ENSURESEC

DELIVERABLE

D3.1 – Legal and Ethical Requirements for ENSURESEC's platform Development

Project Acronym	ENSURESEC
Project Title	End-to-end Security of the Digital Single Market's E-commerce and Delivery Service Ecosystem
Grant Agreement number	883242
Call and topic identifier	H2020 – SU-INFRA01-2018-2019-2020
Funding Scheme	Innovation Action (IA)
Project duration	24 Months [1 June 2020 – 31 May 2022]

Document Information			
Work Package:	WP3	**Task:**	T3.1
Due Date:	30/11/2020		
Version:	1.0	**Status:**	Final
Nature:	PUBLIC		
Lead Partner:	KUL		
Contributors:	ITTI		
Keywords:	Ethics, legal, data protection, privacy, security		
Abstract:	This deliverable provides the legal and ethical requirements applicable to ENSURESEC. It is based on the findings of D1.5. D3.1 takes its starting point in international conventions and EU primary legislation and identifies legal requirements embedded in secondary EU legislation. It also addresses possible future developments in the legal field. In addition, the framework consists of ethical requirements. The ethical principles are especially important for emerging innovations, such as artificial intelligence. The legal and ethical framework described in detail has also been applied to the ENSURESEC innovative tool. D3.1 lays the basis for the impact assessment to be carried out in WP8 and which will result in D8.5.		

Document History			
Version	**Date**	**Contributor(s)**	**Description**
0.1	21/09/2020	KUL	Initial version; ToC and structure
0.2	09/10/2020	KUL	Sections 2 and 3
0.3	13/10/2020	ITTI	Contribution on GDPR
0.4	21/10/2020	KUL	Section 4 and draft section 5
0.5	06/11/2020	KUL	Executive Summary, Introduction and Conclusions
0.6	13/11/2020	KUL	Final draft sent for internal review
0.7	26/11/2020	KUL	Inputs from first review integrated; Sent for second internal review
0.8	27/11/2020	KUL	Second review inputs integrated
1.0	30/11/2020	KUL	Final version

Document Authors	
(Responsible) KUL	Jenny Bergholm Gabriela Ivan-Cucu Sofie Royer
ITTI	Aleksandra Pawlicka (ITTI)

Document Internal Reviewers	
SONAE	Sandro Sandri
SIMAVI	Mircea Predut
ITTI	Marek Pawlicki

DISCLAIMER

This document does not represent the opinion of the European Union, and the European Union is not responsible for any use that might be made of its content. This document may contain material, which is the copyright of certain ENSURESEC consortium parties, and may not be reproduced or copied without permission. All ENSURESEC consortium parties have agreed to full publication of this document. The commercial use of any information contained in this document may require a license from the proprietor of that information.

Neither the ENSURESEC consortium as a whole, nor a certain party of the ENSURESEC consortium warrant that the information contained in this document is capable of use, nor that use of the information is free from risk, and does not accept any liability for loss or damage suffered by any person using this information.

ACKNOWLEDGEMENT

This document is a deliverable of ENSURESEC project. This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement Nº 883242

Executive Summary

This deliverable maps the legal and ethical requirements applicable to ENSURESEC. In the first part, the international conventions and EU primary legislation are discussed, in order to provide the background needed for interpreting the applicable secondary legislation. D3.1 identifies legal requirements embedded in the GDPR, the NIS Directive, the ePrivacy Directive, the Cybersecurity Act and the eCommerce Directive. In addition to the legislation as it exists at the moment of the writing of this deliverable, D3.1 also takes into account upcoming regulatory instruments and updates, still being processed by the European legislator, mainly upcoming legislation concerning artificial intelligence, revision of the ePrivacy Directive and of the NIS directive.

In the second part, the description of the framework surrounding the deliverable would not be complete without a part on ethical principles. These are increasingly gaining relevance for emerging innovations, such as artificial intelligence. Guidance by ethical principles can help to avoid situation, in which existing legislation might create grey zones or not be able to provide legal certainty. In such situations, guidance should be found in ethics, which often also reflect fundamental and human rights interpretations. Further, adhering to ethical principles also helps to build trust in the ecommerce ecosystem.

In the third part, the deliverable applies the legal and ethical framework has been applied to the ENSURESEC innovative tool. For the development of the tool, as well as for the use-cases, data protection principles of the GDPR provide a solid basis,[1] such as lawfulness, purpose limitation, data minimization, accuracy, storage limitation, confidentiality and accountability. Additionally, the principles are completed by, and should be read in light of data protection by design and by default. Data protection by design and by default seeks to develop processes, which already rely on the minimal usage of personal data and where the interest of the data subject is central. Where personal data is used, it should be processed preferably by means of privacy-friendly tools.

Furthermore, key legal aspects that will be addressed, are which partners (or all jointly) can be considered as controllers and/or processors of personal data. Likewise, processing of sensitive data, transfers of personal data to third countries and challenges raised by artificial intelligence are discussed. Also, both the GDPR and the NIS Directive set requirements for the security of processing of personal data, and the GDPR require data subjects to be notified in case of data breaches, if the breach is likely to result in a high risk to the rights and freedoms of natural persons.

The deliverable dives into particular considerations of ENSURESEC, and attempts to propose guidance and options, in order to ensure the quality and security of the delivered tools. Further, recommendations for each of the three use-cases are given. The use-cases will need to respect the applicable legislation, mainly the GDPR, the ePrivacy Framework and the NIS Directive. Further, topics requiring attention are certain categories of data (sensitive data), transfer of personal data to third countries, involvement of employees and tracking of geographic positions.

[1] The principles set out in the GDPR were inspired by the Generally Accepted Privacy Principles (GAPP), developed by the Canadian Institute of Chartered Accountants (CICA) and the American Institute of Certified Public Accountants (AICPA).

Table of Contents

List of Figures

1. Introduction

1.1. Scope of the document

Deliverable 3.1 bears the title Legal and Ethical Requirements for ENSURESEC's Platform Development and Pilots. Therefore, the scope of this deliverable firstly focuses on further specifying the legal and ethical requirements, which were identified in D1.5, by describing them more in detail. Secondly, the deliverable applies these requirements to ENSURESEC, both giving recommendations for the Pilots (also called use-cases in this deliverable) and for the development of the ENSURESEC platform as a whole. The scope focuses on data protection and privacy as well as on security legislation, as outlined in the Description of Action. Further, the findings of this deliverable will be further implemented and assessed under deliverable 8.5 Data protection impact assessment.

1.2. Methodology

This deliverable builds on the findings and preliminary remarks laid out in D1.5 and aims to provide a targeted analysis of legal and ethical consideration and solutions to guide the development and integration of the ENSURESEC platform. It provides both the legal and ethical requirements to be integrated. The deliverable analyses academic and regulatory aspects of the identified legal and ethical requirements. The methodology of each section of the deliverable is as follows.

First Section (Chapter 2)

The first section recalls a number of sources of international law and EU primary law sources. The purpose of this section is to provide a solid basis of descriptions of fundamental and human rights as well as EU primary law. The section is based on legal descriptive research.

Second Section (Chapter 3)

The second section further recalls sources of secondary EU legislation, and also notes the importance of national legislation for the implementation of EU law. The section builds on an analysis of the legislative sources through legal descriptive research.

Third Section (Chapter 4)

The third section builds on the ethical requirements identified in D1.5. It further looks into the relationship between the ethics and the law and contains as well a descriptive research of the ethical framework surrounding the development of the platform. The section also applies the findings on the ENSURESEC project in particular and puts forward recommendations for mitigation strategies.

Fourth section (Chapter 5)

On the basis of the legal analysis made in the first, second and third sections, the fourth section applies the findings of the first three sections to the case of ENSURESEC and provide some recommendations. The deliverable will provide specific recommendations both for the use cases of ENSURESEC as well as for the development of the platform as a whole.

1.3. Relation to other deliverables

The current report provides a targeted analysis of the ethical and legal aspects relevant to ENSURESEC. It builds upon the foundations established in WP 1.4 which provided a high-level overview of the ethical and legal frameworks susceptible of application to the current project. The deliverable aims to establish meaningful requirements and constraints that ought to be considered by technical partners in the implementation and piloting phases. More precisely, requirements with regard to the core principles of data protection will be discussed along with applicable ethical norms.

The deliverable develops the findings in Deliverable 1.5, which mapped the legal and ethical landscape. Additionally, Task 2.4 will produce a summary of the relevant developments to the regulatory landscape. Together with descriptions of developments concerning security threats and business state of practice the developments to the regulatory framework will be consolidated in D2.4 due in M24.

D3.1 provides a detailed description of the ethical and legal framework surrounding the project with recommendations for the use-cases and the development of the platform ENSURESEC. Further detailed recommendations advising the partners with regard to the applications of the relevant legal norms are also included in D.1.6. D.1.6 is a continuous task encompassing the entire duration of the project while the current deliverable sets the requirements for the development of the platform ENSURESEC. Due to the difference in timing of D3.1 and D1.6, some changes to the content are expected to occur, taking into account findings of the project and potential regulatory developments. In addition, this deliverable establishes the point of reference for the study and completion of the data protection impact assessment (DPIA) of WP8. In other words, this deliverable sets the ethical and legal requirements while WP8 aims at evaluating – specifically in the data protection domain – the platform's conformity to the values and norms discussed in the following pages.

Lastly, a disclaimer is in order. The context and the summary of the legal and ethical sources are laid out in deliverable 1.5. It goes into the details of each relevant source and analyses its impact on the ENSURESEC project. Therefore, deliverable 3.1 should be read in the light of D1.5 for a deeper analysis on the background and the overall structure of the ethical and legal framework applicable to the project.

2. International conventions and EU primary law

2.1. Sources of international law

The partners of ENSURESEC are established in jurisdictions that are bound by a number of legal obligations found in international treaties. International treaties are applicable foremost to States who have signed and ratified the treaty in question and sets obligations for these states to ensure the rights enshrined in the conventions. This is also the case for the conventions presented below. This being said, those conventions are not directly applicable to ENSURESEC, but to the Member States where the partners are established. They provide guidance in uncertain legal situations. Moreover, in the same international instruments are enshrined the principles providing the basis for the directly applicable legislation. The following sections provide a short overview of the international legal instruments that may be indirectly relevant for ENSURESEC. However, the main focus of this deliverable will focus on relevant EU legislation on data protection, as many of them are directly applicable to private parties and therefore to ENSURESEC also.

2.1.1. The European Convention of Human Rights (ECHR)

The ECHR[2] does not create direct obligations for private legal persons; but is imposing to the signatory states that have ratified it to establish the appropriate legal instruments in order to ensure the protection of these rights. Hence, if states do not ensure an adequate level of protection, it is possible that natural and legal persons can bring nation states before the European Court of Human Rights (ECtHR) for violations of the ECHR.

The ECHR is an international convention ratified by all Member States of the European Union and, which is relevant for the consortium, the Republic of Serbia. The ECHR protects fundamental human rights and liberties. Amongst its provisions, of particular relevance for ENSURESEC is Article 8, which protects the right to respect for private and family life. It states:

"1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

Art. 8 establishes the basic form of the right to privacy. The concept of private life is broad and includes the activities planned by the consortium, inter alia, the collecting and processing of personal data for research purposes and the protection of e-commerce operators from cyber and physical threats.

Any interference with the right to privacy must be in accordance with the law and necessary in a democratic society in order to fulfil one of the legitimate aims that are mentioned in Art. 8 ECHR. In addition, the interference shall be balanced with competing values and objectives of democratic societies. The normative content of the ECHR is both negative (to abstain from interference and positive, as it obliged its signatories to implement appropriate measure to ensure the protection of the rights enshrined in Art. 8, but also to abstain from interference with the privacy of its citizens. Further, the right to privacy comes with a necessity test, which regulates the interference with the rights and is essential to justify violations of Art. 8. The ECtHR has defined necessity as an interference which responds to a pressing social need, and which is proportionate to the legitimate aim pursued. Thus, necessity also requires that a measure is proportionate. Proportionality is also a requirement under EU law and will be discussed below.

In the context of ENSURESEC, the comprehensive set of regulations adopted by the EU in the area of privacy and data protection concretises the right and will be the main focus for this deliverable. The

[2] Convention for the Protection of Human Rights and Fundamental Freedoms Rome, 4.XI.1950, available at European Convention on Human Rights (coe.int).

principles set by the ECHR shall though be taken into account when entering legal grey zones and EU law should always be interpreted also in the light of the ECHR.[3]

2.1.2. The Council of Europe's Convention 108 on Personal Data

The Convention for the protection of individuals with regard to automatic processing of personal data (also known as Convention 108, here "c180") is the only instrument of international law concerning solely the protection of personal data.

Adopted in 1981, and modernised through a Protocol in 2018[4], c180 forms the foundation of several data protection legal frameworks. This instrument imposes obligations for the signatories to implement appropriate safeguards into national law. The basic principles of data protections established in Art. 5 of the c108 are worth illustrating. These principles, found in Art. 5, are:

- Lawful and fair processing;
- Purpose limitation;
- Data quality and accuracy.

These principles have laid the foundations for modern data protection instruments. In addition, c108 introduced the distinction between personal and sensitive data, which will be discussed further below, under the section on EU law. In this context, it is enough to mention that Art. 6 of c108 defines sensitive data as *"personal data revealing racial origin, political opinions or religious or other beliefs as well as personal data concerning health or sexual life"*.

The c108 also introduced rights for data subjects, which shall be ensured by the signatories. Art. 8 c108 establishes

- the right to information;
- the right to rectification or erasure.

c108 has an established role in the jurisprudence of the ECtHR and is often referred as guidance when assessing the scope of the aforementioned Art. 8 ECHR. Another important aspect of data protection which was first addressed by the c108 is the international transfer of personal data. Chapter III, and especially Art. 12(3), point a, c108 deals with the transborder flow[5] of personal data, which introduced the basic principle for the legitimate cross-border transfer of data, i.e. equivalent protection. This

[3] Article 53 of the Charter.

4 Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), available at https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=090000168089ff4e, last visited 23 November. NB. The Protocol is not yet in force pending ratification by the member states to the convention (as of November 2020 ratified by 40 member states).

[5] C108 defines transborder flows of personal data as a transfer of personal data to the jurisdiction of another party to the c108.

principle is still prominent in the instruments governing transnational data flow as will be discussed further in this report.

2.1.3. The Council of Europe's Convention 108+ on Personal Data (c108+)

As mentioned earlier, the CoE has updated the c108 to reflect the technological changes and the new methods for processing data introduced since its adoption. This resulted in an updated version of the text, namely the Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, also known as the Convention 108+ ("c108+"). Without intervening on the principles introduced in the original c108, this revision aims at extending its application to a wider range of player to prevent forum shopping by data controllers.[6]

Among the relevant novelties of the c108+ is the updated definition of the category of special personal data provided in Art. 6, with the notable inclusion of biometric data, sensitive data, trade-union membership and ethnic data.

Also, Art. 9 of c108+ introduces the right of data subjects as the right *"not to be subject to a decision significantly affecting him or her based solely on automated processing without having his or her view taken into consideration"*. This translates into an obligation for providers of technologies like big data analysis tools or machine learning/artificial intelligence algorithms to lay down transparent and explainable processes within their design activities7. A similar norm is found within the General Data Protection Regulation ("the GDPR")[8], which is directly applicable to the consortium partners of ENSURESEC. In practice, the right also includes the right to become aware if decision-making policies behind automated processing. Therefore, when using automated processing, such as machine learning, transparent and explainable processes for the design activities are needed.

Both c108 and c108+ are relevant for ENSURESEC as a resort for guidance in situations where the directly applicable regulatory framework does not provide clear direction. Interpretations in line with the CoE and EU conventions and guidance documents are also important to implement for data protection by design and default.

2.1.4. The Cybercrime Convention

In this context, a brief overview of the Cybercrime Convention (also known as the Budapest Convention), or Convention 185 (also "c185") is in order. Adopted in 2001 by the CoE, c185 established an international standard for the criminalization of cyber-related offences. C185 has been ratified by 65 States it applies to all the States in which the members of the consortium are established.

[6] Forum shopping by data controlling means the practice of relocating a business entity to a different jurisdiction with less stringent legal requirements.

[7] Bryce Goodman and Seth Flaxman, 'European Union Regulations on Algorithmic Decision-Making and a "Right to Explanation"' (2016) arXiv.org; Ithaca <https://search.proquest.com/docview/2074006289?rfr_id=info%3Axri%2Fsid%3Aprimo> accessed 20 May 2019.

[8] 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), OJ L 119, 4.5.2016.

The main effect of c185 is requiring participating jurisdictions to amend their criminal legislation to fulfil the criteria set in c185. More precisely, c185 aims for signatory and ratifying states to introduce legislation targeting activities, which compromise the so called CIA-triad; data and network Confidentiality, Integrity and Availability. In addition, it enumerates a number of criminal offenses that belong to the following categories:

- Computer-related crimes;
- Computer-assisted crimes;
- Computer-environmental crimes.

Lastly, c185 introduces several mechanisms for the international cooperation of enforcement bodies on electronic data and related evidence exchange. It is also important to note, that the CoE has started a public consultation to draft an additional protocol to c185 on the issue of electronic exchange of evidence.

From the perspective of the partners of the consortium involved in mapping the existing threats to e-commerce operators, c185 may offer a starting point to categorize the relevant conducts considered as criminal offences. Also, since ENSURESEC aims at safeguarding e-commerce operators from cyber and physical threats, it is likely that parts of the set of cyber threats qualify as cybercrimes under international law.

2.2. Primary EU legislation

Primary EU legislation consists of the Treaty of the European Union ("TEU")[9], the Treaty of the Functioning of the European Union ("TFEU")[10] and the Charter of Fundamental Rights of the European Union ("the Charter")[11]. These sources of primary law create the legislative basis for the European Union and all its actions and are always given precedence over secondary legislation[12]. All secondary legislation, including what is described below, is to be interpreted in the light of primary law. Through case law of the CJEU, primary EU law is directly applicable to private parties[13], such as the ENSURESEC consortium.

Furthermore, all secondary legislation must be interpreted in the light of the Treaties and the Charter, they may become relevant for ENSURESEC, as a point of guidance.

[9] Treaty on European Union (Consolidated version 2016), OJ C 202/1, 7.6.2016, p. 15.

[10] Treaty on the Functioning of the European Union (Consolidated version 2016), OJ C 202/1, 7.6.2016, p. 47.

[11] Charter of Fundamental Rights of the European Union, OJ C 202, 7.6.2016, p. 389.

[12] Secondary EU legislation consists of regulations, directives and decision. These provide rights and obligations of private parties.

[13] See cases such as Case 26/62 Van Gend en Loos, ECLI:EU:C:1963:1 and Case 43/75 Defrenne, ECLI:EU:C:1976:56. Please also note that there is also an ongoing discussion on whether the Charter can have direct horizontal effect. In practice, this means that private parties could perhaps be obliged to ensure the fundamental rights of its user for example. However, this discussion is beyond the scope of this deliverable. Also, the GDPR embodies much of the content of primary law when it comes to data protection, privacy and security. The discussion of direct effect of EU primary law is outside the scope of this deliverable.

2.2.1. The Charter of Fundamental Rights of the European Union

The Charter entered into force in 2009 and is a synthesis of the Member States' constitutional traditions. The importance of the Charter is twofold. On one hand, it lays the basis for guidance for the ethical values established within the EU. In this capacity, it also drives the actions of institutions and Member States alike and provides guidance when new technologies are developed in legal grey areas. On the other hand, the Charter is legally binding for all EU institutions and all Member States of the EU since 2009 and a primary source of EU law. As such it establishes the fundamental rights of EU citizens and lays the basis for all legislation and actions by the EU and its Member States.

The relevant provisions for ENSURESEC are Article 7 and Article 8. Article 7 establishes the right to privacy of citizens in several areas, stretching from the physical private life to communications. Article 8 enshrines the right to protection of personal data. It also sets the conditions for processing of personal data and sets the control of compliance under the regime of the independent authority, namely the European Data Protection Supervisor.

Article 7 "respect for private and family life" reads:

"Everyone has the right to respect for his or her private and family life, home and communications."

