules and possibly achieve a certification.</p>
<p>CyberSANE processes data that may constitute digital evidence, after a cyber-attack or attempted attack has taken place</p>	<p>CyberSANE must allow for a criminal investigatory process by law enforcement to take place</p>

D2.2 – Legal and Ethical Requirements

<p>The CyberSANE system processes data that may constitute digital evidence, after a cyber-attack or attempted attack has taken place</p>	<p>CyberSANE must keep all information relevant to the cyber-criminal offence in question, which could be used for the investigatory process. CyberSANE must separate digital evidence from rest datasets. CyberSANE must preserve the digital evidence in a manner that does not allow any alteration or unauthorised access.</p>
<p>The CyberSANE end-user might be also subject to the DPLED</p>	<p>CyberSANE must allow for different data protection rules/policies to be applicable but in any case make sure that at least one of the two regimes (DPLED or GDPR) applies. CyberSANE should allow for the purpose limitation to be applicable in cases of data initially processed for a purpose different than cybersecurity and cybercrime.</p>
<p>The CyberSANE end-user is subject to the E-Evidence framework, upon its entry into force</p>	<p>CyberSANE must allow for the processing of production and preservation orders</p>
<p>The CyberSANE system (product, process or service) includes components based on AI-systems.</p>	<p>The technical partners involved in the development of AI systems within CyberSANE, as well as the end-users of the CyberSANE system involving AI components, should follow the Ethics Guidelines for Trustworthy AI, with a view to assess and tackle - through the lens of the principles and requirements outlined therein - possible risks entailed by the incorporation of AI systems.</p> <p>The same entities should consider how the assessment list included in the Guidelines can be adapted and implemented in their organization, taking in this regard the most appropriate measures - in terms of processes and governance - to address the risks posed by the AI systems at issue. The entities involved in the development or deployment of an AI-based CyberSANE must also be aware that a new, revised version of the above-mentioned check-list will be proposed to the Commission in early 2020, based on the experience of the stakeholders engaging in the piloting of the list during the first months following the publication of the Guidelines.</p>

9 List of Abbreviations

Abbreviation	Translation
Charter	Charter of Fundamental Rights of the EU
CI	Critical Infrastructure
CJEU	Court of Justice of the EU
CoE	Council of Europe
DPIA	Data Protection Impact Assessment
DPLED	Directive (EU) 2016/680
DPO	Data Protection Officer
EC	European Commission
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
ENISA	European Union Agency for Network and Information Security

D2.2 – Legal and Ethical Requirements

EU	European Union
E-evidence	Electronic evidence
E-privacy	Electronic privacy
GDPR	General Data Protection Regulation
IP	Internet Protocol
NIS	Network and Information Systems
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union
USA	United States of America
WP29	Article 29 Data Protection Working Party

10 Bibliography

Bruni A., *Promoting Coherence in the EU Cybersecurity Strategy*, in Anton Vedder, Jessica Schroers, Charlotte Ducuing and Peggy Valcke (eds.), *Security and Law, Legal and Ethical Aspects of public Security, Cyber Security and Critical Infrastructure Security*, Intersentia, 2019

Cavoukian, A. Privacy by Design, *Leading Edge*, IEEE Technology and Society Magazine, 2012, 31/4.

CoE, ECtHR, EU Data Protection Supervisor, EU Agency for Fundamental Rights, “Context and background of European data protection laws”, in *Handbook on European data protection law*, Luxembourg, Imprimerie Centrale in Luxembourg, 2018, available at https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf.

Cooperation Group, *Reference document on security measures to be adopted by Operators of Essential Services*, 01/2018, available at <https://ec.europa.eu/digital-single-market/en/nis-cooperation-group>

Cooperation Group, *Reference Document on Incident Notification for Operators of Essential Services*, 02/2018, available at <https://ec.europa.eu/digital-single-market/en/nis-cooperation-group>

De Hert P. and Papakonstantinou, V. The Police and Criminal Justice Data Protection Directive: Comment and Analysis, *Computers & Law Magazine of SCL*, Vol. 22 Issue 6, 2012

European Commission, EC Communication, *Building a European Data Economy*, COM(2017) 9, 10.01.2017, available at <https://ec.europa.eu/digital-single-market/en/news/communication-building-european-data-economy>;

European Commission, EC Communication, *Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union*, COM(2019) 250, 29.05.2019, available at: <https://ec.europa.eu/digital-single-market/en/news/practical-guidance-businesses-how-process-mixed-datasets>

European Commission, High Representative of the EU for Foreign Affairs and Security policy, *Joint Communication, Cybersecurity Strategy of the European Union: an Open, Safe and Secure Cyberspace*, Brussels, 7.2.2013, JOIN (2013).

European Commission Staff Working Document on the free flow of data and emerging issues of the European data economy Accompanying the document Communication Building a European data economy, 10.1.2017 SWD(2017) 2 final, available at <https://ec.europa.eu/digital-single-market/en/news/staff-working-document-free-flow-data-and-emerging-issues-european-data-economy>

Finck, M. and Frank P. They Who Must Not Be Identified - Distinguishing Personal from Non-Personal Data Under the GDPR. *SSRN Electronic Journal*, 2019

D2.2 – Legal and Ethical Requirements

Freitas, P. M. F. and Gonçalves, N. Illegal access to information systems and the Directive 2013/40/EU, *International Review of Law, Computers & Technology*, Vol. 29, No 1, 2015

High Level Expert Group on Artificial Intelligence, *Ethics Guidelines for Trustworthy AI* (hereinafter, “the Ethics Guidelines”), 2019, available at: <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai>.

Leroux, O. Legal admissibility of electronic evidence, *International Review of Law, Computers & Technology*, 18:2, (2004)

Luc, R., Hendrickx, J. M. and de Montjoye, Y-A. Estimating the Success of Re-Identifications in Incomplete Datasets Using Generative Models. *Nature Communications* 10, no. 1 (December 2019): 3069

Markopoulou D., Papakonstantinou V., De Hert P., *The EU Cybersecurity framework: The NIS Directive, ENISA’s role and the General Data Protection Regulation*, *Computer Law and Security Law Review* 35 (2019).

Metzinger T., *Ethics Washing Made in Europe*, *Tagesspiegel*, 8 April 2019, available at <https://www.tagesspiegel.de/politik/eu-guidelines-ethics-washing-made-in-europe/24195496.html>

Purtova, N. Between the GDPR and the Police Directive: Navigating through the Maze of Information Sharing in Public–Private Partnerships. *International Data Privacy Law* 8, no. 1

Rogers, M. *Forensic Evidence and Cybercrime* in T. Holt, A. M. Bossels (eds.) *The Palgrave Handbook of International Cybercrime and Cybercrime*, Springer Nautre (Switzerland 2019)