CALL H2020-SU-DS-2018-2019-2020
Digital Security
TOPIC SU-DS05-2018-2019
Digital security, privacy, data protection and accountability in critical sectors

AI4HEALTHSEC

"A Dynamic and Self-Organized Artificial Swarm Intelligence Solution for Security and Privacy Threats in Healthcare ICT Infrastructures"

D2.2 – Legal and Ethical Requirements

Due date of deliverable: 31.03.2021
Actual submission date: 31.03.2021

Grant agreement number: 883273
Start date of project: 01/10/2020
Revision 1

Lead contractor: CNR
Duration: 36 months

Project funded by the European Commission within the EU Framework Programme for Research and Innovation HORIZON 2020	
Dissemination Level	
PU = Public, fully open, e.g. web	✓
CO = Confidential, restricted under conditions set out in Model Grant Agreement	
CI = Classified, information as referred to in Commission Decision 2001/844/EC.	
Int = Internal Working Document	

D2.2 – Legal and Ethical Requirements

Editors
Dusan Pavlovic (PN)
Djordje Djokic (PN)
Farhan Sahito (PN)

Contributors
Stephan Kiefer (FHG-IBMT)
Dmitry Amelin (FHG-IBMT)
Gabriele Weiler (FHG-IBMT)

Reviewers
Vassiliki Andronikou (ICCS)
Vasilis Tountopoulos (AEGIS)

VERSION	DATE	REVISION AUTHOR	SUMMARY OF CHANGES
0.1	30.11.2020	PN	ToC (and a section justifying and explaining it)
0.2	23.12.2020	PN	Completed Intro, Chapter 1, 2 and 3. Proposed content for Chapter 4 (pending input from FHG-IBMT)
0.3	15.01.2021	FHG-IBMT	Updated content
0.4	22.02.2021	FHG-IBMT	Updated content
0.5	04.03.2021	PN	Added table numbers, figure numbers Completed and prepared for internal review
0.6	16.03.2021	ICCS	Quality Assurance completed
0.7	22.03.2021	AEGIS	Quality Assurance completed
0.8	25.03.2021	PN	Addressed reviewers' comments
1.0	29.03.2021	PN	Final edits, Updated tables, figures

The work described in this document has been conducted within the project AI4HEALTHSEC, started in October 2020. This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883273

Executive Summary

This document entails analysis of existing regulatory requirements for development, implementation and realization of privacy program including information security management. It contains description of legislative and regulatory requirements deriving from the sources adopted by the Council of Europe as well as sources from the EU Law. A brief overview of international and supranational sources of law that regulate privacy protection, data protection and data security matters are given to introduce a reader in general principles and relevant provisions that affect privacy program and information security management.

Apart from the regulatory requirements, the document contains discussion about relevant ethical discourse. As a follow up of the presentation and discussion, the document provides a regulatory framework specifically designed to contribute to the project objectives. Development and implementation of the framework serve the following two goals:

- To achieve material compliance of project outcomes with relevant requirements of relevant regulation,
- To contribute to design of manageable approach needed to operationalize the controls necessary to properly handle and protect personal data within (and related to) the context of AI4HealthSec.

By achieving these goals, the framework allows not only to meet legal requirements but also expectations related to the successful realization of this project.

Contents

Executive Summary **3**
List of acronyms **5**
List of tables **6**
List of figures **7**
Introduction, Blueprint of the document **8**
1 Interplay between similar (but not the same) concepts **9**
1.1 Privacy and Data Protection 9
1.2 Data Protection and Data Security 9
1.3 Regulation and Legislation – context of the AI4HealthSec 10
2 Structure of the European data protection regulatory framework **11**
2.1 The Council of Europe 11
2.1.1 European Convention of Human Rights 11
2.1.2 Convention 108 12
2.1.3 Case Law 12
2.2 The European Union Law 12
2.2.1 Charter of Fundamental Rights of the European Union 13
2.2.2 GDPR 13
2.2.3 NIS Directive 18
2.2.4 ePrivacy Directive and proposal for ePrivacy Regulation 18
2.2.5 Proposal for ePrivacy Regulation 19
2.2.6 Regulation on Medical Devices 745/2017 (MDR) 19
2.2.7 Medical Device Coordination Group Document (MDCG) 2019-16 20
2.2.8 Case Law of the Court of Justice of the European Union 20
2.2.9 European Data Protection Board and national data protection authorities 21
3 European data protection regulatory framework and its ethical aspects **22**
3.1 Fairness 23
3.2 Transparency 24
3.3 Accountability 25
3.4 Ethics Guidelines for Trustworthy Artificial Intelligence 26
3.4.1 Components of the AI 26
3.4.2 Requirements of Trustworthy AI 28
3.4.3 Assessment of Trustworthy AI 28
4 AI4HealthSec regulatory framework **30**
5 Conclusion **35**
6 Bibliography **36**

List of acronyms

Table 1 - List of Acronyms used in this deliverable

Abbreviation	Meaning
CJEU	Court of Justice of European Union
CSIRT	Computer Security Incident Response Team
ECHR	European Convention of Human Rights
ECtHR	European Court of Human Rights
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
GDPR	General Data Protection Regulation

List of tables

Table 1 - List of Acronyms used in this deliverable 5
Table 2 - Data governance 30
Table 3 - Data security 32
Table 4 - Risk-based approach 33
Table 5 - Privacy by design 33
Table 6 - Incident response 34

List of figures

Figure 1 - Secondary Use of Personal Data under GDPR 15
Figure 2 - The CSIRTs Network is a network composed of EU Member States' appointed CSIRTs and CERT-EU ("CSIRTs Network members"). 18
Figure 3 - Safety vs Security 20
Figure 4 - EDPB Logo 21
Figure 5: Ethics Guidelines for Trustworthy Artificial Intelligence Cover 26
Figure 6 - Realizing Trustworthy AI throughout the system's entire life cycle 27
Figure 7: Interrelationship of the seven requirements: all are of equal importance, support each other, and should be implemented and evaluated throughout the AI system's lifecycle 28

Introduction, Blueprint of the document

This document contains five chapters. Each chapter is divided into sections, and sections into subsections.