Article 8 "right to personal data protection" states:

"1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority."

These provisions establish the fundamental requirements for the processing of personal data within the EU. These basic principles of EU law find application in secondary sources of law, such as the ePrivacy Directive and the GDPR, which will be discussed in section 3.1. Another relevant provision of the Charter is Article 52, which introduces the principle of proportionality and sets the scope of the fundamental rights. Hence, it provides the legal basis and justifications for the limitations of such rights within the European legal order. In this context, it sets the basis for all processing of personal data in the EU and provides a balancing test between the rights and the limitations.

Article 52(1) sets out the requirements for when and how fundamental rights can be limited. These concerns all the rights enshrined in the Charter, and therefore also Article 7 and 8. On this basis, limitations on the exercise of the rights and freedoms recognised by the Charter are valid if they:

- Are provided for by law;
- Respect the essence of the right;
- Are proportionate and necessary;
- Meet the objectives of general interest recognized by the EU or the need to protect the rights and freedoms of others.

The reference to the essence of the rights and freedoms is significant. It means that limitations that are so extensive as to devoid a fundamental right of its basic content are unlawful. Note that, if the essence of a right is not respected, it automatically violates EU fundamental rights.[14] As an example, it can be noted, that legislation providing public authorities access to content of electronic communication on a generalised basis has been considered violating the essence of the right to private life (Art. 7).[15] Furthermore, the respect for the essence of rights enables a distinct interpretative lens to assess the validity of possible limitations.

Also, as mentioned in Art. 52(3), the scope of the rights is similar to the ECHR and tights the two instruments together. The Charter shall always be interpreted in the light of the ECHR.

The Charter, and especially Article 7 and 8 and Art. 52(1), are relevant to ENSURESEC as they provide the test for when a limitation to the rights is proportionate, and therefore also in line with EU legislation. However, the principles of the Charter have been materialised into directly applicable legislation through the GDPR and the ePrivacy framework, which are directly applicable to ENSURESEC. The Charter can provide guidance in situations of uncertainty.

Special attention should be paid to the principle of proportionality. As has already been noted in the previous chapter, Article 52(1) sets down criteria for when a limitation to the rights and freedoms of the Charter, such as the right to data protection and to privacy, is lawful.

According to Article 52(1) of the Charter, the principle of proportionality sets out that limitations must be i) necessary, ii) genuinely meet the objective of general interest recognised by the Union or the need to protect the rights and freedoms of others.

Therefore, for any limitation of the right to privacy or data protection, a test needs to be carried out considering whether the limitation is necessary. The test requires an assessment on whether i) the measure is suitable to achieve the goal which is set out as a justification of a specific measure, ii) if that goal is necessary and iii) whether the measure is necessary to achieve the goal.[16]

Even though this test mainly applies to Member States and European Union institutions when exercising their respective powers, the principle of proportionality offers guidance on how to interpret legislation. It also sets the frameworks for what can be justified in the balancing act of balancing two fundamental rights and freedoms against each other, such as the right to data protection and freedom of expression.

The principle of proportionality should be kept in mind when considering how for example the GDPR and other legislation is interpreted.

[14] This was the case concerning the essence of the fundamental right to respect for private life (Art. 7) and the right to effective judicial protection, enshrined in Art. 47 of the Charter in Case C-362/14 *Schrems I* , para. 94 ad 95.

[15] Case C-362/14 *Schrems I*, para. 94.

[16] Craig and De Burca (2015), page 551.

2.2.2. The Treaty of the European Union and the Treaty on the Functioning of the European Union

Together with the Charter, the Treaties make out the primary law of the EU. Through case-law, the Treaties have been given direct effect, meaning that the provisions therein can be relied upon by private parties. In the TEU, the EU Member States established among themselves the European Union and sets the founding principles of the EU. The TFEU organises the functioning of the European Union and determines the areas of competences, limitations and arrangements of exercising the competences of the EU institutions and of the Member States.

When it comes to the Treaties of the EU, Article 16 TFEU is of main interest for ENSURESEC. It reinforces that data protection is to be considered a fundamental right and lays down the legal basis for all data protection legislation. Moreover, Art. 16 TFEU also restates that the compliance with data processing rules shall be subject to control of an independent authority. The content of this Article corresponds to that of the sources of international law examined above. Article 16 of the TFEU refers to Article 39 of the TFEU. The TEU establishes the purpose of the EU, its central institutions (and respective governance structure) and the basic rules on the values of the EU as well as e.g. external, foreign and security policy. In its present form, Article 39, states that the Council shall – in derogation of Article 16(2) TFEU – establish the rules relating to the protection of personal data when carrying out activities relating to foreign and security policy. In addition, the competency of the Council concerning the free movement of personal data is also established, as concerns foreign and security policy.

Article 16 of the TFEU is the basis for the data protection legislation in the EU. Since ENSURESEC is concerned with data protection aspects, the legal basis therefore is good to keep in mind. However, it can be anticipated that the practical relevance of these provisions for ENSURESEC is limited. Most of the applicable legal frameworks to the activities planned by the member of the consortium are covered by secondary EU sources to which this report now turns. However, in cases of legal uncertainty, guidance and interpretation shall be in accordance with the implementation of the sources of primary EU law and international treaties and conventions.

3. ENSURESEC - Legal Requirements

This part will present the secondary EU legislation which is applicable to ENSURESEC, as well as interpretation of that legislation. In Chapter 4, the legal requirements will be translated into legal considerations, providing interpretation and recommendations specifically useful for ENSURESEC. The structure of this part is divided according to the source of law, focusing on EU secondary legislation.

There are several sources of secondary EU legislation relevant for the purposes of ENSURESEC. In this section, the key provisions relating to data protection and security will be laid out and explained. Secondary sources of legislation are foremost regulations and directives. Regulations are directly applicable in all EU Member States from the moment it enters into force, and do not rely on any transposition of the Member States. Directives on the other hand, sets the framework on EU level, but needs to be transposed into national legislation. Directives only have limited direct effect, and as a main rule, the national transposing legislation need to be observed. They operate under the principles and objectives enshrined in the EU Treaties on the basis of the principle of conferral. This particular section is intended to present the relevant legislation and to discuss the legal requirements that are attributed to ENSURESEC.

3.1. The General Data Protection Regulation

3.1.1. General remarks and scope of application

One of the most significant data protection legislations in the world has been **General Data Protection Regulation**. Even before it came into force in May 2018, it had been called the **toughest privacy** and **security regulation** in the world.[17] The reputation has been built on the fact that the regulation imposes obligations on organisations everywhere, as long as they handle the data of individuals in the EU, and introduces **severe penalties** for the ones who mistreat the data. In a nutshell, the GDPR is about: **penalties**, **the need for determining a solid legal basis for processing personal data**, **data protection by design and by default**, **data breach** notification and **pseudonymisation**[18] It is composed of 10 chapters concerning: general provisions, principles, rights of the data subject, duties of data controllers and/or processors, transfers of the data to third countries or international organizations, independent supervisory authorities, cooperation and consistency, remedies, liability and penalties, provisions relating to specific processing situations, delegated acts and implementing acts and final provisions.

[17] https://gdpr.eu/what-is-gdpr/?cn-reloaded=1

[18] Taurino, 2018.

The scope of application of the GDPR extends to activities of controllers and processors established in the EU, and under certain circumstances also if the data processing takes place outside the EU.[19] This can be the case when data subjects are present in the EU-territory. These are if they are offering goods or services to data subjects in the EU or if they are monitoring the behaviour of data subjects in the EU.[20]

Since it is foreseen that ENSURESEC will process personal data at least to some extent, the GDPR is of great importance as a whole, and some sections are more crucial. In this section, the provisions important for ENSURESEC will be described. The implications thereof will be discussed under the section "Legal considerations".

3.1.2. Key concepts

1. *Defining personal data*

The GDPR is designed to regulate the processing of personal data in various different contexts and to set rules for the free movement of personal data.[21] **Personal data is defined** as *"any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly"*.[22]

Categorising and defining **personal data** is a dynamic process, and the scope of application is broad due also to the broad application of c108.[23] For the purpose of this discussion, the question on what "*any information"* comprises of is important. It includes "any sort of statements about a person"[24], which comprises both objective and subjective information about a person as well as information related to a natural person "by content, purpose or effect"[25]. There is no need for the data to be true or to be proven.[26] The format of the data, for example digital or physical documents, is irrelevant, since information in whatever form can be personal data.[27]

Further, the data shall relate "*to an identified or identifiable natural person*". Therefore, different solutions such as anonymisation and pseudonymisation can be used to minimise the data used or to fully prevent identification of a data subject. This will be discussed further under "Legal considerations". Information can even constitute personal data where only a third party has the additional data necessary to identify that person.[28] Examples of personal data are names, social security or identity numbers, IP-address, email-addresses.

[19] Article 3(1) GDPR.
[20] Article 3(2) GDPR.
[21] Article 1(1) of the GDPR.
[22] Article 4(1) GDPR.
[23] Article 29 Working Party, "Opinion 4/2007 on the concept of personal data", 20 June 2007, p.4
[24] Article 29 Working Party, "Opinion 4/2007 on the concept of personal data", 20 June 2007, p. 6
[25] Article 29 Working Party, "Opinion 4/2007 on the concept of personal data", 20 June 2007, p. 10-11.
[26] Article 29 Working Party, "Opinion 4/2007 on the concept of personal data", 20 June 2007, p. 6
[27] Article 29 Working Party, "Opinion 4/2007 on the concept of personal data", 20 June 2007, p. 7
[28] CJEU in the Case C-582/14 *Breyer v Germany.*

2. *Processing of personal data*

Processing of personal data is defined as *"any operation or set of operations which is performed on personal data, whether or not by automated means"*.[29] Article 4(2) of the GDPR lists examples of what constitutes processing, for example activities such as collecting, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combining, restriction, erasure or destruction.

Processing of personal data is also subject to a very broad definition. Inevitably, grey-zones on what constitute personal data may occur. It is therefore important to note, as a guideline, that the objective behind the notion of personal data is to protect the fundamental rights of individuals, and in particular the right to data protection and privacy. This is especially important when trying to define what personal data is, and particularly in situations where the rights of the individual might be deprived if a narrow definition is applied.[30] Such a situation could be making the assessment that a person is no longer identifiable by the data being processed, and therefore falling outside the scope of the GDPR.

3. *Data controllers and data processors*

The GDPR follows the same centralized approach to controllers as was the case under its predecessor the Data Protection Directive (the DPD). Therefore, in systems where components from different organisations (potential data controllers) are integrated, the identified controller still carries the responsibilities for ensuring compliance under GDPR.[31]

Article 4 GDPR deals with the basic definitions that are used in the regulation. From the point of view of ENSURESEC, the definitions of **data controller** (Article 4, paragraph 7) and **processor** (Art 4(8)) are the most relevant. The **controller** is a body (a natural or legal person, public authority, agency, etc.) that is responsible for determining the purposes and means of the personal data processing, either alone or jointly with others. In case Union or Member State law determines the purposes and means of the processing, the controller or their nomination's criteria can be provided for by Union or Member State law. A **processor** is a body (a natural or legal person, agency, public authority…) that processes personal data, on the controller's behalf.

4. *Joint controllers*

Organisations engaging in data processing for the same purpose on different scales can become **a joint controller**. Societal developments and new types of technologies service modules carried out by a set of partners, how to apply the centralized approach of the GDPR to a structure with many partners need to be discussed.[32]

According to Article 26 of the GDPR, joint controllers arise in a situation where *"two or more controllers jointly determine the purposes and means of processing"*. A joint controllership arise, when

[29] Article 4(2) GDPR.

[30] Article 29 Working Party, "Opinion 4/2007 on the concept of personal data", 20 June 2007, p 4

[31] Mahieu et al., page 87, para 11.

[32] Gürses and van Hoboken (2017), cited in *Mahieu et al, para. 12, page 87.*

partners together determine the purposes and means at least to some extent and for some part of the data processing, but the GDPR fails to introduce any indication as to what extent a party needs to be involved in the data processing to become a joint controller . [33]

Joint controllers *"shall in a transparent manner determine their respective responsibilities for compliance with the obligations"*.[34] This is especially important when it comes to the rights of the data subject and for fulfilling their duties towards upholding the rights of data subjects.

The joint controllers can divide their responsibilities for ensuring compliance for example by designating a contact point for the data subject. Such division shall be done by means of arrangements and shall *"reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects"*[35]. Further, the essence of this arrangement shall be made available to the data subject. This does however not release the partners from the joint responsibilities and the data subject can exercise his or her rights under the GDPR "*in respect of and against*" each of the controllers.[36]

In this context, it is important to keep in mind, that even if the GDPR points towards an attribution of responsibility between the partners based on an agreement, it does not specify what kind of agreement, or how to divide the responsibilities in cases where no clear agreement exists[37].

As mentioned above, a controller is the one who "*determines the purpose and means of the processing of personal data*". The purpose of the processing can answer the question why and how it is being processed can be answered by looking at the essential means of the processing. [38] This is important for determining who are the controllers and processors under the GDPR. This can be done by looking at what the purpose of the processing is, and who is the partner deciding that, and what the means are therefore, and which partner is responsible for that. In order to identify purposes or essential means, one needs to take into account the factual circumstances, and especially so when no clear agreement exists between the parties. [39]

The **scope of joint controllership** has recently been given a broad meaning by the CJEU. First, a joint controller can be an administrator of a fan page on a social network, together with the social network operator.[40] Second, a community together with the individual members of that community can be joint controllers, when the activities are "organized, coordinated and encouraged" by the community.[41] Thirdly, embedding a plug-in on a webpage can turn the administrator of that webpage into joint controllership together with the operator of the plugged in service, even for processing of

[33] Mahieu et al, para 18, page 89
[34] Article 26(1) GDPR
[35] Article 26(2) GDPR.
[36] Article 26(2)-(3) GDPR.
[37] Mahieu et al, para 18, page 89
[38] Mahieu et al, para 18, and See also Patrick van Eecke and Maarten Truyens, 'Privacy and Social Networks' (2010) 26 Computer Law & Security Review 535, 539.:
[39] Mahieu et al, page 89, para. 19
[40] As in C-210/16 *Wirtschaftsakademie Schleswig-Holstein*.
[41] As in Case C-25/17, *Jehovan todistajat*

data that the webpage administrator do not have access to.[42] Accordingly, ECJ confirms, that both natural and legal persons can be (joint) controllers without written guidelines or instructions from the controller, as long as the natural or legal person "*exerts influence*" over the personal data processing for his or her own purposes and who participates in determining the purposes and the means thereof.[43]

Likewise, as concerns the **division of responsibility between the parties**, the CJEU has been sticking to the principle of effective and complete protection.[44] The statement of the CJEU is clear:

" […] the existence of joint responsibility does not necessarily imply equal responsibility of the various operators involved in the processing of personal data. On the contrary, those operators may be involved at different stages of that processing of personal data and to different degrees, so that the level of responsibility of each of them must be assessed with regard to all the relevant circumstances of the particular case."[45]

Accordingly, the responsibilities of the parties can vary, depending on the factual situation. Some further advice stems from the case *Google Spain*[46] in which the division between the parties is referred to as "*within the framework if its responsibilities, powers and capabilities*"[47]

Two interpretations for the division of responsibility have been developed by scholars:

"*each controller is responsible for what it is able to do even without proper coordination with other joint controllers*."

and

"Alternatively, it could mean that whenever one of the controllers is able to prevent infringement of data protection laws, they should do so, either by persuading their joint controller to commit to all data protection obligations, or by not integrating the infringing service." [48]

Even though the current legal discussion does not set any clear criteria as to how to divide the join responsibilities, it seems clear that partial and different degrees of responsibilities of the partners is possible. Therefore, one interpretation could be that every partner is responsible for the processing

[42] As in *Case C-40/17, Fashion ID)*

[43] C-25/17 *Jehovan todistajat*, para. 67-68.

[44] Introduced in Case C-131/12 *Google Spain SL, Google Inc v Agencia Espailola de Protecci6n de Datos (AEPD) and Maria Costeja Gonzdlez* EU:C:2014:317**,** para. 34 and manifested in C-210/16 *Wirtschaftsakademie Schleswig-Holstein*,

[45] C-210/16 *Wirtschaftsakademie Schleswig-Holstein*, para. 43

[46] Case C-131/12 *Google Spain SL*

[47] Case C-131/12 *Google Spain SL*, paras 38 and 83. This criterion is also referenced by AG Bot in Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein*, EU:C:2018:388, Opinion of AG Bot, para 63.

[48] Mahieu et al, page 96, para 56

activities or the parts of which it is taking part in.[49] and depending on their degree of involvement[50]. What further complicates the matter is, that there is no legal basis in the GDPR or its predecessor Directive 95/46/EC for such a division of responsibilities. [51]

Further, it is also not clear what the consequences for a **lack of a clear agreement** between the partners of a joint controllership, or not upholding such an agreement, could be.[52] Nevertheless, there seems to be consensus on that the effectiveness of data protection law is at risk of being undermined without clear responsibility allocations.[53]

5. *Implications for ENSURESEC*

The nature of the GDPR and the discussion above may cause some **implications important to note for ENSURESEC**. Depending on the structure laid out in the Data Management Plan of ENSURESEC in deliverable 1.7, controllers of data processing activities need to be identified. Also, if more than one of the partners of the consortium are taking part in the processing of personal data, they could be considered joint controllers. It shall be noted, that the controllership does not follow designation, but is determined by the factual circumstances. The interpretation of who is a controller is so broad, because the identification thereof is crucial for the realization of the data subjects' rights. Therefore, any of the partners who "*determine the purposes and means of processing*" could be considered a data controller, either alone or jointly, depending on the circumstances. Joint controllers have full responsibility and liability towards the data subject, even if they distribute the potential cost of non-compliance among themselves.[54]

Having said the above, it is clear that both data controllers, joint controllers and data processors depend on each other **to fulfill their compliance obligations**.[55] The lines between being a processor or a controller can be blurry and at this point in time, one should be aware that the case law suggests that almost any "arrangement that involves collaboration in data collection or use" might be considered a joint controllership.[56] This is of interest for the consortium of ENSURESEC, where different partners might take part in different phases of personal data processing and to varying extent. Nevertheless, it is very likely that many of them will fall under the broad interpretation on being a controller or a joint controller, and the obligations that comes with it.

[49] Mahieu et al, para26, page 90

[50] Article 29 Data Protection Working Party, 'Opinion 1/2010 on the Concepts of "Controller" and "Processor"' (2010), 1, 22 and33; Article 29 Data Protection Working Party,'Opinion 10/2006 on the Processing of Personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)' (2006), 2.

[51] Mahieu et al, para 28, page 90

[52] Mahieu et al., page 3, para 4

[53] WP29 opinion 01/2010, page 18, also Christopher Kuner, European Data Protection Law: Corporate Compliance and Regulation (2nd edn, Oxford University Press 2007), 71-77*, indicating that the existence Of these unclear situations is not a mere theoretical concern.*

[54] Mahieu et al, para 30, page 90, interpreting Article 29 Data Protection Working Party, 'Opinion 1/2010 on the Concepts of "Controller" and "Processor"' (2010)

[55] Milliard 2019, International Data Privacy Law, 2019 Vol. 9 No. 4, page 218.

[56] Milliard 2019, International Data Privacy Law, 2019 Vol. 9 No. 4, page 218.

Potential scenarios will be further discussed under the section "Legal considerations".

3.1.3. Data protection principles

The GDPR has been designed to be technology neutral, meaning that the regulation shall be applicable and enforceable no matter the technology used for the processing. Therefore, the structure of the regulation is centralised around seven principles for processing of personal data. Article 5 addresses the ways personal data should be treated, i.e. the principles of:

- **lawfulness, fairness and transparency** –in relation to the data subject, data must be processed lawfully, fairly and in a transparent way (a);
- **purpose limitation** – the principle states that the data must be collected "for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes"[57]. It must be emphasized that, in accordance with Article 89(1), further processing for archiving purposes (in the public interest), scientific or historical research purposes or statistical purposes is not seen as incompatible with the initial purposes (b);
- **data minimization** – which means that the data collected ought to be adequate, relevant and limited only to the extent that is necessary in relation to the purposes for which they are processed (c);
- **accuracy** – the data must be accurate, up to date and steps must be taken to make sure that inaccurate data are erased or rectified (d);
- **storage limitation** – personal data must be kept in a form "which permits identification of the data subject for no longer than is necessary for the purposes for which the data are processed"; if the data is to be kept longer, then further conditions apply (e);
- **integrity and confidentiality** – the data's processing must ensure appropriate security; it must be protected against unauthorized or unlawful processing, accidental loss, destruction or damage.

Paragraph 2 of the Article 5 also establishes the principle of **accountability** – according to which it is the data controller who is responsible for demonstrating compliance with Paragraph 1. The issue of accountability will be mentioned in point 5. later in this section. An in-depth description of the principles in the light of ENSURESEC shall be discussed under "Legal considerations" below.

1. *Lawfulness and fair processing*

According to the GDPR, processing is only **lawful** if and to the extent one of the legal basis below applies:

- the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- 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;
- processing is necessary for compliance with a legal obligation to which the controller is subject;
- processing is necessary in order to protect the vital interests of the data subject or of another natural person;

[57] Article 5(1) b of the GDPR

- 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;
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

For the purpose of this deliverable, the most important ones are the first and the second; consent or processing necessary for the performance of a contract to which the data subject is a party. The nature of consent will be discussed further below in this deliverable.

2. *Transparency and the right to information*

The questions of **transparency** of the processing are raised in the Articles 12-14 GDPR. Article 12 addresses the issues of **transparent** information, communication and modalities for the exercise of the rights of the data subject; Article 13 describes the information to be provided where personal data are collected from the data subject, and Article 14 indicates the information to be provided where personal data have not been obtained from the data subject.

In short, the Article 12 GDPR states that the controller must ensure that the communication with the data subject as well as the information provided to them is **concise**, **transparent**, **intelligible** and in an **easily accessible** form. The **language** used by the data controller must be **plain** and **clear**; the information must be provided in **writing** or by other means (e.g. electronic ones); it may be given in an oral way, providing the data subject's identity has been proven Article 12(1). They should **facilitate** the exercise of the rights of the data subjects, under Articles 15-22 (2) and provide the information **on request** without undue delay, under certain specific conditions (3) and inform the data subject if they do not take action on request, giving the reasons for this decision (4). The information shall be provided **free of charge** (5), unless the requests from the data subject seem "manifestly unfounded", excessive and/or repetitive. When in doubt about the data subject's identity, the controller may ask for further data to confirm the identity of the data subject (6), and so on.

According to Article 13 GDPR, if the personal data is collected from the subject, he/she are to be provided by the data controller with such **information** as the identity and contact details of the controller (1a), if applicable: the contact details of the data protection officer (1b), the purposes and the legal basis for the processing (1c), if applicable: the legitimate interest pursued either by the controller or a third party (1d), the recipient of the data, or the categories of the recipients (1e), or detailed specific information in the cases the controller intends to transfer the personal information abroad (1f).

In the cases when the personal data have not been obtained from its subject, Article 14 makes the data controller provide the subject with the following **information**:

- the identity and contact details of the controller (1a),
- if applicable: the contact details of the data protection officer (1b), the purposes and legal basis for the processing (1c),
- the categories of the personal data in question (1d),
- if applicable: the recipients or categories of recipients of the data (1e),
- detailed specific information if the data controller intends to transfer the data abroad (1f)

In order to ensure that the processing is **fair** and **transparent**, the controller is to provide the following data:

- the period for which the data is to be stored (2a),
- the legitimate interests pursued by the controller or a third party, if applicable (2b);
- the existence of the rights to get the access to, rectify or erase the data, restrict the processing, object to processing and the right to data portability (2c),
- the right to withdraw consent (2d)
- the right to lodge a complaint with the supervisory authority(2e).
- information about the sources from which the personal data originate and if the source is publicly available (2f)
- whether the data is subject to automated decision-making, including profiling (2g)
- if giving the personal data is part of a contract, or a statutory/contractual requirement (2e)
- whether the data subject is obliged to provide their personal data and what will happen if they do not do this.

The information should be given within a reasonable period after obtaining the data (but no longer than a month) (3a); if the data are to be used in order to communicate with the subject, it must happen at the latest at the first communication to that subject (3b). If a disclosure to a recipient is envisaged, the information must be given at the first instance of disclosure (3c). It is worth noting that the Paragraphs 1-4 do not apply if the data subject already possesses the information (5a), the provision of such information is not possible or involves a disproportionate effort (5b), the obtaining or disclosure has been expressly laid down by Union or Member State law (5c), or when the data must remain confidential subject to professional secrecy (regulated by Union or State Member law) (5d).

Natural persons need to be informed about risks related to the personal data processing. In addition, the principle of purpose limitation, storage limitation and other principles of the GDPR are important to ensure fairness and transparency.[58]

On the next page, a pictogram of processing of personal data has been included, to ease the comprehension of the concept.

[58] Recital 39 GDPR.

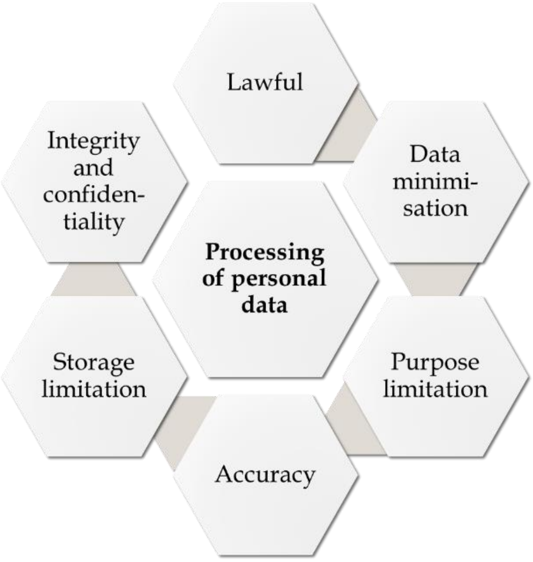

Figure 1 A visualization of the concept of processing of personal data

3. *Security, Integrity and Confidentiality*

Another relevant part of the Regulation is the Article 32, concerning the **security of processing**. It states that the controller and processor are obliged to implement the **measures** ensuring an appropriate level of **security**, taking into account the state of the art, the costs of implementing them, the purposes, context, scope and nature of processing, as well as the risks of varying severity and likelihood for the person's rights. This may include:

- **pseudonymization and encryption** of the data (1a),
- ability to ensure ongoing **confidentiality, integrity, availability** and **resilience** of the systems and services aimed at processing (1b),
- **availability to restore and access** the data in the event of an incident, either physical or technical (1c), and
- **testing, assessing and evaluating** the **effectiveness** of the measures ensuring the security (1d).

These measures are also important for ensuring integrity and confidentiality. The principle of integrity and confidentiality require that personal data will be processed with appropriate level of security. This includes the protection against unauthorized or unlawful processing, accidental loss, destruction or damages. This concerns both technical and organization measures.

Additionally, Paragraph 2 states it that the assessment of the level of security should take into account the risks that result from the processing, especially from **destruction** of data (either accidental or unlawful), as well as data **loss** and **alteration**, and unauthorized **disclosure** of, or **access** to the processed personal data. Finally, Paragraph 4 states that all the steps must be taken to ensure that any natural person acting under the authority of the controller or the processor does not process the data **except on instructions** from the controller, unless they are required to do so by Union or Member State law.

4. *Accountability*

The data controller's **accountability** has already been mentioned when discussing the data protection principles above. Further articles specify other duties that contribute to it. For instance, the data collector is obliged to **maintain a record** of all the activities done as part of the processing. Article 30, Paragraph 1 specifies that the said record must contain **pieces of information** such as the name/contact details of the controller/s (1a), the purpose of the processing (1b), the categories of data subjects and personal data (1c), the description of the ones the data will be disclosed to (1d), and if applicable: transfers of the data abroad, including the suitable safeguards (1e), the limits for erasure of the data (1f) as well as a description of security measures mentioned in the Article 32. If the actions have been carried out by a processor on behalf of the controller, they must keep a very similar record of the processing, including the contact details of the processors, controllers and data protection officers (2a). All the records that Paragraphs 1 and 2 refer to must be written and an electronic form included (3); the records must be **made available** to the supervisory authority **on request** (4). The obligations that Paragraphs 1 and 2 define do not apply in a few cases, e.g. in the organizations that employ fewer than 250 people (unless the data processing poses a high risk to the rights and freedoms of an individual), the processing cannot be called occasional, or when the processing includes data belonging to the special categories or the data relating to criminal convictions and offences (5).

As the responsibility of upholding the principles of the GDPR belongs to the data controller, it is important to identify, in every single case, which party *de facto* constitutes the controller under the GDPR. Accountability also comes with the responsibility to be able to demonstrate compliance with the principles and the legislation.

In order to ensure accountability, the EDPS highlights[59] measures including adequate documentation on what personal data are processed, how it is being processed, for which purpose and for how long. The controller shall also document processes and procedures which are intended to address data protection and privacy issues hands-on and in an early stage of the processing, and how it responds to data breaches and how it includes the Data Protection Officer of the company to participate in organizational planning and operations.

The principle is also closely connected to lawfulness, transparency and purpose limitation, since it requires transparency in demonstrating that the principles and the regulation as a whole is being implemented. When it comes to lawfulness, it requires accountability as concerns the legal basis for the processing, together with purpose limitation requiring that data is only processed for the purposed for which a legal basis exists. It should be noted that the principle also concerns data processors.

In a nutshell, accountability means that each partner which is engaged in processing of personal data, either as a controller or as a processor, shall be able to demonstrate compliance with the GDPR and also in which manner compliance is achieved. The European Commission stresses, that in cases where

[59] https://edps.europa.eu/data-protection/our-work/publications/speeches-articles/put-data-protection-accountability-practice_en and https://edps.europa.eu/data-protection/our-work/subjects/accountability_en .

a consortium in a H2020 project shares the responsibilities of processing personal data, the project might have a joint controllership. In such a situation, the partners must set out the respective responsibilities of the consortium in an agreement, which is available to data subjects. The data subject must also be provided with a single point of contact.60

5. *Accuracy*

Personal data being processed should be accurate. The data controller must also ensure that the data is kept up to date and that there is a possibility for the data subject to inspect the data, and to have the data rectified as needed. According to the requirements of the GDPR, 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.

6. *Data Minimisation*

One of the outstanding principles for the processing of personal data is data minimisation, introduced in Article 5(1), point c of the GDPR. It requires that personal data "adequate, relevant and limited to what us necessary in relation to the purpose".

Data minimisation aims to minimise the use of personal data processed all together by using technical opportunities to anonymise or otherwise turn personal data into non-personal data (not allowing identification or possibilities of identification of the data subject). Data minimisation is therefore closely linked to data protection by default and by design.

Data minimisation can be achieved with different technical solutions. One way of minimising the amount pf personal data, and thereby also adhere to the principles of the GDPR, is anonymising the data, and if not possible, by pseudonymisation. The use of the technique relates first hand to the definition of what constitutes personal data, as set out by the scope of the GDPR.

Whether or not data is considered to be personal data depends on the effectiveness of the pseudonymisation procedure. Consequently, retraceable pseudonymised data may constitute personal data and be subject to data protection legislation. The GDPR defines pseudonymisation as "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person"

7. *Purpose limitation*

In the previous sections, the basic actors of processing of personal data as well as the definition of what constitute processing and the scope of the GDPR has been explained. As has been discussed, processing of personal data need to be subject to a legal basis. The principle of lawfulness and purpose limitation are closely connected, since personal data can only be processed for the purposes it has been collected.

[60] European Commission, Ethics and data protection, H2020, p.5

The principle of purpose limitation is defined in Article 5(1) of the GDPR and substantiated in Article 24(1). Accordingly, "*personal data shall be collected for specific, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes*".

It is the responsibility of the controller to implement appropriate technical and organizational measures to ensure and to be able to demonstrate that the processing is performed in accordance with the GDPR. This responsibility shall be implemented taking into account the nature, scope, context and the purposes of processing.[61]

Therefore, as has been described above, the purpose of processing of personal data must be identified prior to the processing. The principle of purpose limitation in practice limits the data processing to these predefined purposes. This should also be taken into account when planning the future use potentials of the tools, especially when it comes to potential future exploitation of the data for further development of the tool for example. Processing for any other purpose, which has not been identified when the personal data was initially collected, will not be possible unless provided for by Union or Member State legislation.

Recital 50 of the GDPR provides clear guidance for factors to take into account when considering further use of collected personal data:

"*In order to ascertain whether a purpose of further processing is compatible with the purpose for which the personal data are initially collected, the controller, after having met all the requirements for the lawfulness of the original processing, should take into account, inter alia:* ***any link between those purposes and the purposes of the intended further processing****; the* ***context in which the personal data have been collected****, in particular the* ***reasonable expectations of data subjects*** *based on their relationship with the controller as to their further use; the* ***nature of the personal data****; the* ***consequences of the intended further processing for data subjects****; and the* ***existence of appropriate safeguard****s in both the original and intended further processing operations*."

8. *Storage limitation*

The principle of storage limitation entails that personal data can only be kept in a form, from which the data subject can be identified, for no longer than necessary. Exceptions exist for scientific and historical research, statistical purposes as well as reasons of public interest.

Hence, technical measures ensuring either deletion or anonymisation as soon as the storage is no longer necessary for the purposes for which it has been collected may help to meet this principle. Accordingly, data controller makes sure that there are possibilities to erase or anonymise personal data after that period has expired.

A simple example is an online purchase of goods. The data of the data subjects will be collected for purposes of fulfilling the contract, including delivery and a potential return period. After the delivery of the good has taken place and the return period is over, the personal data of the customer shall be

[61] Article 24(1) GDPR

either anonymized or erased, unless the data subject has consented (if consent is the legal basis for the processing) to data processing for other purposes, such as online marketing.

3.1.4. The rights of the data subject

When it comes to **the rights of the data subject**, they are regulated by the Articles 15-22, which are as follows:

- Article 15 – Right of access by the data subject,
- Article 16 – Right to rectification,
- Article 17 – Right to erasure ("Right to be forgotten"),
- Article 18 – Right to restriction of processing,
- Article 19 – Notification obligation regarding rectification or erasure of personal data or restriction of processing,
- Article 20 – Right to data portability,
- Article 21 – Right to object, and
- Article 22 – Automated individual decision-making, including profiling.
- Article 15 states it that the data subject has the **right** to have it confirmed whether the information concerning them is being processed or not (Paragraph 1).

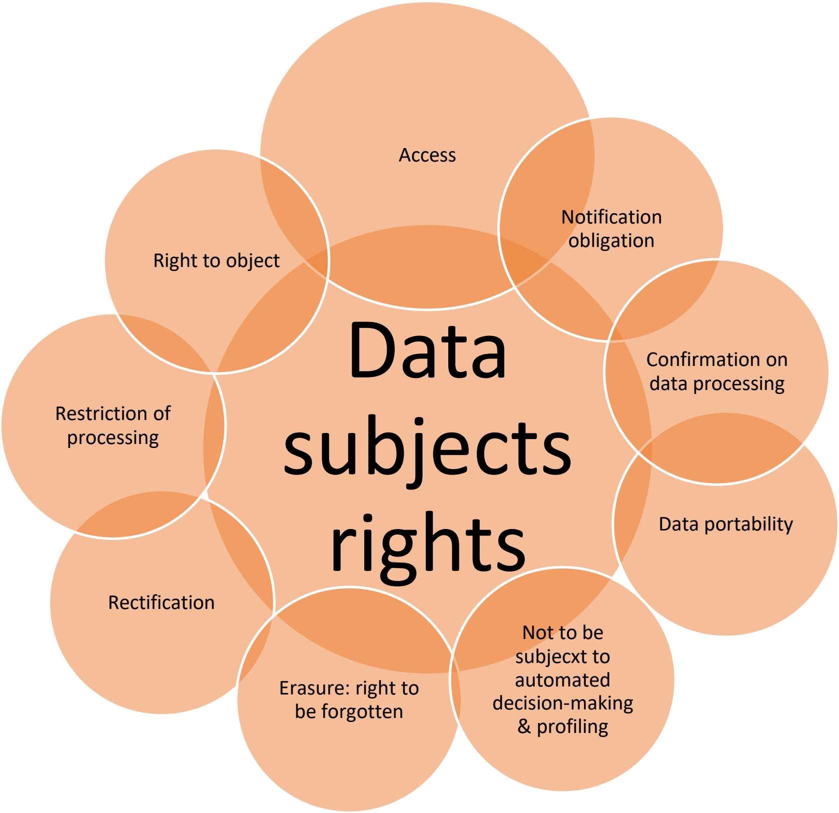
Access
Notification obligation
Right to object
Data subjects rights
Confirmation on data processing
Restriction of processing
Data portability
Rectification
Erasure: right to be forgotten
Not to be subjecxt to automated decision-making & profiling

Figure 2 An illustration of the rights of data subjects. Access to information about the data processing enables the exercise of many of the other rights.

If the personal data of a data subject is being processed, the data subject is entitled to **access** the data and be informed of the purpose of the processing, the categories of the data, who will receive the data and how long it will be stored (1a-g). If there are automated decision-making and profiling involved, the data subject also has the right to know the logic involved, the consequences of such processing and its significance (1g). It must also be mentioned that if there happens the transfer of personal data to an international organization or a third country, the data subject has the right to know which safeguards relating to the transfer have been ensured (Paragraph 2).

Article 16 gives the data subject the **right to rectify** inaccurate personal data concerning them, or to have incomplete data completed, all without undue delay.

Article 17 concerns the **right to erasure**, commonly known as "the right to be forgotten". The data subject has the right to demand their personal data being erased if, e.g. the data is no longer necessary (a), the data subject has withdrawn their consent and there is no other legal ground for processing (b), the data have been unlawfully processed (d), and so on. There are exceptions to this, which have been described in the Paragraph 3, i.e. the aforementioned erasure does not apply if the processing is essential to the exercising the right of freedom of expression and information (a), for compliance with legal obligation (b), if the public interest concerns public health (c), for archiving purposes in the public interest and for scientific purposes (d) and for the establishments, exercise or defence of legal claims (e).

The next article (Article 18) defines the **right to restriction of processing**; the data subject has it when the accuracy of the personal data is contested by the data subject (a), the processing has been unlawful but instead of the erasure, the data subject requests the restriction of their use (b), the controller does not need the data but the subject does; for the establishment, exercise or defence of legal claims c) or the data subject has objected to processing (d).

Under Article 19, the controller is obliged to **communicate** any instances of **rectification**, **erasure** or **restriction** of processing of personal data to the **data subject,** carried out in accordance with the aforementioned Articles 16-18, unless it is **impossible**, or the effort it involves is **disproportionate**.

Article 20 defines the **right to data portability**. It states that the data subject has the right to get the personal data that concerns them in a "structured, commonly used and machine-readable format". The Article also gives them the right to transmit the data to another controller, where certain conditions apply (a-b). However, the right should never affect the freedoms and right of others in a negative way.

Article 21 explains that the data subject has the **right to object** on grounds relating to their particular situation, including profiling based on those provisions. Unless the controller presents compelling legitimate grounds for the processing, which either overrides the interests, rights and freedoms of the data subject, or for establishing, exercising or defending legal claims, the controller is not able to process the personal data (1). If the personal data are processed for marketing purposes, the data subject has the right to object at any time of processing (including profiling) (2,3). If the data are processed for research or statistical purposes, the data subject may object to processing of the data concerning them, unless the processing is essential to the task carried out for reasons of public interest (4).

Finally, Article 22 states it that the data subject has the **right not to be subject to decisions** based solely on **automated processing** (profiling included), which yields legal effects on them or affects them in a similar, significant manner (1). This does not apply if the decision is essential to entering or performing the contract between the data subject and data controller (2a), is authorized by Union or Member State law (which also safeguard the data subject's rights and freedoms; also at least give the right to human intervention (also in Paragraph 3) (2b) or the data subject has expressed their explicit consent to the decision-making (2c). The decisions referred to in Paragraph 2 must not be based on special categories of data described in Article 9(1), unless the data subject's rights, freedom and legitimate interest are safeguarded (4).

3.1.5. Consent as a legal basis for processing personal data

The Regulation also attaches great significance to the question of data subject's **consent** and defines it in detail. Specifically, the issues are dealt with in Article 6. According to it, processing of the personal data is legal only if the data subject has given their specific, unambiguous consent to do so. It may be granted by various means, e.g. by opting to an e-mail list.

The rules concerning what constitutes consent are quite strict. First of all, it has to be "**freely given, specific, informed and unambiguous**". The request for it should be in "**clear and plain language**", as well as "**clearly distinguishable from the other matters**". The data subject's consent may be withdrawn whenever needed and the decision has to be honoured. In fact, "data subjects must be able to withdraw consent as easily as it was given"[62]. **Underage individuals** are able to give consent only if their parents agree. The Council Directive 93/13/EEC[63] has also defined it that the form of declaration of consent that the controller has pre-formulated should be **intelligible** and easily **accessible**, it must use **clear** and **plain language** and it cannot contain **unfair terms**. It should also be mentioned that informed consent includes the data subject being at least aware of the controller's **identity** and the **purposes** for collecting the personal data. Lastly, if the data subject had no free or genuine choice, or they are unable to withdraw consent without detriment, it is not regarded as given freely.[64]

If there is no explicit consent, for the data processing to be legal, it must be justified with one of the following legal bases:

a) the processing is **essential** for preparing or executing a **contract** with the data subject
b) the personal data has to be processed to comply with some **legal obligations** (e.g. based on an order from the court)
c) the processing is needed **to save a person's life**
d) the processing is part of carrying out **official functions** or performing a task in the **public interest**, or
e) the organization processing the data has a **legitimate interest** to do it.

For using point e), a Legitimate Interest Assessment (LIA) should be made. A LIA is not a concept explicitly mentioned by the GDPR, but serves as a risk assessment based on the specific context and circumstances of the processing. A LIA can be a good way to demonstrate that the use of legitimate interest is justified as a legal basis. As a part of the LIA, the fundamental rights and freedoms of the

[62] Lifely & Robertson, 2017
[63] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts (OJ L 95, 21.4.1993), 1993.
[64] Recital 42 of the GDPR.

data subject must be carefully considered in what is known as the balancing test and given priority over business-interests in unclear situations.

When the **lawful basis** for the data processing has been determined, it must be documented, and the data subject has to be notified. If the justification is to be changed later, it must be well-grounded, the new reason has to be documented, following the notifying the data subject again. Hence, personal data can only be processed for the purposes it has been collected. Consequently, the data subjects will need to consent to every purpose for which personal data will be processed. In order for the consent to be valid, the data subject shall have the possibility to separately consent (or not consent) to each purpose separately. The data subject also need to have a possibility to recall the consent.

Consent can be obtained by using different kinds of technical solutions, which also allows for demonstrating that consent has been retrieved on a later stage. It is the responsibility of the controller to be able to demonstrate that consent has been retrieved, and for which purposes. This is included in the principle of accountability. Noteworthy, the CJEU has ruled that pre-ticked boxes do not amount to valid consent.[65]

Natural persons need to be informed about risks related to the personal data processing. In addition, the principle of purpose limitation, storage limitation and other principles of the GDPR are important to ensure fairness and transparency.[66]

3.1.6. Special categories of information

Another crucial aspect to consider is whether the data in question does not belong to one of the **special categories of information**. These are also often referred to as *sensitive data.* Article 9 specifies it that it is prohibited to process the personal data that reveals one's "racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership". Furthermore, it is also prohibited to process "genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation" (Paragraph 1). There are ten exceptions to this, e.g. when the data subject might have given explicit consent to the processing (Paragraph 2, point 1), the processing is necessary for various purposes (2.2—4,6-10) or the data subject has made the data explicitly public.

In the context of ENSURESEC, as one of the use-cases concerns an online pharmacy, special attention should be paid to medical data. Under the GDPR, the definition of medical data is broad.[67] Recital 35 thereof specifies the definition of sensitive data in the field of health data in the following:

"*Personal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject*

[65] C-673/17 Planet49 GmbH ECLI:EU: 2019:18 and Recital 32 of GDPR.

[66] Recital 39 GDPR.

[67] As was also the case already under Directive 95/46/EC in C- 101/01 *Lindqvist*, para. 50.

[…]

and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test."

It should be noted, that doctor prescriptions[68], and therefore also the purchase of products which requires a prescription, should be considered as sensitive data and can only be processed with the data subjects' explicit consent. As concerns purchases of other medical products, which might not be prescribed by a doctor, or bought for self-care reasons, the situation is not as clear cut. As a guideline, if a conclusion about a person's health status can be drawn from the purchases of medical products, devices or services, the information should be treated as health data.[69]

This is the case especially when the purchases are combined with other information, such as previous purchases, gender of a person or other type of information which in combination with the purchase information can be considered sensitive. The purchase of some products could reveal more sensitive medical information, such as the purchase of pregnancy tests or products connected to sexual or mental health, or a combination of products which can lead to a conclusion about the health. Such an example could be where a person only buys paracetamol, it does not say much more about the person that he or she might get headaches every now and then. However, if he or she is also buying other products, such as nose sprays and pills for sore throat, it is easy to jump to the conclusion that the person has a cold, which is already clearly health data. Additionally, in cases where the data is transferred to third parties or if the data is combined with other information, it is also directly considered as sensitive.

In conclusion, personal data is health data firstly, when data clearly is medical data, such as doctors' prescriptions. Second, data is health data when the "raw data can be used itself or in combination with other data to draw a conclusion about the actual health status or health risk of a person"[70] or thirdly conclusions are draws irrespective of whether they are correct or not. This should be taken into account when considering whether e.g. the purchase of lifestyle products such as vitamins, can

[68] Opinion of the European Data Protection Supervisor on the proposal for a directive of the European Parliament and of the Council on the application of patients' rights in cross-border healthcare (2009/C 128/03), para. 15.

[69] ANNEX - health data in apps and devices, Annex to letter From WP29 to the European Commission, page 2, https://ec.europa.eu/justice/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf

[70] ANNEX - health data in apps and devices, Annex to letter From WP29 to the European Commission, page 5, https://ec.europa.eu/justice/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf

be considered health data and therefore also sensitive data. This will be further discussed under "*Legal considerations*".

3.1.7. Breach notifications

The GDPR introduces an obligation to notify personal data breaches. This obligation has been inspired by the personal data breach notification under the e-Privacy Directive.[71] Unlike the need to ensure a significant level of security as described above, the obligation to notify falls on the controller solely.

In case of a personal data breach, both the supervisory authority and the data subject shall be notified.[72] The time line for such a notification is as soon as the controller becomes aware of it, without undue delay, and if feasible, within 72 hours after having become aware of the breach.[73] However, the obligation is limited to a notification to the supervisory authority if the controller can demonstrate that the breach is "*unlikely to result in a risk to the rights and freedoms of natural persons*".[74]

Article 33 regulates the steps of **communication** with the **supervisory authority** that should be taken when a personal data **breach** occurs. In such a case, the controller is obliged to **notify the breach** to the supervisory authority "without undue delay" and no later than 72 hours after having become aware of it (if it is not made within 72 hours, the reasons for such a delay must be given), if it is feasible. This does not apply if the breach is not likely to pose risk to the rights and freedoms of natural persons (1).

The processor, after becoming aware of a personal data breach is obliged to notify the controller without undue delay (2). Paragraph 3 makes specifies what such notification should encompass: the **nature** of the breach (including categories and approximate numbers of data subjects and personal data records concerned, if possible (a)), **contact details** of the data protection officer or other source of further information on the incident (b), the likely **consequences** of the breach (c), the **measures** already **taken** (or proposed) in order to address the breach and mitigate its adverse effects (d). The breaches must be documented, along with their effects and remedial actions taken (5). If it is not possible to give the details of the incident at the same time, it must be provided in phases (4).

However, if it is likely that the breach will present a high risk to the rights and freedoms of natural persons, the data subject shall also be notified.[75]
Article 34 regulates the **communication of a breach** to the data subject. The incident must be communicated to the data subject without undue delay if it is likely to pose a **high risk** to the rights and freedoms of natural persons (1); the nature of the breach and its details (referred to in Article 33) must be described in clear and plain language (2). The communication is not required if: the controller has applied appropriate measures to the affected data to make it **unintelligible** (3a), the measures

[71] COM(2012)11, p. 10, Article 4(3) of the E-Privacy Directive 2002/58/EC.
[72] Article 33 respective 34 of the GDPR.
[73] Article 33(1) and Recital 85 of the GDPR.
[74] Article 33(1) and Recital 85 of the GDPR.
[75] Article 34 of the GDPR.

that ensure that the **risk** mentioned in (1) is **not likely to occur** (3b), or the effort the communication involves is **disproportionate**, in such a case the communication should be **made public** instead (3c).

A personal data breach is defined as "*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*".[76]

The definition is further specified in Recital 85:

"*A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned.*"

In this context, it is important to note that also the NIS Directive, which will be discussed below, obliges the data processor to notify security breaches and sets requirements for so called essential services. This will be discussed in the section concerning the NIS Directive.

Actors who do not comply with the security rules under GDPR, risks being subject to fines. [77] This concerns not only security measures, but adhering to data protection principles and other obligations under the GDPR as a whole.

3.1.8. Privacy Impact Assessment

The GDPR has introduced a significant tool for **privacy impact assessment** (PIA) or **data protection impact assessment** (DPIA), in the Article 35 of the Regulation. The data controller is obliged to conduct an assessment of the impact and have it documented, before the intended processing of data begins; the assessment may be bundled for multiple procedures. A DPIA is to be conducted whenever the processing might pose a **high risk** to the freedoms or rights of a natural person; some of the issues resulting in high risk are, for instance "profiling, automatic decisions which lead to legal consequences (…), systematic monitoring, processing of special personal data, data which is processed in a large scale, the merging or combining of data which was gathered by various processes, data about incapacitated persons or those with limited ability to act, use of newer technologies or biometric procedures, data transfer to countries outside the EU/EEC and data processing which hinders those involved in exercising their rights"(intersoft consulting, n.d.). A DPIA may not be absolutely essentials if only one of the criteria is fulfilled. If several criteria are met, the risk is thought to be high and the impact assessment is **necessary**, though. If it is **hard to determine** a high risk, or it raises **doubts**, the DPIA ought to be conducted anyway; it is advised to repeat the process every three years. Moreover,

[76] Article 4(12) of the GDPR.

[77] Huge fines, see for example https://www.cpdp.bg/index.php?p=news_view&aid=1519; https://www.bfdi.bund.de/DE/Infothek/Pressemitteilungen/2019/30_BfDIverhängtGeldbuße1u1.html; https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9256486; https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000038552658&fastReqId=119744754&fastPos=1.

the regulation makes the national supervisory authorities set and publish a list of processing activities that always need a DPIA in their jurisdiction (the so-called blacklist); they may also decide on the activities for which a PIA is not needed (whitelist). Whichever steps taken when conducting a DPIA, if there is a Data Protection Officer appointed, their opinion must be taken into account (intersoft consulting, n.d.).

3.1.9. Data protection by design and by default

Data protection by design is described as one of the added values of ENSURESEC and shall therefore also be introduced in this context. Data protection by design and by default is put forward in Article 25 of the GDPR. According to ENISA, with reference to Recital 78 of the GDPR, Article 25 of the GDPR has an indirect effect, meaning that it does not directly target "producers of products, services and applications".[78]

Article 25(1) states:

"*Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects*."

Hence, data protection by design concerns data controllers and should be kept in mind already at the beginning of the lifecycle of any activity that involves, or might involve, processing of personal data. It shall be implemented at the "*time of determination of the means for processing*" and "*at the time of the processing itself*".[79] It comprises both technical and organizational aspects and what the concept entails can be different under different circumstances, *"taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risks, likelihood and severity"*[80]. Based on every particular circumstance, the measures needed to reach data protection by design can vary. In summary, the requirements of the GDPR as concerns data protection by design requires build-in data protection principles identified in Article 5 of the GDPR, to ensure default settings which fulfil data protection requirements and focuses on the necessity requirement. Data protection by design is closely interlinked with the concept of data protection by default, which will be described next.

[78] ENISA 2018, page 14 and Recital 78 of the GDPR
[79] Both quotations from Article 25(1) GDPR.
[80] Article 25(1) GDPR.

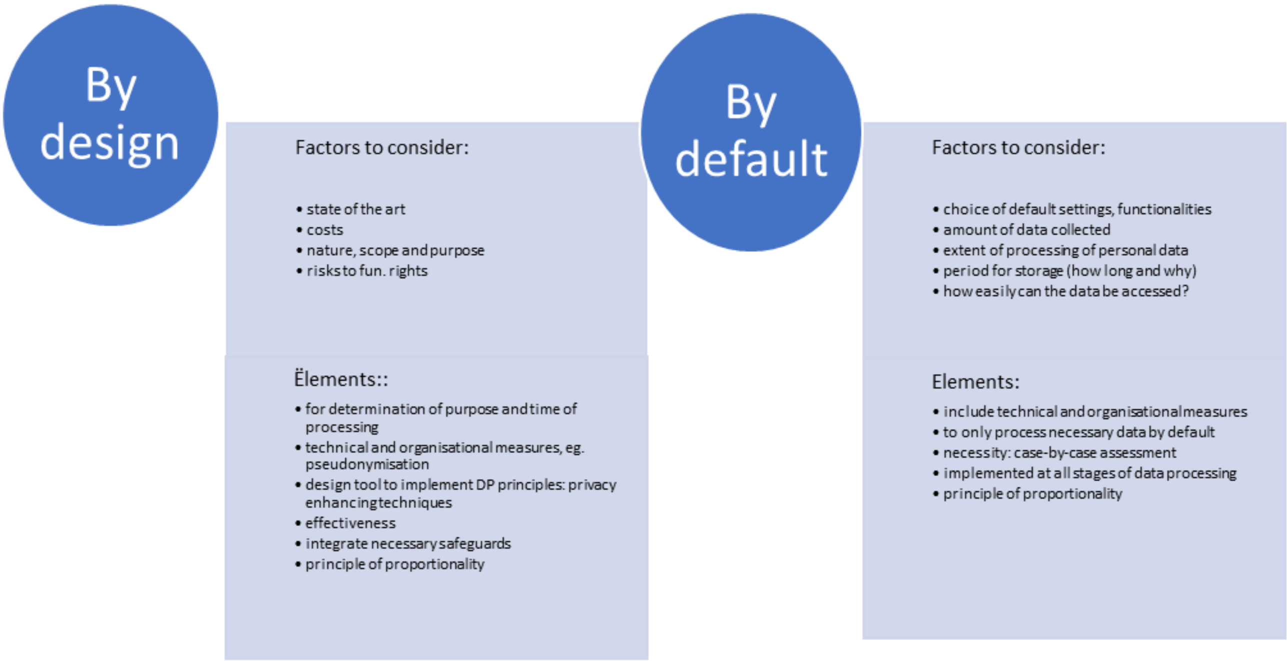
By design
Factors to consider:
• state of the art
• costs
• nature, scope and purpose
• risks to fun. rights
Ëlements::
• for determination of purpose and time of processing
• technical and organisational measures, eg. pseudonymisation
• design tool to implement DP principles: privacy enhancing techniques
• effectiveness
• integrate necessary safeguards
• principle of proportionality
By default
Factors to consider:
• choice of default settings, functionalities
• amount of data collected
• extent of processing of personal data
• period for storage (how long and why)
• how easily can the data be accessed?
Elements:
• include technical and organisational measures
• to only process necessary data by default
• necessity: case-by-case assessment
• implemented at all stages of data processing
• principle of proportionality

Figure 3 A comparison between data protection by design and by default. Both be implemented simultaneously.

Data protection by default is described in Article 25(2) of the GDPR, and includes the following elements.

Data protection by default means, that appropriate technical and organisational measures have been included, which makes sure that by default, only personal data which is necessary is processed. What is necessary depends on a case-by-case assessment for each processing purpose that has been identified. *These measures should comprise considerations on the amount of personal data collected, to which extent the personal data is processed, for which period it is stored and how easily the data can be accessed. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons*."

Data protection by default should be considered for the implementation of all stages of data processing – when deciding e.g. the extent of collecting, which data to process, how and for how long to store that data when implementing ways to access the data. In other words, it concerns the choices of default settings when implementing desired functionalities of IT systems or IT-based services.[81]

Article 25 of the GDPR is closely linked to the data protection principles defined in Article 5 of the GDPR. Of these, the principle of necessity together with the principle of purpose limitation as well as the principles of accountability are especially relevant. The principle of accountability indicates that the data controller shall be able to demonstrate compliance with GDPR. This also entails how the

[81] ENISA 2018, page 10

processing is designed and how and whether technical and organizational measures are being upheld and applied.[82]

Observance of data protection by default is a way to implement principles of the GDPR, especially the rule to limit data processing to what is necessary for its purpose, the principle of data minimization and storage limitation as a result of principle of purpose limitation.[83]

ENSURESEC claims to offer solutions which enhance data protection by design and by default. This added value is also in line with the GDPR. Therefore, the partners of the consortium as well as the project as a whole shall prioritize options which by their design and technical solutions and by default puts the data subjects and the principles of the GDPR in focus, including in particular necessity, purpose limitation and accountability.

In practice, data protection by default relates to four criteria, namely the minimum amount of personal data, the minimum extent of processing of the personal data, the minimum period of the storage of the personal data and minimum accessibility to the personal data.[84] From the point of view of the minimum amount of personal data, ENISA identifies the need to collect as little data as possible, and choose the data based on necessity. This can also be connected to the purpose of the processing, not all purposes having the same necessary minimum. The collection of the personal data should be adapted to what is necessary for each separate purpose. Further, the means of the processing must be proportionate to fulfil the purpose identified. In order to implement the principle of data minimization the use of privacy enhancing techniques can be of help, such as pseudonymization or encryption techniques. Further, ENISA recommends a minimized risk approach, where non-sensitive data is preferred over sensitive data or giving preference to anonymized data instead of pseudonymized data.

With concern to the minimum extent of processing of personal data, one outstanding recommendation is the use of tools which empowers the data subjects to realize their rights to information (rights enshrined in Article 12-20 of the GDPR.

As regards the storage period, the storage of the data should be connected to what is necessary, with the guidelines that the shorter the period, the better. This is also enshrined in the principle of storage limitation enshrined in Article 5 of the GDPR.

3.1.10. Data transfers to third countries

Transfer of personal data within the scope of the GDPR to partners outside the EU is subject to restrictions and conditions. According to Article 44 of the GDPR any transfer of personal data, which is being processed or intended to be processed after the transfer to a third country, can only be

[82] ENISA 2018, page 12.
[83] ENISA 2018, page 12.
[84] ENISA 2018, page 22.

pursued if the transfer fulfils the conditions set in the GDPR. These conditions are applicable both to data controller and to data processors.

Transfers can be lawful based on adequacy decisions[85], or in the absence of such decisions, based on appropriate safeguards and availability of enforcement of data subjects' rights[86]

The main option for lawful transfers of personal data outside of the EU is that the Commission has taken the decision that a third country ensures an adequate level of data protection ("adequacy decision"). In such a case, there is no need for specific authorisation.[87] So far the Commission has adopted adequacy decision for 12 countries, Serbia not being one of them.

In case no adequacy decision is available, data transfers to third countries can only take place if the controller or the processor transferring the data provides appropriate safeguards. GDPR presents a few options for how such appropriate safeguards can be provided:

a) Legally binding and enforceable instrument between public authorities
b) Binding Corporate Rules ("BCRs")
c) Standard data protection clauses and adopted/approved by a supervisory authority or by the Commission ("SCC's")
d) Approved codes of conduct
e) Approved certification mechanisms[88]
f) Contractual clauses between the controller or processor in the EU and the controller, processor or recipient of the personal data in the third country, approved by the competent supervisory authority applying the consistency mechanism set out in Art. 63 of the GDPR, or
g) Provisions in administrative agreements between public authorities/bodies.[89]

Further, enforceable data subjects rights and effective legal remedy for data subject must also be available.[90]

In other words, according to Article 46 of the GDPR, a controller or processor can only transfer personal data to third countries if it has i) provided appropriate safeguards via one of the listed options and ii) the data subjects rights are enforceable and effective legal remedies are available.[91]

For the purpose of ENSURESEC, the most relevant options are appropriate safeguards under SCC's as contractual clauses between the data controller in the EU and the data controller situated in the third country.

[85] Article 45 of the GDPR.
[86] Article 46 of the GDPR.
[87] Article 45(1) of the GDPR.
[88] Options listed in Article 46(2) GDPR.
[89] Options f) and g) listed in Article 46(3) GDPR.
[90] Article 46(1) GDPR.
[91] Article 46(1) of the GDPR.

The safeguards shall, in particular, ensure that the processing is carried out in a way which ensures the rights of the data subjects and that it is done in compliance with the EU data protection requirements.[92] This includes that the rights of the data subject need to be enforceable and that the data subject have access to effective legal remedies, such as effective administrative or judicial redress and possibility to claim compensation, either within the EU or in the third country. When assessing whether the data transfer allows for these rights to be observed, the general principles of personal data processing and data protection by design and default must be considered. This is important to ensure that the data subject can continue to enjoy the fundamental rights and safeguards.[93]

SCC's provide possibilities to third parties located outside the European Union where no adequacy decisions are available, provided that it allows data subject the same level of protection, oversight and access for data subjects, as would be the case under an adequacy decision. The clauses are available as templates, which have been approved by the European Commission.[94] At the moment, following the case *Schrems II*, the application of SCC's are uncertain. Since SCC's are merely contractual instruments, additional safeguards need to be taken at the use of SCC's and requires an assessment of the data protection legislation of the third country. According to *Schrems II*, it is for the controller/processor established in an EU Member State, together with the recipient in the third country of destination, to make a case-by-case assessment on if EU-level protection can be ensured. [95] Should this not be the case, they must take additional safeguards to ensure the protection.

Therefore, SCC's, as approved by the Commission, are as such still legally valid, but require that controllers and processors take appropriate safeguards for ensuring the rights of data subjects. Which exactly such appropriate safeguards are has not been defined. Scholars have identified these as compensating for any lack of equivalent level of data protection in a third country, and the safeguards would therefore depend on identified shortcomings in the level of protection.

The European Commission has, on the 12 November 2020, initiated a public consultation on new Draft implementing decision on standard contractual clauses.[96] The SCC's have therefore not been adopted yet by the Commission, but shows some direction.

EDPB has also set guidelines for what entails appropriate safeguards, which need to be ensured for transferring personal data to a third country. It provides that:

- Processing should be based on clear, precise and accessible rules
- Necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated
- An independent oversight mechanism should exist

[92] Recital 108 GDPR.
[93] Recital 114 GDPR.
[94] See https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en
[95] C-311/18 Facebook Ireland and Schrems, ECLI:EU:C:2020:556, para. 134.
[96] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Commission-Implementing-Decision-on-standard-contractual-clauses-for-the-transfer-of-personal-data-to-third-countries

- Effective remedies need to be available to the individual[97]

Contractual clauses would entail a legally binding document between the processor or controller situated in the EU and the one in the third country. These shall be approved by the supervisory authority of an EU Member State.

Additional guidance for transfers to third countries can be found in CJEU case law. The CJEU has developed case law, which provides that third countries shall ensure a level of privacy protection "essentially equivalent" to the EU level. This condition relates both to the level of data protection, the possibility for government agencies to access personal data and the data subjects' rights to redress. Consequently, the third country of destination, need to have a legal structure for the protection of data protection which is similar to that of the EU, even if it does not need to be identical. In practice, the assessment of what constitutes essentially equivalent is determined by looking at the Charter and the case law of the CJEU. [98]

3.2. ePrivacy Directive

For the purpose of ENSURESEC, the ePrivacy Directive[99] is also important to be mentioned. Together with GDPR, it provides the legal framework ensuring digital privacy within the EU

The ePrivacy Directive applies to services that consist wholly or mainly of the transfer of signals as opposed to e.g. provisions on content. It applies to electronic communications services (ECS) offering publicly available services and networks in the EU, over an electronic communications network.[100] Communication is defined as "a*ny information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service*"[101].

ENSURESEC is not a tool providing electronic communication services by itself. However, situations may arise when the ePrivacy Directive becomes relevant. Such a situation could be collect information or personal data via its web-page by using cookies. Further, the use-cases will benefit from the SONAE platform for e-commerce activities. SONAEs' e-commerce platform is concerned by the ePrivacy directive. Taking these two scenarios into account, the ePrivacy Directive need to be discussed.

The ePrivacy directive is considered *lex specialist* to the GDPR and extends not only to the protection of personal data, but also includes the protection of confidentiality in electronic communications both concerning the content of the communication and the metadata. This kind of data will often be

[97] EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, adopted 10.11.2020, page 8-9..

[98] Christopher Kuner, "Developments Reality and Illusion in EU Data Transfer Regulation Post Schrems" 18, no. 04 (2017): 38.2017, p.895.

[99] Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector, as amended in 2009.

[100] Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, 12 March 2019 p. 26, https://edpb.europa.eu/sites/edpb/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf

[101] Article 2(d) of the ePrivacy Directive.

personal data. It also applies to any communication using a publicly available electronic communication network. As a consequence, it is possible that some of the sharing of information which does not fall under GDPR, falls under the scope of application of the ePrivacy directive.

Article 5(3) and Article 13 of the ePrivacy Directive apply to providers of electronic communication services as well as website operators (e.g. for cookies) or other businesses (e.g. for direct marketing). Also, the use of cookies to create user profiles for advertising or market research purposes requires the users' explicit consent.

However, in 2017, European Commission adopted a proposal for a Regulation on Privacy and Electronic Communications[102]. The main innovation of the proposed legislation is that the scope would be extended to services such as Skype and WhatsApp. Nevertheless, the proposal has not yet been agreed within the EU between the European legislator, and therefore the legislation currently in force is the one from 2009. [103]

One of the proposed changes included in the proposal suggests a broader approach including "*the processing of electronic communications content data in transmission and of electronic communications metadata carried out in connection with the provision and the use of electronic communication services*"[104]. It is relevant to mention that if and when the European legislator passes the proposed regulation, the focus will concern the confidentiality of conversations and metadata through for example anonymization or deletion of this metadata (think about time and location of calls, and to limit tapping, intercepting, scanning or storing communications. There will also be new rules on cookies (making it easier to accept them for example) and spam.[105] At the time of this writing, the final version has not yet been adopted.

The development of the ePrivacy Directive will be closely followed in the context of Deliverable 1.6, 2.4 and will also be taken into account under task 8.5.

3.3. Directive on Security of Network and Information Systems

Directive 2016/1148 concerning measures for a high common level of security of network and information systems across the Union, also known as the Network and Information Systems Directive ("the NIS Directive")[106] establishes measures to achieve a common level of security of network and information systems as to improve the functioning of the internal market of the EU.

[102] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM(2017) 10 final.

[103] Status of the proposal can be followed: https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2017/0003(COD)&l=en

[104] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM(2017) 10 final., Art. 2.1(a)

[105] https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation

[106] 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
OJ L 194, 19.7.2016, p. 1.

The NIS Directive is divided into three parts, namely national capabilities, cross-border collaboration and national supervision of critical sectors. Member States need to ensure a certain level of national security capabilities. The NIS Directive lays down the collaboration within EU countries and lastly, Member States must supervise the cybersecurity of critical market operators, such as energy, transport, digital infrastructure and finance sector as well as supervision for critical digital service providers. The NIS Directive aims at minimum harmonisation allowing more stringent rules to be adopted at Member State level. Therefore, to ensure compliance with relevant legislation, the partners of ENSURESEC need to take into account the national legislation of the Member State where it is situated. This, however, falls outside the scope of this deliverable.

It should be noted that, when this instrument requires the processing of personal data, the data protection framework described above applies. Therefore, the NIS Directive needs to be read together with the security obligations under GDPR.

The directive introduces a security and incident notification obligations for operators of essential services (OES) and digital service providers (DSP). DSPs are online marketplaces (intermediaries, not regular stores), online search engines and cloud computing services. SMEs are normally excluded from the scope of the directive, unless it is a part of a larger organization or group (+50 staff or annual turnover +10 million).

The NIS Directive defines *network and information systems* as:

- An electronic communication network within the meaning of point(a) of Article 2 of Directive 2002/21/EC[107] ;
- Any device or group of interconnected or related devices, one of more of which, pursuant to a program, perform automatic processing of digital data; or
- Digital data stored, processed, retrieved or transmitted by elements covered under points (a) and (b) for the purpose of their operation, use, protection and maintenance.

In addition, the security of network and information systems is defined as the ability of these systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems.

This instrument mandates Member States to harmonise their national framework. In the context of DSPs, the following sectors are relevant:

- Online marketplaces;
- Online search engines; and
- Cloud computing services.

[107] Directive 2002/21/EC

On the other hand, OES are defined as operators providing services that are of crucial importance for the society or the economy of a country which is depending on a network and information system which, if affected by an incident would result in significant disruptive effects on the provision of the service.

Member States are required to maintain a list of the OES within their jurisdiction. To this end Articles 5 and 6 provide the criteria to help Member States to identify the OES. Moreover, the NIS Directive provides a list of entities to be regarded as OES. Of interest in this report is the inclusion of the banking sector identified as credit institutions as defined in point (1) of Article 4 of Regulation (EU) 575/2013.

If an entity falls under the scope of the NIS Directive, the following requirements are to be imposed Member States to comply with the Directive. In general, for both EOS and DSP:

- Take appropriate and proportionate technical and organisational measures to manage the risks, having regard with the state of the art;
- Take measures to prevent and minimise the impact of incidents with the aim to ensure the continuity of the service; and
- Notify the competent authority of incidents having a significant impact on the continuity of the essential service provided for EOS or a substantial impact for the provision of the service for DSO.

Article 1 of the NIS Directive on subject matter and scope lays down measures with a view to achieving a high common level of security of network and information systems within the Union so as to improve the functioning of the internal market. Keeping this in mind, the NIS Directive introduces an obligation for Member States to adopt a national strategy on security of networks and information systems. It is a directive of minimum harmonization, setting the minimum level of actions to be taken by Member States.[108] This means, that Member States can adopt a higher level of protection by setting stricter requirements in their national legislation. Additionally, Article 2 of the NIS Directive refers to the data protection framework of the EU. Therefore, for issues concerning data protection, the GDPR will apply.

The Directive establishes security and notification requirements for OES and DSP, which also partially overlap with the security breach notification of the GDPR mentioned above in 3.3.1.8.

Article 5 of the NIS Directive sets criteria for identifying operators of essential services. The criteria are the following:

- an entity provides a service which is essential for the maintenance of critical societal and/or economic activities;
- the provision of that service depends on network and information systems; and
- an incident would have significant disruptive effects on the provision of that service.[109]

It should also be noted that the NIS directive states several elements to be considered in the context of DSO, as to allow for less stringent requirement with respect to EOS. Concerning the appropriateness

[108] Article 3 of the NIS Directive.
[109] Article 5(2), point a – c.

and proportionality of the technical and organisational measures to manage risk the following elements should be considered:

- The security of systems and facilities;
- Incident handling;
- Business continuity management;
- Monitoring, auditing and testing; and
- Compliance with international standards.

NIS directive also provides the framework for determining if an incident has substantial impact – which will require the notification to the competent authority. These parameters are:

- The number of users affected by the incident;
- The duration of the incident;
- The geographical spread with regard to the area affected by the incident;
- The extent of the disruption of the functioning of the service; and
- The extent of the impact on economic and societal activities.

It should be noted that the operators do not have an obligation to inform the public as is the case concerning personal data breaches under the GDPR. However, if the security incident also includes a personal data breach, the notification requirements of both the GDPR and the NIS Directive apply. The result of this might be that a security notification to the supervisory authority, and in some situations also to the data subjects, would need to be done twice by the data controller

ENSURESEC should pay careful consideration of the parameters mandating the notification of security incidents within the part of the systems designed to share information. Further, under the NIS directive, it seems necessary to consider Caixa Bank as an operator of essential service which is relevant for the pilot scenario. Therefore, the obligations laid out above, such as risk management, take preventive measures and measures minimizing impacts of potential breaches as well as ensuring that a system concerning notification is in place is of essence. Lastly, national implementations of the NIS Directive should be considered when implementing the sociotechnical solution of ENSURESEC.

The NIS Directive has also been supported with the NIS Toolbox[110], which communicates and compares best practices concerning the implementation of the Directive. The Toolbox is important for interpretation and implementation of the Directive.

The NIS directive is under review, announced in the Work Programme of the European Commission in 2020. A public consultation ended at the beginning of October 2020.

[110] Communication from the Commission to the European Parliament and the Council Making the most of NIS – towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union, COM(2017) 476 final/1-2

3.4. The Cybersecurity Act

The Cybersecurity Act111 includes a permanent mandate for the European Union Agency for Cybersecurity ("ENISA") to ensure operational cooperation and crisis management and to support the implementation and development of the EU's Cybersecurity policy. ENISA also plays a key role in setting up and maintaining the new European Cybersecurity Certification Schemes (ECCS).
ECCS is intended to increase quality of EU products and services, containing different assurance levels (basic, substantial and high), where the basic level sometimes allow for self-assessment.

The schemes set out in the Act are optional for a period of probation of four years but it might be interesting to follow up which schemes will become mandatory.
The optional schemes created by ENISA under the Cybersecurity Act can be followed to indicate goodwill and add value to the project (e.g. if solutions can be adopted along existing certification schemes or standards; project solutions might even help in drafting those schemes or standards).

3.5. eCommerce Directive

The Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce in the internal market[112], also known as the e-commerce directive, harmonises national legislation of the Member States on certain aspects of e-commerce.[113] This instrument does not appear to be directly relevant to the activities carried out by ENSURESEC, as ENSURESEC does not engage directly in the e-commerce activities of the user of the tool, but provides for the security surrounding that e-commerce platform. It is therefore interesting to be aware of the types of regulatory requirements which the eCommerce actors are facing, in order to understand their products and their needs better.

First, the purpose of the Directive is to remove obstacles to cross-border online services within the internal market. Second, it seeks to remedy legal uncertainty related to such activities. The Directive promotes a flexible, technically neutral legal framework, and aims at enhancing the competitiveness of European service providers.

The e-commerce directive enables the abolition of prior authorization for the taking up and pursuit of the activity of an information society service ("ISS"). It is important to note that the instrument of the directive applies horizontally whenever a provision of an information society service is concerned. The notion of ISS includes a wide range of online activities such as:

- Online sellers of goods and services;

[111] 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.
[112] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, OJ L 178, 17.7.2000, p. 1.
[113] The e-commerce directive is also under review, and will be replaced by the Digital Services Act though the final version thereof has not yet been agreed by the European legislators.

- Information service providers; and
- Search engines.

Regarding the scope of application of the directive, it can be noted that the e-commerce directive does not apply to the data protection, taxation matters, and gambling activities.

Article 5 of the eCommerce Directive lays out the details on establishment and information requirements and general information which is to be provided in a way that is easily, directly and permanently accessible to the user of the e-service in question. The minimum information to be provided are the name of the service provider and the geographic address of its establishment, other details concerning the service provider, such as email address, in order to allow the user to contact the provider rapidly, directly and effectively. Further, for service providers which are registered in a public register, the registration number or equivalent shall be provided. Also, in situations where the activity of the service provider is subject to an authorization scheme, the details of the supervisory authority shall be accessible. Special requirements also exist for regulated professions and where the activities of the service provider are subject to VAT.

Article 6, on the other hand, concerns commercial communications in particular. Accordingly, additional requirements shall apply for commercial communications which are a part of or constitute information society services. Among other things, it sets requirements requiring clear identification of promotional offers such as discounts.

Article 9 enables electronic contracts by obliging the Member States to ensure that their national legislation allows for electronic contracts while not depriving the contract of its legal effectiveness and validity.

3.6. Importance of national legislation

It should be noted, that on the parts of this description which concern EU Directives, the EU requires each Member State to transpose the directive into national legislation. The directive sets the framework and level of protection, rights and obligations, but it is up to the Member States to decide how to put it into practice. Therefore, in each EU Member State, there is national legislation putting in place the directives described in this deliverable. Thus, there might be nuances in the means and ways of transposing the national legislation.

. A deeper research into the national legislations applicable to the partners of the consortium is outside the scope of this deliverable. Consequently, compliance with relevant national legislation shall be observed by the respective partners.

4. ENSURESEC -Ethical Requirements

4.1. Introduction

Ethical requirements play a vital role in projects funded in the framework of the H2020 program. Regulation 1291/2013[114] establishes Horizon 2020, the Framework Programme for Research and Innovation and highlights the importance of ethics throughout the EU research programme. More precisely, Article 19 clarifies the core ethical values that ought to be adhered to throughout the research activities funded under the H2020 initiative. It reads:

"1. All the research and innovation activities carried out under Horizon 2020 shall comply with ethical principles and relevant national, Union and international legislation, including the Charter of Fundamental Rights of the European Union and the European Convention on Human Rights and its supplementary protocols.

2. Particular attention shall be paid to the principle of proportionality, the right to privacy, the right to the protection of personal data, the right to the physical and mental integrity of a person, the right to non-discrimination and the need to ensure high levels of human health protection."

At first glance, this disposition appears to resolve the ethics of research projects in the compliance with relevant legislation at the international, EU and national level. Indeed, the respect for ethical principles is often accomplished by ensuring compliance with a given set of legal rules. However, the aforementioned norm contains an explicit – open – reference to *ethical principles*.

The purpose of this report is to clarify those principles in order to guide the development of ENSURESEC. One way of doing so is to look for ethical principles in the spirit of the fundamental legal sources of the EU order, which is appropriate. Yet, a growing part of the current ethics is found in expert opinions often requested by the Commission. On this basis, the first section of this report scouts for ethical principles across the various authoritative source – both legal and non-legal. The goal here is to lay out the unnamed ethical principles to which the Regulation 1291/2013 refers.

More ambitiously, this report aims to provide ethical requirements to inform the consortium of the good path toward a socio-technical solution for safeguarding the e-commerce component of the Digital Single Market. Accordingly, the following paragraphs are organized as follows:

First, section 4.2 briefly summarizes the sources in which the ethical principles might be found. It is worth to note that a more detailed report on such sources is found in deliverable 1.4. Further, the discussion will focus on ethical principles related to artificial intelligence. Lastly, the chapter will conclude the ethical discussion before proceeding to discuss the legal requirements.

[114] Regulation (EU) No 1291/2013 of the European Parliament and of the Council of 11 December 2013 establishing Horizon 2020 - the Framework Programme for Research and Innovation (2014-2020) and repealing Decision No 1982/2006/EC, OJ L 347, 20.12.2013, p. 104.

The ethics section describes the sources that contain the several ethical requirements that ought to guide the activities of the partners. First, it describes the international sources of law that contain the basic values of the European Communities before diving into more detail sources concerned with the ethics of particular areas.

International law provides the starting point to identify the overarching ethical principles that apply to ENSURESEC. While the principles discussed below are not easily transposed into operational requirements, it is necessary that the partners consider them carefully when carrying out the activities envisioned in the project. The ensuing paragraphs will deal with principles rather than with every single source. In addition, many of the sources touch upon the same topics and several relevant instruments can be considered the sources of moral obligations.

4.2. Ethics and the law

This section is intended to briefly describe the relationships between ethical requirements and legislation, and why attention should also be paid to the ethics, and not limit oneself to simply comply with legislation.

Firstly, this question concerns ENSURESEC, as a H2020 financed project. The European Commission stresses, that projects funded by the European Union, and especially by H2020, shall not only comply with relevant legislation, but also be guided by the ethical principles on which the EU is built.[115]

Further, law and ethical requirements are very closely related. What is legally allowed is not always considered ethically desirable and sometimes laws are not comprehensive enough. Ethics should be turned to when the law does not provide clear answers, which is often the case when it comes to new technology, which is not clearly regulated. When answers to these issues are not found in the law itself, we turn to ethics,[116] which are often translated by lawyers are standards of good care, fairness or equity.

Ethical requirements often set out the limits of the law, namely how much the law can be stretched into grey zones where the law does not supply a clear answer. This is especially the case for new and innovative technologies. As an example, as GDPR is technologically neutral, it will apply to all personal data processing activities. However, the concepts of the GDPR, such as controllership, are based on a centralized way of processing data. In such situations, it might be difficult to apply GDPR, so when doing so, ethics can provide guidance. In addition, paying attention to ethics can help to build trust and increase reliability, which is especially important for innovative technological solutions.

[115] European Commission, Ethics and data protection, H2020, p. 3, https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-data-protection_en.pdf, H2020 EC, p. 3.

[116] Van der Burg 2010, p. 23,

This is just one example of when ethics is necessary to be taken into account for ENSURESEC. The general principles of privacy and data protection as well as ethics for AI will be discussed in the following chapters.

4.3. General Principles

4.3.1. Privacy

The first relevant ethical principle is the protection of privacy. In its moral content, it entails to abstain from unnecessary, disproportionate, and illegitimate interference with a person's private life. This negative obligation extends to the family, the residence and communications of natural persons. The respect of the privacy of individuals is intimately linked to their autonomy. The absence of privacy produces so-called chilling effect that hampers self-determination and, ultimately, freedom of expression. The crucial role of this principle is made clear by its inclusion in prominent instruments.

The right to privacy is enshrined in the Universal Declaration of Human Rights of 1958 (hereafter The Declaration). There is a debate on the legal effect of The Declaration, some people arguing that it constitutes customary international law while others have doubts it has direct efficacy. Regardless of its legal status, it is significant from the purview of this section as it surely possesses a certain degree of moral authority. More precisely, Article 12 of The Declaration states that:

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

While the meaning of arbitrary interference is uncertain, it is possible to turn to other sources to delineate the moral scope of privacy. The European Convention of Human Rights (henceforth ECHR) is the first one. The ECHR is an international convention, as has been explained above, and is legally binding for states that adhere to the convention. The partners of the consortium are all established in states which are bound by the ECHR. The ECHR also establishes the European Court of Human Rights (known as the ECtHR) in Strasbourg. The disposition concerning privacy reads:

"1. Everyone has the right to respect for his private and family life, his home and his correspondence.

> *2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interest of national security, public safety or the economic well-being of the country for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."*

It is clear that the ECHR imposes more guarantees on the respect of the privacy of natural persons. Therefore, it is important to commit to the respect of the right to privacy of the individuals potentially involved in ENSURESEC as well as of the future users of the solution and of the relevant stakeholders. The prominence of the respect to privacy is further strengthened by Article 7 of the Charter of Fundamental Rights of The European Union (hereafter The Charter). The text under the rubric "Respect of private and family life" says:

Everyone has the right to respect for his or her private and family life, home and communications.

The change of the term correspondence to communication aims to reflect the technological developments, in particular in the field of ICT. This is of particular relevance in the context of the project as it concerns the implementation of a cybersecurity solution for the e-commerce. On this basis, partners should be aware of the moral need to respect the ethic behind the aforementioned provisions.

4.3.2. Data protection

In addition to the principle of privacy, the principle of data protection must be discussed. The principle of data protection is, as well as the principle of privacy, also enshrined in legislation, both on international, European and national legislation. The European Commission emphasizes the need to observe also data protection in research programs funded by the EU and the obligation to demonstrate compliance not only with legal obligations, but also with ethical requirements, all in accordance with the principle of accountability.[117] Especially mentioned are the mechanisms of data minimization, such as pseudonymization and automatization and the data protection by design and by default principles. The informed consent of the data subject is also crucial as is the importance of Data Protection Impact Assessments ("DPIA"). A DPIA will be carried out in task and deliverable 8.5. In the light of ENSURESEC, tracking, automated decision-making and big data, as well as data security is of great importance.

To start with, it is relevant to have a look at how to identify ethical issues that could become relevant to consider. The European Commission has listed factors, which could raise ethical concerns in connection to data protection. These can relate to the *type of data* (sensitive data about racial or ethnic origin, political opinions, religious or philosophical believes, genetic, biometric or health data, sex life or sexual orientation or trade union membership). The concerns can also be *related to the data subject directly*, such as vulnerable people or people who have not given their explicit consent.
Large-scale processing of personal data, systematic monitoring of public spaces or involvements of multiple datasets or combination and analysis of different datasets (big data) also raises concern for the rights of the data subjects.[118] Data-collection or processing techniques such as different privacy-invasive methods such as tracking raise the ethical risks. This is also the case for use of camera systems for monitoring of behaviour, use of artificial intelligence to analyse personal data or automated decision making. Transfer of personal data to countries outside the EU can also raise concerns.

If ethical concerns are identified, a detailed analysis shall be provided for the methodology and mitigation measures. For ENSURESEC, a detailed analysis and assessment will be made in D8.5, the DPIA.

[117] European Commission, Ethics and data protection, H2020, p. 3,

[118] European Commission, Ethics and data protection, p.6.

In order to minimize the data use, project partners should attempt to anonymise and pseudonymize the personal data as much as possible. One must consider carefully the cases where a need to retain the connection to the data subject, and why this is the case. Even for cases where the data subject can no longer be identified, ethical issues can still be present depending on the origin of the data or how it has been retained and the source of the datasets. The timing of the anonymization and the methods used, both technological and organizational, are important. The legal requirements connected to personal data and re-identification will be discussed in the legal section of this deliverable. In addition, data protection by design and by default is the best way to ensure both legal and ethical requirements – that is creating a system which from the beginning is privacy and data protection friendly. Measures to be included can be anonymization, pseudonymization, data minimization, applied cryptography and arrangements which empower data subjects to exercise their fundamental rights. A risk assessment considering the severity of the risks to the data subjects' rights should be the ground for deciding which methods to use, as well as the nature, scope, context and purposes of the processing. Always when possible, options enhancing data protection and privacy should be chosen.

Informed consent is identified as a corner stone of ethical research, according to the EC. Whenever personal data is collected from individuals, the data controller need to make sure that the data subject has understood the purpose of the research and the potential risks involved. For especially intrusive methods, such as geo-location, a specific informed consent process shall be implemented. The records demonstrating informed consent of the data subject shall be kept and the data subjects must be provided with detailed and clear information about the data processing, in an understandable and easily accessible form, using clear and plain language. These requirements apply to all data processing activities of the project. Before any potential changes in the data process is made, the data subjects must be informed thereof.

If the personal data collected for research purposes, e.g. for the development of the platform is used also for secondary use, ethical risks may arise. In the case questions concerning consent, transparency and privacy, rights and expectations of the data subjects are arising, the plan for mitigating the ethical issues must be provided.

Last but not least, the ethical issues in which profiling, automated decision-making and big data can result, need to be mentioned. If such methods are used, a detailed analysis of the ethical issues of the processing must be included in the methodology. This includes overviews of all planned data collection and processing, identification and analysis of the ethical issues connected to the processing. Finally, it should also be explained how the ethical challenges will be mitigated.

Data security is relevant for both ethical and legal concerns. In order to ensure the fundamental rights and freedoms of data subjects, the obligation to protect the data and ensure proper protection of the information is key. The higher the risk to the fundamental rights and freedoms is connected to the processing, the more safeguards needs to be taken. These risks are especially connected to the type of data involved as well as the risk for unauthorized access to, or disclosure, accidental deletion or destruction of the data. The risk should be evaluated case-by-case and for high-risk activities, a clear explanation of the mitigation of the risks needs to be laid out.

4.4. Principles for Artificial Intelligence

There are several definitions of AI stressing different elements of software-driven systems that exhibit 'intelligent' behaviour. The High-Level Expert group on Artificial Intelligence set up by the European Commission (AI HLEG) defined AI as:

"Artificial intelligence (AI) refers to systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals.
AI-based systems can be purely software-based, acting in the virtual world (e.g. voice assistants, image analysis software, search engines, speech and face recognition systems) or AI can be embedded in hardware devices (e.g. advanced robots, autonomous cars, drones or Internet of Things applications)."

.[119] ENSURESEC aims to combine two types of AI, namely formal methods and machine learning (ML). These techniques will be integrated into several components, such as the physical asset monitor (T5.4) and the AI-based incident monitor (T5.6). AI methods provide significant benefits for reaching the goal of ENSURESEC; however, they also create risks that ought to be mitigated. The purpose of this section is to discuss the risks of AI usage and the approach of the European Commission and of the European Parliament to mitigate those risks.

Many institutions, governments, NGOs and corporations have issued documents detailing the ethics of AI. The focus should be placed on the European approach to AI-related ethics. The issue lies in harnessing the benefits of AI in a way that respects fundamental values and puts human in the centre, an approach known as human-centric AI. Moreover, risks associated with so-called revenge effects and unintended consequences arise when the execution of AI systems unfolds in a complex environment and behaves in an unpredictable, non-deterministic way. Examples of undesirable outcomes of AI systems are many, ranging from misidentification of human faces to questionable tweets.

The relevant sources for the issue of ethical-AI are 168 of 2019 along with the documents produced by the HLEG on AI. The aforementioned sources describe the risks of AI systems and methods, which relate to:

- fundamental rights (including privacy, data protection, and non-discrimination);
- surveillance;
- safety;
- liability.

The EC makes it clear that AI is not an end-product in itself; rather, it is a tool. Therefore, an approach that upholds the fundamental values of European societies is needed. Against this backdrop, the two main pillars of the ethical AI strategy within the EU are:

- trustworthiness;
- human-centric AI.

[119] AI HLEG, Definition of AI, 2019, Ethics guidelines for trustworthy AI | Shaping Europe's digital future (europa.eu) .

Trustworthiness is the fundamental ambition of AI development, because confidence in AI applications can only be attained by a clear and comprehensive framework. According to the HLEG on AI, there are three components of trustworthy AI, namely:

- Lawfulness;
- Ethics;
- Robustness.

The ethical dimension entails that AI applications shall comply with all applicable laws and regulations, but also require AI systems to respect the four ethical imperatives identified by the HLEG as:

- Human autonomy;
- Prevention of harm;
- Fairness;
- Explicability.

Lastly, the third component of trustworthy AI, technical robustness, is closely linked to the principle of prevention of harm and requires the following, technical, attributes:

- Resilience to attack and security;
- Fall-back plan and general safety;
- Accuracy;
- Reliability and reproducibility.

The characteristics outlined above are the pillars of a trustworthy AI which implement a human-centric approach. The following section will apply both ethical and legal frameworks to ENSURESEC, and provide guidance on how to mitigate such challenges.

- Participation of humans
- Pay specific attention to power imbalance of employees of end user's organisations
- Relevant aspects for use cases
  - Sensitive data of the online pharmacy
  - Data related to MSPED
  - Employees involvement
  - Deceptive practice in research

The CoE's work on artificial intelligence should also be observed. CoE have noted that also the right to free expression, personal data protection, privacy and political freedoms can be affected by the developments of AI technologies due to opacity (the so called black box effect), complexity and unpredictability. These characteristics of AI might have consequences for the protection of these rights, protected by the ECHR.[120] It raises difficulties to verify compliance with rules as well as issues

[120] Council of Europe study DGI(2017)12 Algorithms and Human Rights, https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5

related to the effective enforcement of rules enshrined in European legislation, which seeks to protect these fundamental rights.

In addition, CoEs's Ad hoc Committee on Artificial Intelligence or CAHAI is developing a legal framework for development, design and application of artificial intelligence cased on the standards of human rights, democracy and the rule of law.

Until such a framework is adopted, the relevance of the ECHR and other conventions for ENSURESEC is limited to interpretation of existing legal frameworks. EU legislation, such as the GDPR, shall be interpreted in the light of the Charter of Fundamental Rights[121], but also of the ECHR.[122] This effect can provide much needed guidance on how to apply existing legal frameworks to emerging technologies. AI related features, such as algorithmic accountability are relatively new topics, and are not (yet) directly incorporated in directly applicable legislation, and this is a good example on when the interpretation must be done in the light of human rights.

[121] Charter of Fundamental Rights of the European Union, OJ C 202, 7.6.2016, p. 389.

[122] According to Article 52(3) of the Charter, those rights enshrined in the Charter that corresponds to rights of the ECHR, the meaning and the scope of those rights shall be the same as those guaranteed by the ECHR.

5. ENSURESEC: applying legal and ethical requirements

5.1. Preliminary considerations for ENSURESEC

In this Chapter, special attention will be paid to the considerations of the legal challenges that have been identified in the light of the relevant legal and ethical framework. The chapter will discuss the principles of the GDPR in the light of ENSURESEC and point towards matters which needs to be taken into account when developing ENSURESEC.

It is foreseen that personal data will be processed while developing the ENSURESEC tools intended to provide security to e-commerce services. The finalised ENSURESEC-tool will most likely also involve the processing of personal data. One practical example is coordination data for the purpose of tracking physical assets and protecting against theft. If combined with other data, such as data on who worked on a specific day, this data will be personal data in the form of location data delivery workers.

Another situation where personal data will clearly be processed is in the context of for the second use-case, where customer data of the customers of the online pharmacy will be processed in order to fulfil the purchase. In this case, the type of data processed and the legal basis therefore must be carefully considered. Since the case concerns a pharmacy, some of the personal data or combination of data may be medical and thus sensitive data, and therefore requires special attention.

It is also foreseen that algorithms and machine learning will be used for providing the tools of ENSURESEC. In such situations, attention should be paid to what data sets are being used to train the machine, and the ethics highlighted previously in this deliverable. Further, when it comes to the use of DLTs, it is recommended to implement the principle of data minimisation, in order to avoid storing personal data on the ledger and thereby make it more difficult to ensure the rights of data subjects.

These are a few examples of personal data which will be processed. The types of data will become more concrete as the project advances. In the next sections, the implementation of the main legal considerations and potential challenges will be discussed, before wrapping up in concluding remarks. The sections will discuss the legal problems and provide recommendations to mitigate the legal risks.

5.2. GDPR principles and ENSURESEC

When developing a project like ENSURESEC, it is imperative to take into consideration the data protection principles laid down by the GDPR already at the stage of creation. The project itself as well as the end product of ENSURESEC will need to comply with the relevant framework. However, these principles can provide some guidance on the implementation of the GDPR for ENSURESEC. The core of the principles has already been described in Chapter 3.1.1.3. This chapter will focus on the implications thereof to ENSURESEC.

5.2.1. Lawfulness, fairness and transparency

The GDPR requires that every processing of personal data has a legal basis. For the purpose of ENSURESEC, the most important options for a legal basis are consent or processing necessary for the performance of a contract to which the data subject is a party.

For ENSURESEC, the legal basis for the processing can be the consent of the data subject. The consent of the involved persons is especially important for the use-cases, since participation in research projects requires the consent of the participation, but also for other types of processing of personal data within the course of the project. In addition, mechanisms of consent of the data subjects will be integrated in the technical solutions of the ENSURESEC end-product to ensure compliance of the tools.

Consent can be obtained by using different kinds of technical solutions, which also allows for demonstrating that consent has been obtained on a later stage. It is the responsibility of the controller to be able to demonstrate that consent has been retrieved, and for which purposes. This is included in the principle of accountability.

The ENSURESEC technical solutions must include possibilities to retrieve clear and qualitative consent, as well as allowing data subjects to withdraw the consent at any time. Especially for technologies based on machine learning and distributed ledger technologies, withdrawing of the consent can become technically difficult. Therefore, these issues need to be taken into account already during the designing phase, to allow implementation of the legal requirements into technical solutions.

Further, personal data can only be processed for the purposes it has been collected. Therefore, the technical partners of ENSURESEC will need to include technical solutions for getting the consent, demonstrate consent and for the data subject to take back their consent. In addition, it is important that the measures for obtaining the consent, demonstrating it and allowing data subjects to take back the consent is available for each purpose of processing. Therefore, a terms of use of privacy policy with all the purposes listed and only one consent opportunity for all of the purposes is not sufficient, as it does not allow the data subject to opt-out. Further, a situation when the data subject is forced to consent to be allowed to use a webpage or a service, does not fulfil the criteria for consent. Additionally, any type of technical solution or privacy policy of ENSURESEC will need to be clear and understandable for the data subject and also provide options for the data subject.

For the use-cases, the legal basis for processing the personal data of the individuals involved need to be consent. For future reference, depending on how the ENSURESEC-tool is finally constructed, the use of other legal bases could also be possible. These can be that the processing is necessary for the performance of a contract to which the data subject is a party. This is the case for the ENSURESEC tool itself, whereas for the use-cases, explicit consent of the data subjects is preferred. When it comes to processing of potential sensitive personal data, processing can only be based on the explicit consent of the data subject. Further, for automated individual decision-making, including profiling, explicit consent can also be used to ensure the lawfulness of the processing. In such cases, suitable safeguards need to be taken, such as the right of the data subject to obtain human intervention on the part of the controller in order to express his or her point of view, and to contest the decision. Guidance on the suitable legal basis for different types of processing can be found in the table below.

Type of processing	Suitable legal basis	Additional measures
Processing for H2020 research, components of ENSURESEC, such as use-cases	Consent	Take into account also H2020 ethics
Use of ENSURESEC security tool (once finalised product)	Performance of a contract and/or consent	All below, depending on the final outcome
Sensitive data, Location data	Explicit consent	Data subject's awareness of risk of processing
Automated individual decision-making (profiling)	Explicit consent	Suitable safe-guards for upholding fundamental rights of data subject, Data subject's awareness of risk of processing
Machine learning tools	Explicit consent	Data subject's awareness of risk of processing

Figure 4 The table illustrates types of processing and legal bases and additional measures as guidance for the design of ENSURESEC

To meet the requirements of fairness and transparency, ENSURESEC shall include measures for the right to transparent information, meaning that the data subject shall have the possibility to receive concise, transparent, intelligible information in an easily accessible form. The language used need to be clear and plain. It shall be provided in written, or where appropriate, by electronic means or orally upon request of the data subject. Further, the data subject need to have a possibility to get information on the identity of the controller and the purpose of the processing and other information needed to make sure that the data subject can access information about the processing and communicate with the controller.

Natural persons need to be informed about risks related to the personal data processing. In addition, the principle of purpose limitation, storage limitation and other principles of GDPR are important to ensure fairness and transparency.[123]

5.2.2. Purpose limitation

The principle of purpose limitation sets the limits for the use of the data processed for ENSURESEC. The purpose of processing must be identified prior to the processing and communicated to the data subject.

To enable this, a detailed planning considering the purposes and the desired functionalities of ENSURESEC in an early stage is mandatory. Any wish to process or use the data for other purposes than has been identified necessary for the ENSURESEC-tool's core-activities, such as marketing, further development of the tool etc, must be identified already at the planning stage of the process. Processing for any other purpose, which has not been identified when the personal data was initially

[123] Recital 39 GDPR.

collected, will not be possible unless informing the data subjects thereof and possibly obtaining the consent of the data subjects also for that purpose.

The data subject must have the opportunity to consent (or not consent) to each of the purpose separately. This sets requirements for the way the partners collect the consent of the data subjects. The purposes need to be laid out clearly, and no data processing should be executed for other than the communicated purposes.

5.2.1. Data Minimisation

For ENSURESEC, data minimization is closely connected with data protection by design and by default, and should be treated with special attention.

The first step is to make sure, that the innovation is based on personal data as little as possible. Hence, personal data should be minimised in every possible way and only used when absolutely necessary, and when there are no alternatives. Data protection-friendly solutions should always be prioritised. This principle will materialise in many different ways in practice.

First, it needs to be considered at the stage of the planning and of the development of the tool, that it involves as low personal data amounts as possible. For this, the definition of what constitutes personal data is essential. Data which does not allow identification or identifiability of persons does not constitute personal data, and therefore, every technical measure which diminishes or if possible eliminates the identifiability are also measures of data minimisation.

One effective tool for this is anonymization of the data. Second, where personal data is used, technical and operational measures need to be taken to ensure sufficient protection of the rights of the data subjects. Pseudonymisation, encryption and restricted access are important tools for this purpose.

When it comes to the use of distributed ledger technologies, it is recommended to not store personal data on the ledger, if possible.

5.2.2. Accuracy

Personal data being processed should be accurate. In order to keep the data accurate, the data controller need to ensure that the data is kept up to date and that there is a possibility for the data subject to inspect the data, and to have the data rectified as needed. According to the requirements of the GDPR, every reasonable step must be executed to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

Therefore, the partners of ENSURESEC shall ensure technical possibilities to allow data subjects to inspect the personal data being processed and to have it rectified or erased when appropriate.

5.2.3. Storage limitation

The principle of storage limitation entails that personal data can only be kept in a form, from which the data subject can be identified, for what is necessary. Hence, ENSURESEC shall include technical and organizational measures ensuring either deletion or anonymization as soon as the storage is no longer necessary for the purposes for which it has been collected.

A simple example is an online purchase of goods. Personal data will be collected for purposes of fulfilling the contract, including delivery and a potential return period. After the delivery of the good was realised and the return period was closed, the personal data of the customer shall be either anonymized or erased, unless the data subject has consented (if consent is the legal basis for the processing) to data processing for other purposes, such as online marketing.

The principle of storage limitation should be incorporated in the ENSURESEC technical solutions already at the point of design and planning. ENSURESEC partners need to ensure that there are technical and organizational possibilities to protect the principle – to ensure deletion or anonymization of the personal data once it is no longer necessary for the purposes for which they have been collected.

5.2.4. Integrity and confidentiality – ways to implement security requirements

Keeping the wording of GDPR in mind, it is important for the partners of ENSURESEC that the security of personal data is ensured. This is also complementary to the principle of data minimization and data protection by design and by default. If less personal data is being processed in the first place, the security risks linked thereto will also be minimized.

Therefore, this should be the starting point of any activity of ENSURESEC, and to be complemented with integrity and confidentiality through security measures for the personal data which is deemed necessary to process for the purposes of ENSURESEC.

5.2.5. Accountability – data controllers and processors

It is the responsibility of the data controller to uphold the principles of the GDPR. Therefore, it is important to identify, in every single case, which party *de facto* constitutes the controller under GDPR. Accountability comes with the responsibility to be able to demonstrate compliance with the principles and the legislation.

For ENSURESEC, it is important to establish who is the data controller, in accordance with the principles laid out in the description of the legislation in this deliverable. Further, the partners need to take technical and organizational measures to be able to demonstrate that the innovations effectively comply with the relevant the GDPR. Recommended measures includes:

- adequate documentation including which personal data are processed,
- how the personal data is being processed,
- for which purpose the processing is carried out,
- for how long the personal data is processed

The controller shall also document processes and procedures which are intended to address data protection and privacy issues actively at an early stage of the processing. , and how it:

- responds to data breaches and
- includes the Data Protection Officer of the company to participate in organizational planning and operations.

In a nutshell, for ENSURESEC accountability means that each partner which is engaged in processing of personal data, either as a controller or as a processor, shall be able to demonstrate compliance with GDPR and how compliance is achieved. The European Commission requests that in cases where the consortium shares the responsibilities of processing personal data, the project might have a joint controllership. In such a situation, the partners must set out the respective responsibilities of the consortium in an agreement, which is available to data subjects. The data subject must also be provided with a single point of contact.[124]

5.3. Particular considerations for use cases

This chapter will focus on particular concerns connected to the use cases. The use cases should comply with the principles of GDPR and other relevant legislation, as well as the H2020 requirements. Additionally, a few issues have been identified as needing some special attention. In this section, general requirements applicable to all the use-cases will be described. Below, particular aspects of each use-case will be discussed.

It is important that the participants taking part in the use-cases, both businesses and private persons have given their explicit and informed **consent**. Especially important is informing the data subjects of the risks involved with the use-case and the mitigating efforts made to limit the effects. The use-case will most likely also process personal data, including sensitive personal data such as passwords and usernames. For this, sub-section 3.1.6 of 3.1 Special categories of information need to be observed.

Even with the consent of the participants of the use-case, some aspects need to be taken into account. The use-case need to have a **plan** designed previous to the use-case concerning which data that will be processed, how personal data will be managed in accordance with the relevant legislations and how to ensure that no personal data is processed for other purposes than that the data subject has agreed to and how to dispose of the personal data safely after the use-case has been finalised. Such a plan will also help to provide the data subject with sufficient information, and to attend to the obligations under the GDPR.

There are also ethical aspects of carrying out use-cases with personal data. As a first resort, as little personal data should be used, and where possible encrypted, anonymized and pseudonymised. More information about the ethical aspects can be found in the Ethics section 4.3 General Principles.

5.3.1. Sensitive data

As has been discussed above, GDPR forbids the processing of sensitive data, as a main principle. Sensitive data can, however, be processed with the explicit consent of the data subject. As has also been mentioned above, health data is considered sensitive data under GDPR.

In the case of ENSURESEC, the use of sensitive data in the form of online purchase of medical products is relevant for use case 2. The concept of sensitive data and health related data are subject to a broad interpretation.

[124] European Commission, Ethics and data protection, H2020, p.5

The preparation of the use-cases need to include an assessment on which data will be used for the use-cases, and in particular which personal data will be involved.

When considering the sensitivity of the data, attention should be paid to the type of data, and if the data will be combined with other data or transferred to other partners of the consortium. This is important, since seemingly non-sensitive data may become health and hence also sensitive, data in combination with other types of data.[125]

The collection of sensitive data should be minimized. As is the case for all processing of personal data, sensitive data should only be processed, stored or transferred to the extent which is necessary for achieving the purpose of the processing. Further, processing of sensitive data requires the explicit consent of the data subject.

Relevant mitigation of risks need to be involved already at the planning stage. The planning of the use case should keep data protection by default and design in mind and give priority to, firstly non-personal data, and secondly, non-sensitive data rather than sensitive data.

5.3.2. Use-case 1: Cyber-attacks on e-commerce platform

Use-case 1 aims to target the increasing number of personal data breaches relating to online systems and the exploitation of the collected data and to show how ENSURESEC provides protection to the companies which are a part of the SONAE group and to their clients. Relevant regulation guiding the use-case and SONAE's platform is the ePrivacy directive, the GDPR and the NIS Directive. All of these are described above in section 3 of this deliverable.

Other than the legal and ethical requirements discussed previously in this deliverable, a few elements should be discussed paying special attention to use-case 1. Most importantly, any participant must explicitly consent to taking part in the use-case, after having been thoroughly informed about the use-case, the risks connected to the use-case and the mitigation measures. This also includes mapping the risks involved and setting up a plan on how to mitigate them. Also, where employees of companies take part in the use-cases, it is vital for fulfilling the ethical requirements, that the employer clearly states that the participation is voluntary, and that no negative consequences will follow for not wishing to participate or by dropping out in the middle of the use-case.

The use-case is at the intersection of three cornerstones of legislation, namely the NIS Directive, the GDPR and the ePrivacy framework. It uses the e-commerce platform provided by SONAE, which collects and/or processes personal data in connection with electronic communication services (GDPR and ePrivacy), and provides either essential or digital services (NIS). Therefore, the descriptions of the legislation above in section 3. ENSURESEC - Legal Requirements should be taken into account.

The use-case foresees to target phishing of clients' personal data, monetary information and shopping profile in order to obtain sensitive information, like financial credits. The scenario foresees a data

[125] ANNEX - health data in apps and devices, Annex to letter From WP29 to the European Commission, page 3, https://ec.europa.eu/justice/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf

breach as a result. Scenario 1.2 includes a cyber-attack with physical impact, where a client profile is used to enable the theft of purchased goods and stage a successfully completed transaction, where the good ends up in the hands of the person causing the attack.

In this case, it is particularly important to ensure that the data subjects involved are properly informed and have consented to the participation in the use-case. Therefore, staging attacks without the knowledge of data subjects is not recommended. Additionally, a plan for mitigation of risks need to be developed.

5.3.3. Use-case 2: Physical attacks on pharmacy e-commerce operator

In particular, for ENSURESEC, the use of sensitive data shall be observed in use case 2. The use case involves an online pharmacy and a partner ensuring the logistics of the delivery of ordered products. As a first step, it is important to minimize the amount of data, and in particular also sensitive data, used. This is in line with the principles of data minimization and data protection by design and by default. For the sensitive data which is identified as necessary to process, the explicit consent of the data subject is necessary. As a practical example, for a person purchasing bandage online, the data controller should not ask for their height, as this is simply irrelevant.

The planning of the use case should keep data protection by default and design in mind and give priority to, firstly non-personal data, and secondly, non-sensitive data rather than sensitive data. One option could be to limit the use case to purchase data from the online pharmacy to less sensitive products, such as skincare or other types of products which are less sensitive. This would minimise the risks of including personal data which are automatically considered as sensitive, such as sexual and reproductive health or medical conditions. Further, it is vital to ensure mechanisms to retrieve, to demonstrate and to withdraw the explicit consent of the data subjects.

5.3.3.1. Personal data transfers to third country

GDPR sets certain requirements for transferring personal data to third (non-EU) countries. This has been discussed in the section on secondary legislation. In order for a transfer to a third country to be lawful, the transfer needs to be based on a Commission adequacy decision, or that appropriate safeguards have been taken for the protection of the personal data.

Since ENSURESEC has one partner established outside the EU, namely in Serbia, and there is no adequacy decision between the EU and Serbia, the interesting options for ENSURESEC are to take appropriate safeguards in the form of SCC's or contractual clauses between the controller or processor in the EU and the controller of the personal data in the third country, approved by the competent supervisory authority applying the consistency mechanism set out in Art. 63 of the GDPR.

For the transfer of the data, it will need to be determined if MSPED will be the data controller outside the EU and who is the transferring party within the EU. This is important, since both SCC's and contractual clauses depend on both parties inside and outside the EU commit, in written, to the data protection level.

As a first step, the consortium and the involved parties need to determine the *purpose* of the transfer. That purpose is probably related to the transport of the products bought via an online platform. For this deliverable and for ENSURESEC as a whole, the scope should be limited to transport within the European Union, as the territorial scope of the GDPR protects data subjects within the EU.

Second, the partners will need to make the assessment on which personal data is *necessary* to process to fulfil the purpose of the processing – e.g. name and address of the buyer, in order to deliver the purchased products. The data transferred outside the EU should be kept to a minimum.

Considering the option of SCC's, a transfer requires a careful consideration of the essential equivalence of the level of protection in the third country. The Serbian data protection legislation is similar to that of the GDPR, but as the CJEU has been very strict on third country transfer, a detailed analysis will need to be made. As the CJEU has stated, additional safeguards will need to be put in place in order to ensure the rights of the data subjects when SCC's are used. The level of data protection in Serbia will need to be looked into and based on discrepancies with the level of data protection of the EU, the additional safeguards could be identified.

If the mechanism of contractual clauses is sought, the contract will need to be approved by the competent supervisory authority of the EU member state where the transferring party (the controller in the EU) is having its seat. Contractual clauses would entail a legally binding document between the partners situated in the EU and outside (the transferring and the receiving party).

Use-case 2 concerns an online pharmacy situated in Greece (TOFAR) and the transport organisation MSPED, registered in Serbia, the above should be noted. Particular attention will also need to be made when designing the use-case. The transferred data outside the EU should be minimised, and if possible, process data only in the EU. Further, the use-case should only focus on customers which are situated in the EU, as this corresponds to the scope of European legislation. For any transfer of personal data to Serbia, the above should be noted and implemented.

5.3.3.2. Monitoring location data of transport

Monitoring of individuals come with certain remarks. Location and GPS-data is a form of personal data, which can become very invasive depending on how it is used.

This is important to note for use-case 2. To ensure security of the transported goods, tracking of a vehicle carrying the products is foreseen. This transport will be carried out by a driver of the transport vehicle. The geographical tracking of the vehicle therefore also involves the potential tracking of a person, namely the employee of the logistic company. It is assumed that the tracking would be used for security purposes and in order to ensure a good service and traceability of the good being transported. However, the security of the transported good need to be balanced against the need to protect the personal data of the employee or the person driving the vehicle.

First, it should be considered how this data can be minimised. For example, real-time monitoring of every move is most likely excessive. As an alternative, the location of the vehicle could be pinpointed on a regular basis, for example once an hour. This would allow for having a good picture of whereabouts the vehicle is, without compromising the data protection of the driver too much. Also other ways to minimise the data collected can and should be considered, such as encryption of the data, by restricting access to the data only to those necessary and pseudonymisation. These option need to be considered already at the state of design of the innovation, in order to provide data protection by design and default.

Second, another important measure which will limit the amount of personal data involved is ensuring not to cross the data with other types of data, such as work schedules, or vehicles that are always driven by the same driver and can thereby identify the individual driving. Pseudonymisation can also help to make the identification of a person less likely. Which measures is deemed suitable depends on the technical implementation of the innovation. These measures are not only proposed as limiting person data issues, but also security issues for both the information, but also for the goods being transported.

It should be noted, that within the frame of ENSURESEC, GDPR must be adhered to at all times, also when the data subject might be outside the EU. This is the case since it also adheres to the H2020 rules.

5.3.4. Use-case 3: Cascading cyber-physical attacks on e-commerce platform for SMEs

This use-case involves a cascading cyber-physical attack, stress-testing the resilience of SME's employees to cyber-attacks by using cyber-security assessments. As a part of the scenario the following is described as follows: "A promotional email, a social media advert of a twitter post is sent to the employee with a goal of 'catching' him/her such that malware can be installed on employee's machine to steal the user's data".

Since this involves employees as human beings, it is important to note that the employee need to be informed of the testing going on and have consented to it. It is understandable that this might destroy the surprise effect intended by such a test. However, these are important ethical principles, which needs to be covered for. The testing could be designed to ask for volunteers, inform them about the content, the effects, the means and the risks connected to the use-case, and set a time period during which it is carried out. Other mitigating measures include thorough anonymization of the employees.

It is also important to consider the data protection and privacy rights of the employees, especially when it comes to monitoring.

Additionally, the same aspects as has been described for the other use-cases concerning consent, use of sensitive data and planning for mitigating the effects of the use-case also applies to use-case

5.4. Legal considerations of innovative technologies

5.4.1. Artificial Intelligence as an innovative technology

Artificial Intelligence or AI has already been discussed in this deliverable in 4.4 Principles for Artificial Intelligence. This section aims to discuss AI in the light of the relevant legislation, mainly fundamental rights and GDPR. Nevertheless, it should be kept in mind that ethics and law often go hand in hand and one is not isolated from the other. At the moment of writing this deliverable, there is no *lex specialist* at EU level targeting specifically artificial intelligence technologies. As it is foreseen that ENSURESEC will make use of AI (through use of machine learning and distributed ledger technologies), it is necessary to discuss the existing legal framework and its implications to ENSURESEC. The chapter will take on the most pressing requirements of the legislative framework as regards the applicability and adaptability to AI technologies. However, first a discussion with regards to fundamental rights is appropriate.

Before entering into this discussion, it should be noted that the European Commission is working on drawing up a legal framework on AI, with a first proposal to be expected early 2021. The problem definition and an assessment on the possible adjustments to existing EU legislation concerning AI were identified in the Commission White Paper on Artificial Intelligence.[126] It is likely that the proposal will be recognising AI-systems with different levels of risk assessment[127] and includes some kind of liability scheme[128].

Nevertheless, the legislation will most likely not become applicable during the lifespan of ENSURESEC. Even so, the development must be closely followed in order to take it into account as much as possible so that ENSURESEC remains competitive also after such legislation is introduced. Therefore, one needs to consider the current legislation and apply it in light of the purposes and activities of ENSURESEC.

Until any further framework is achieved, the European Commission points towards European legislation on fundamental rights, consumer protection and product safety and liability legislation.[129] The EC also acknowledges, that some of the features of AI render the application and enforcement more challenging.

It should be noted, that ENSURESEC is already subject to EU legislation on fundamental rights, which aside from data protection also comprises non-discrimination, consumer protection and liability rules. When it comes to AI, especially important is taking note of the fundamental rights described herein. Special attention should be paid to the right to privacy and data protection and the principle of proportionality, necessity and purpose limitation as well as the data protection and security framework. The European Commission also identifies fundamental rights related issues on data protection and privacy, safety (including cybersecurity) and liability issues as the most central risks connected to AI.[130]

The EC identifies the major risks to be connected to the application of rules which seek to protect fundamental rights, such as privacy, data protection and non-discrimination, safety and liability.[131] While recognising the potential benefits of AI system, the EC acknowledges the likelihood that in the future individuals will more often be subject to actions and decisions taken by AI systems. Also, the increased possibility to track and analyse daily actions of individuals raises the concerns for breaches of EU data protection legislations.[132] Concerns are also raised with regard to bias and non-discrimination, as is enforcement of current legislation. The so called "black-box effect", as well as the

[126] European Commission White Paper On Artificial Intelligence – A European approach to excellence and trust, COM (2020) 65 final.

[127] European Commission White Paper On Artificial Intelligence – A European approach to excellence and trust, COM (2020) 65 final

[128] European Parliament Report with recommendations to the Commission on a civil liability regime for Artificial Intelligence, (2020)/2014(INL), para. 14-16

[129] COM (2020) 65 final, page, 10.

[130] COM(2020) 65 final, page 10.

[131] COM (2020) 65 final, page, 10.

[132] COM (2020) 65 final, p. 11.

complexity and the unpredictability of sometimes autonomous behaviour renders it complicated to identify compliance and non-compliance with such legislative frameworks which are intended for the protection of fundamental rights. As a good example, the GDPR is intended to protect the fundamental right to privacy and data protection[133], while the centralised approach thereof can make the applicability to AI systems challenging.

At the time being, there is no internationally recognised definition of AI. Even the European Commission provides different definitions:

In 2018, the EC defined AI by functionality:

"*Artificial intelligence (AI) refers to systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals. AI-based systems can be purely software-based, acting in the virtual world (e.g. voice assistants, image analysis software, search engines, speech and face recognition systems) or AI can be embedded in hardware devices (e.g. advanced robots, autonomous cars, drones or Internet of Things applications)*."[134]

However, in its recent White Paper, AI is defined as

"*a collection of technologies that combine data, algorithms and computing power*".[135]

In the case of ENSURESEC, the most relevant technology is distributed ledger technologies (DLTs), which have been defined by *Kuner et al*. as

"*a particular type of blockchain system that is 'distributed' across several, potentially many, 'nodes' (i.e. individuals or organizations that hold a copy of the distributed ledger)*"[136]

As all other kinds of artificial intelligence technology, DLT remains regulated by general legislation such as the GDPR, which applies to processing of personal data.

In addition, based on reports from the EU legislator, a liability scheme is foreseen, focusing on liability for damage caused in connection to AI[137] and with connection to the Product Liability Directive[138]. The European Parliament also calls for a liability scheme which takes into account risk levels, meaning that AI-systems representing a higher risk would be identified and listed. Further, the European Parliament

[133] Recital 1 – 4 of the GDPR.

[134] Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions Artificial Intelligence for Europe, COM(2018)237 final, page 2.

[135] EC White paper COM(2020) 65

[136] IDPL 2018, vol 8, no 2, Kuner et al 2018, p. 103

[137] Report with recommendations to the Commission on a civil liability regime for artificial intelligence, 2020/2014(INL), https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2020/2014(INL).

[138] Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products
OJ L 210, 7.8.1985.

has called for ethical principles[139] and legal obligations, which would be applicable when developing, deploying and using artificial intelligence and related technologies. The principles laid out includes human-centric and human-made AI, safety, transparency and accountability. Also safeguards against bias and discrimination, right to redress, social and environmental responsibility and respect for privacy an data protection is included. Also user's choices for refusing AI enabled personalization features have been highlighted.

AI is also mentioned in the Report from the European Parliament[140] concerning the revision of the e-commerce directive, presented by the Commission as the Digital Services Act. The report accentuates on the fundamental rights of users, transparency and accountability.

5.4.2. Challenges to data protection

As have been established before, the GDPR applies when processing of personal data and aims to harmonise the protection of fundamental right to data protection in the EU. In addition, GDPR sets requirements on data controller, data processors and joint controller as well as for data transfers to third countries and the protection of data subjects.

Importantly, GDPR is based on the principle of technology neutrality.[141] Therefore, the need to comply with the GDPR, applies to all processing of personal data, irrespective of the processing is being carried out by a system relying on AI or not.[142] In a Communication to the European Parliament and the Council from 2018, the European Commission identifies the GDPR and as ensuring " *a high standard of personal data protection, including the principles of data protection by design and by default*".[143] EC also highlights the right of the data subject to be provided with meaningful information about the logic serving as the basis of decision-making based on automated processing.[144] The individual also has the right not to be subject to automated decision-making, as in Article 22 of the GDPR.

As has been discussed above, GDPR applies in any operation or set of operations where personal data is being processed. Due to this broad definition and technology neutrality, GDPR also applies to blockchain [145]users, nodes and miners, in case they process personal data.[146] Further, personal data

[139] Report with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies, (2020/2012(INL), https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2020/2012(INL).

[140] Report with recommendations to the Commission on the Digital Services Act: Improving the functioning of the Single Market, (2020/2018(INL)), https://www.europarl.europa.eu/doceo/document/A-9-2020-0181_EN.html .

[141] Recital 15 of the GDPR

[142] COM(2020) 65 final

[143] COM(2018) 237 final, p. 14

[144] COM(2018) 237 final, p. 14 and Articles 13 (2) f), 14 (2) g) and 15 (1) h) of the General Data Protection Regulation.

[145].Bacon et al. discuss blockchains, whereas ENSURESEC in general work with distributed ledgers technologies. Therefore, the scope of this discussion is DLT-technologies. However, many similarities can be drawn from other AI technologies, and therefore also sources concerning blockchain can be used.

[146]Bacon et al., p. 39.

can be any data which relates to an identifiable person. As Millard et al lays out, a distributed ledger technology will usually contain two types of data, namely metadata related to transactions and data on the object of the transaction.[147]

In cases where the user of the service is a natural person, metadata, such as the sender's and recipient's addresses would qualify as personal data. Metadata is also considered personal data if a person can be identified by e.g. linking different types of information, if as a result the user identify can be revealed.

Based on these preliminary observations on the modules of ENSURESEC, a discussion on artificial intelligence, machine-learning, metadata/big data and monitoring in the light of the GDPR is in order.

In addition to the GDPR, the Whitepaper of the Commission has laid out principles to be comprised for a potential future AI legal framework, including human agency and oversight, technical robustness and safety, privacy and data governance, transparency, diversity non-discrimination and fairness, societal and environmental wellbeing and accountability.[148] In addition, it needs to ensure socially, environmentally and economically optimal outcomes and compliance with EU legislation, principles and values.[149] This is not binding law yet, but the same type of principles has also been identified as the ethical framework of ENSURESEC, and should therefore be kept in mind.

In order to ensure compliance with GDPR, the partners should consider the legal principles of GDPR in their designing of the tool, with especial care for the principle of data protection by design and by default. These need to be integrated in the innovation, in order to provide data protection by design and by default.

Also the main actor under the GDPR, the controller, is interpreted broadly.[150] This has already been discussed above under Secondary legislation. However, considering the technology neutrality of the GDPR and the principles behind it, it is reasonable to interpret it as also distributed ledger technologies will have some level of controllership. The definition of the GDPR mentions that the any natural or legal person who "*alone or jointly with others determines the purpose and means of the processing of personal data*" is considered the controller. *Inter alia*, a technology cannot be a data processor, but the responsibility, and in the long run also the liability, would be directed to the natural or legal person *de facto* determining purposes and means. The determination of the controllership is based on a case-by-case analysis. In a AI context, this would likely mean either the programmer programming the algorithms, or the legal person otherwise responsible, like a company or non-profit organisation.

Further, to those issues, to which GDPR or other secondary legislation offer a solution, ethics and fundamental rights, as well as the data processing principles of the GDPR, can be used to find guidance. Any interpretation of the rules in a practical situation must be data protection and fundamental rights friendly.

[147] Bacon et al.

[148] Commission White Paper on Artificial Intelligence – A European approach to excellence and trust, COM(2020) 65 final, page 9.

[149] COM(2020) 65 final, page 10.

[150] C-131/12 *Google Spain*, para. 34-38.

5.4.3. Components of ENSURESEC and AI

One of the components of ENSURESEC is detection by monitoring. An AI-based inductive incident monitor will continuously observe run-time data and will employ machine learning techniques to detect incidents. (T5).

Under the module for response, mitigation and recovery, metadata and logs of operations of compromised interfaces will be used for the offline analysis performed by a distributed ledger technology (T6.2). It is intended to create an understanding of exact causes and potential future impacts of the incidents.

Due to complex threats with cascading effects in the e-commerce field, the module for resilient oriented situational awareness aims to involve both advanced machine learning techniques and data analysis techniques to continuously perform situational analysis of suspected and current incidents and to determine their impact. Also, the analysing methods are also intended to enable sharing of information between business partners and their users.

The threat intelligence of ENSURESEC (T7.2) introduces machine-learning based capability to detect both direct threats and indirect signals that could support the identification/prediction of combined cyber and physical threats or vulnerabilities in e-commerce systems, components and assets.

1. *Minimising risks*

It is important to keep in mind, that when using monitoring and analysing large amounts of data, identifying links between then, the quality of the anonymisation is crucial. Anonymisation means, that the data is no longer personal data, and GDPR is therefore also not applicable. De-anonymisation and other measures to link back to a person, a user of the tool, can present risks to data protection, especially to storage limitation and purpose limitation.

It is recommended for ENSURESEC to programme the innovation so that the least personal data as possible is used, including the use of metadata should be minimised. This concerns the whole tool as such, and is important in particular when it comes to the use of machine learning and other AI-based methods. Likewise, as far as only possible, personal data should be stored on the distributed ledger, unless transparency and accountability can be ensured. In case this is not a possibility, it is relevant to discuss privacy promoting tools such as pseudonymisation.

Already in 2007, the WP 29 defined pseudonymisation as *"the process of disguising identities"* with *"the aim of such a process is to be able to collect additional data relating to the same individual without having to know his identity."*[151] This should be considered especially for situations where personal data is being transmitted via a distributed ledger.

Hashing constitutes a way of pseudonymisation. However, unlike anonymised data, pseudonymisation still makes possible to identify a data subject with the set of data. This possibility to identification makes the GDPR applicable, but allows for a more privacy-friendly tool, in line with data protection by design and default.

Other challenges are posed by the data subjects' right to information. It is especially complex in relation to machine learning and similar technologies with are based on self-improving algorithms, tracing back and extracting each piece of personal data is extremely challenging.

Lastly, the principles of the GDPR and the ethics that has been laid out in the ethics chapter provide a good toolbox and guidance for the partners of ENSURESEC. In order to fulfil not only the legal obligations, but to also provide an innovation with high ethical standards, data protection by design and default are important.

2. *Data controllership*

To be able to meet the requirements of accountability, it is important to identify which party is to be concerned as the controller and processor under the GDPR. This is important to establish responsibility and therewith also legitimacy of ENSURESEC.

The concept of controllers is very broad, and had been given a broad meaning by the CJEU. Basically, any actor which has a purpose for processing, and who has influence over that process, can be considered a controller. Controllers can be both natural and legal persons, meaning that a programmer who is programming an innovation, can also become the controller, if no other structure having influence over the data processing is found.

The controller can also be a joint controllership, or different persons can be the controller for different operations. A joint controllership is mentioned by the Commission in the H2020 documents for a consortium which together is engaged in data protection operations. Such an arrangement should be considered by the partners.

5.4.4. Special concerns for machine learning

Data protection principles should also be applied in the light of machine learning. Again, this is a field, which is not (yet) regulated, other than the general GDPR principles which apply to processing of personal data.

However, from an ethical point of view, a few things need to be taken into account. These are also issues which have been discussed by the EU legislator during the process of setting up a regulatory framework for AI in general.

The first one is the bias which can be embedded in machine learning, setting challenges for the neutralities of the outcome. This then also plays into the accuracy of decisions or actions taken with the machine learning as a basis.

Additionally, machine learning causes issues for accountability of data processing. This is because it becomes more difficult to assess the correctness of information when the functions and impacts of a machine learning process is not clear. Accountability is closely connected to transparency, if there is no transparency into decision-making processes and input data, the transparency of personal data processing is hampered.

5.5. Security considerations of ENSURESEC

As has been discussed above under the description of secondary legislation, the NIS Directive sets out responsibilities for Member States. However, some of the obligations under the directive will have implications for certain service providers. Further, as the NIS Directive determines minimum standards, it is important for the partners also to observe national legislation.

That being said, operators of essential services and digital service providers are required to take appropriate technical and organisational measures to manage risks to the security of network and information systems they use. Measures also need to be taken to prevent incidents as well as minimise the incidents affecting the security of those networks and information systems. Further, an operator of essential services shall be obliged to notify, without undue delay, competent authorities of incidents which have a significant impact on the continuity of their service. It is also possible for non-essential entities to follow the same scheme and notify incidents having a significant impact on the continuity of the services they provide.

Annex I of the Directive contains a list of operators which are identified as operators of essential services. For ENSURESEC, it is important to note that banks are included in that list. Therefore, Caixa Bank would be considered such and operator of essential services falling under the scope of the Directive. For this partner, the obligations on risk management, taking preventive measures, minimising effects of incidents as well as notifying incidents with significant impact are applicable and need to be observed.

Even though the GDPR is a legal instrument regulating concerns of data protection, the GDPR also includes obligations for the security of the data processing. These have also been discussed above. The GDPR defined a personal data breach as a "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*".[152]

The partners of ENSURESEC should take measures to ensure the security and confidentiality of the data. These can be both organisational and technical. It is up to the partners of ENSURESEC to identify security risks in their data processing, including by preventing unauthorised access to the data or use of that data, but also ensuring the security of the equipment used for processing.

Those partners of ENSURESEC who are included in data processing as data controller or data processors (see discussion above) should carry out risk assessments evaluating risks of data processing, and find solutions to mitigate those risks. Risks can be mitigated i.e. through encryption while the measures used should take into account "*the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected. In assessing data security risk, consideration should be given to the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed which may in particular lead to physical, material or non-material damage*."[153]

[152] Article 4 (12) of the GDPR.
[153] Recital 83 of the GDPR.

Improving security features also feeds into the idea of data protection by design, which is also one of the focus points of ENSURESEC. As is included in the key principles of data processing, in particular that of integrity and confidentiality, the data shall be processed "*in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures*."[154]

European or internationally accepted standards and specifications relevant to the security of network and information systems.

5.6. Mitigation of Ethical risks

In order to mitigate the risks related to ethical requirements, a few concrete measures can be taken. First, the recommendations for the use-cases and the specific considerations in this chapter 5 ENSURESEC: applying legal and ethical requirements should be considered.

Also, templates for obtaining consent from the use-case participants will need to be drawn up, together with a detailed privacy policy which will accompany the consent document.

Also, the Data Protection Officer ("DPO") and the Ethical Manager are available for discussions on any concerns or thoughts concerning any issue related to the legal or ethical requirements.

6. Concluding remarks

This deliverable has given an overview of the legal and ethical requirements surrounding ENSURESEC provided recommendations on how to meet these requirements. This should provide a solid basis for the development of the use-cases as well as for the technical partners working on the development of the innovations. The deliverable also lays a good ground for discussions for the consortium on how to deliver data protection by design and by default and a data protection friendly and secure tool.

In conclusion, the principle of accountability requires the consortium to make decision as concerns the controllership structure necessary. Decisions are also outstanding on how to tackle the issue of transfer of personal data to a third country.

Finally, this deliverable will constitute the basis for the Data Protection Impact assessment which will be carried out in deliverable D8.5.

[154] Article 5(1) point f of the GDPR.

List of Abbreviations

Abbreviation	Explanation/Definition
AI	Artificial Intelligence
CJEU	Court of Justice of the European Union
CoE	Council of Europe
DLT	Distributed Ledger Technology
EC	European Commission
ECHR	European Convention of Human Rights
ECtHR	European Court of Human Rights
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
ENISA	European Union Agency for Cybersecurity
EU	European Union
GDPR	General Data Protection Regulation
TEU	Treaty of the Functioning of the European Union
TFEU	Treaty of the European Union
WP	Work Package

Bibliography

Legislation

Council of Europe

Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), Rome, 4.XI.1950, available at European Convention on Human Rights (coe.int)

Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), available at https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=090000168089ff4e, last visited 23 November. NB.

European Union

Primary law

Treaty on European Union (Consolidated version 2016), OJ C 202/1, 7.6.2016, p. 15

Treaty on the Functioning of the European Union (Consolidated version 2016), OJ C 202/1, 7.6.2016, p. 47

Charter of Fundamental Rights of the European Union, OJ C 202, 7.6.2016, p. 389

Secondary law

Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products, OJ L 210, 7.8.1985

Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts (OJ L 95, 21.4.1993), 1993

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

Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector, as amended in 2009

Regulation (EU) No 1291/2013 of the European Parliament and of the Council of 11 December 2013 establishing Horizon 2020 - the Framework Programme for Research and Innovation (2014-2020) and repealing Decision No 1982/2006/EC, OJ L 347, 20.12.2013, p. 104

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, OJ L 194, 19.7.2016, p. 1

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), OJ L 119, 4.5.2016

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

Legislative proposals

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) COM(2012)11

Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM(2017) 10 final

Communication from the Commission to the European Parliament and the Council Making the most of NIS – towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union, COM(2017) 476 final/1-2

Jurisprudence

Case 26/62 *Van Gend en Loos*, ECLI:EU:C:1963:1

Case 43/75 *Defrenne*, ECLI:EU:C:1976:56

Case C- 101/01 *Lindqvist*, ECLI:EU:C:2003:596

Case C-131/12 *Google Spain SL*, Google Inc v Agencia Espailola de Protecci6n de Datos (AEPD) and Maria Costeja Gonzdlez, EU:C:2014:317

Case C-362/14 *Schrems I*, para. 94. ECLI:EU:C:2015:650

Case C-582/14 *Breyer v Germany*, ECLI:EU:C:2016:779

Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein*, ECLI:EU:C:2018:388

Opinion of AG Bot in Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein*, EU:C:2018:388

Case C-25/17 *Jehovan todistajat*, ECLI:EU:C:2018:551

Case C-40/17 *Fashion ID*, ECLI:EU:C:2018:1039

Case C- 673/17 *Planet49 GmbH*, ECLI:EU:C:2019:801

Case C-311/18 *Schrems II*, ECLI:EU:C:2020:556

Official documents, guidance and opinions

Article 29 Data Protection Working Party,'Opinion 10/2006 on the Processing of Personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)' (WP29 2006)

Article 29 Working Party, "Opinion 4/2007 on the concept of personal data", 20 June 2007 (WP29 2007)

Article 29 Data Protection Working Party, 'Opinion 1/2010 on the Concepts of "Controller" and "Processor"' (WP29 2010)

Article 20 Data Protection Working Party, ANNEX - health data in apps and devices, Annex to letter From WP29 to the European Commission, (WP29 2015)

available at https://ec.europa.eu/justice/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf

Council of Europe study DGI(2017)12 Algorithms and Human Rights, https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5

EDPB, Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, 12 March 2019 p. 26, available at https://edpb.europa.eu/sites/edpb/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf

EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, adopted 10.11.2020, available at Recommendations 02/2020 on the European Essential Guarantees for surveillance measures | European Data Protection Board (europa.eu)

EDPS , Opinion of the European Data Protection Supervisor on the proposal for a directive of the European Parliament and of the Council on the application of patients' rights in cross-border healthcare, 2009/C 128/03, OJ C 128, p. 20

EDPS, Put data protection accountability into practice, 15 May 2017, available at https://edps.europa.eu/data-protection/our-work/publications/speeches-articles/put-data-protection-accountability-practice_en

EDPS on accountability, accessible at https://edps.europa.eu/data-protection/our-work/subjects/accountability_en .

ENISA 2018, "Recommendations on shaping technology according to GDPR provisions" https://www.enisa.europa.eu/publications/recommendations-on-shaping-technology-according-to-gdpr-provisions-part-2

European Commission, on ePrivacy Directive, available at https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation

European Commission, Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions Artificial Intelligence for Europe, COM(2018)237 final
European Commission, Ethics and Data Protection, H2020 EC European Commission, Ethics and data protection, H2020, available at h2020_hi_ethics-data-protection_en.pdf (europa.eu)

European Commission, on Standard Contractual Clauses, available at, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en
FIND https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Commission-Implementing-Decision-on-standard-contractual-clauses-for-the-transfer-of-personal-data-to-third-countries

European Commission, White Paper On Artificial Intelligence – A European approach to excellence and trust, COM (2020) 65 final

European Parliament, Report with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies, (2020/2012(INL), https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2020/2012(INL)

European Parliament Report with recommendations to the Commission on a civil liability regime for Artificial Intelligence, (2020)/2014(INL)

European Parliament, Report with recommendations to the Commission on the Digital Services Act: Improving the functioning of the Single Market, (2020/2018(INL)), https://www.europarl.europa.eu/doceo/document/A-9-2020-0181_EN.html

AI HLEG, Definition of AI, 2019, Ethics guidelines for trustworthy AI | Shaping Europe's digital future (europa.eu) .

Literature

Bacon, Jean and Michels, Johan David and Millard, Christopher and Singh, Jatinder, Blockchain Demystified (December 20, 2017). Queen Mary School of Law Legal Studies Research Paper No. 268/2017, Available at SSRN: https://ssrn.com/abstract=3091218 (Bacon et al)

Bryce Goodman and Seth Flaxman, 'European Union Regulations on Algorithmic Decision-Making and a "Right to Explanation"' (2016) arXiv.org; Ithaca

<https://search.proquest.com/docview/2074006289?rfr_id=info%3Axri%2Fsid%3Aprimo> accessed 20 May 2019.

EU Law Text, Cases and Materials, Paul Craig and Gráinne de Búrca, Sixth Edition 2015, Oxford University Press, Craig and De Burca (2015)

Giirses and van Hoboken (2017),

Rene Mahieu; Joris van Hoboken; Hadi Asghari, "Responsibility for Data Protection in a Networked World: On the Question of the Controller, Effective and Complete Protection and Its Application to Data Access Rights in Europe," Journal of Intellectual Property, Information Technology and Electronic Commerce Law 10, no. 1 (2019): 84-104, (Mahieu et al.)

Patrick van Eecke and Maarten Truyens, 'Privacy and Social Networks' (2010) 26 Computer Law & Security Review 535

Christopher Kuner, European Data Protection Law: Corporate Compliance and Regulation (2nd edn, Oxford University Press 2007), 71-77 (Kuner 2007)

Christopher Kuner, Developments Reality and Illusion in EU Data Transfer Regulation Post Schrems 18, no. 04 (2017): 38.2017, p.895 (Kuner 2017)

Christopher Kuner, Fred Cate, Orla Lynskey ,Christopher Millard, Nora Ni Loideain and Dan Svantesson, Blockchain versus data protection - International Data Privacy Law, 2018, Vol. 8, No.2 (Kuner et al. 2018)

Christopher Millard, At this rate, everyone will be a [joint] controller of personal data!, International Data Privacy Law, Volume 9, Issue 4, November 2019, Pages 217–219, https://doi-org.kuleuven.ezproxy.kuleuven.be/10.1093/idpl/ipz027 (Milliard 2019).

Lifely A, Robertson W (2017) Blog: smart airports and the importance of data. Airpt. World http://www.airport-world.com/news/general-news/6050-blog-smart-airports-and-the-importance-of-data.html (last accessed: 07-08-2020) (Lifely & Robertson, 2017)

Wibren van der Burg, Law and Ethics: The Twin Disciplines, Erasmus Working Paper Series on Jurisprudence and Socio-Legal Studies, No 10-02, June 28, 2010, (Van der Burg 2010),
http://ssrn.com/abstract (no. =1631720).