After introduction, Chapter 1 contains an introduction into concepts of privacy and data protection. It clarifies the differences between privacy and data protection, as well as between data protection and data security. Information about the types of legislative/regulatory frameworks governing these areas is also given. This chapter underlines the distinction between concepts of regulation and legislation. By doing so, the concept and scope of the regulatory framework relevant for the context of AI4HealthSec are defined/described.

The following Chapter 2 is composed of two sections that present the European regulatory framework for data protection. The focus is on the EU Law. However, the sources of the Council of Europe are presented firstly, as sources of a more general character (conventions with standards and principles). Presentation of each source contains the overview about application of the source, general principles, rules as well as relevant rights and obligations, contribution to the European regulatory framework and details about interplay with other sources.

Chapter 3 contains discussions on the core values promoted by the European Data Protection Regulatory Framework. The focus is on the sociological/ethical/philosophical perspective of each value. The chapter is rounded up by presentation of the EU Guidance on Ethics in Artificial Intelligence that contains the AI specific ethical requirements.

The chapter about AI4HealthSec regulatory framework (Chapter 4) contains description of specific data security obligations existing in European regulatory framework for data protection. These obligations are grouped into five categories that jointly form the AI4HealthSec regulatory framework. The leading source of the framework is the GDPR. Nevertheless, relevant obligations from other sources supplements overall scope of the AI4HealthSec regulatory framework.

AI4HealthSec regulatory framework is composed of the following parts:

- Data governance
- Data security
- Risk-based approach
- Privacy by design and by default
- Incident response

At the end, the document is completed by an appropriate conclusion (Chapter 5).

1 Interplay between similar (but not the same) concepts

The central concepts of privacy program and information security might be found in privacy protection, data protection, and data security. This chapter sheds a light on these concepts pointing out their similarities but also their differences. In addition, the chapter explains the difference between concepts of regulation and legislation. This difference is addressed in the context of the regulatory framework specifically designed for this project.

1.1 *Privacy and Data Protection*

Even though there is overlapping between privacy protection and data protection, these concepts are not the same. There are similarities between them, but differences should be underlined for the purpose of explaining their scopes and meanings.

In 1890 Warren and Brandeis published the article titled as 'The Right to Privacy' in the Harvard Law Review (Warren & Brandeis, 1890). This article provides one of the first definition of privacy as 'the right to be let alone' (Warren & Brandeis, 1890, 193). Since then, definitions have specified more details about the concept of privacy. Nowadays, the concept of privacy is defined in many ways and there are various classifications about privacy. One of them proposes categorization of privacy classes as follows:

- Information privacy – set of rules that governs collection and use of personal information.
- Bodily privacy – set of rules that protects physical being and any jeopardize thereof.
- Territorial privacy – it protects environment of an individual.
- Communication privacy – it protects means of correspondence and communication (Densmore, 2019)

This privacy typology is not written in stone, and there are many others that additionally develop privacy classes and sub-classes. Regardless of the differences in privacy classifications, it seems that the protection of personal data belongs to the class of information privacy. However, this claim should be taken with caution. Namely, personal information might be processed in activities that intrude other privacy classes. So, it would not be wrong to claim that informational privacy pervades all other classes of privacy. However, informational privacy does not coincide with full scope and meaning of other privacy classes. Therefore, privacy is not only older (if we consider historical efforts to define and regulate it) but also broader concept than personal data. It might be inferred that privacy protection encompasses the protection of personal data, and it has been used as a ground for the development of personal data protection.

1.2 *Data Protection and Data Security*

Information Privacy addresses individuals' right to decide about processing information relating to them. Information Security is about preserving the 'security triad' - confidentiality, integrity and availability of information (Densmore, 2019). There are similarities between privacy and security but also there are factors that disconnect them. Therefore, privacy and security could be seen as supplementary concepts but not complementary.

Integrity of information is about its authenticity and it relates to accuracy and completeness of personal information. Confidentiality of information relates to limited access to information, whereas availability enables access to information but only to those who are authorized to use

information. To satisfy the standards of the 'security triad', appropriate security controls have to be implemented and security incidents should be prevented. By doing so, information security preserves information privacy.

Differences between privacy and security could be found in fact that implementing information security does not necessarily preserve information privacy. Namely, information privacy serves to protect specific type of information. However, there is no information privacy without implementation of information security. Therefore, we can have security without privacy, but we cannot have privacy without security (Densmore, 2019).

1.3 *Regulation and Legislation – context of the AI4HealthSec*

There is a common mistake by using terms regulation and legislation as the same concepts. Obviously, they are similar, but differences between them should not be neglected. Namely, both regulation and legislation contain provisions with rules, rights, and obligations. It would not be wrong to claim that they regulate certain relations, entities or fields. However, there are at least two distinct lines between these concepts.

The first one is about the respective sources. Whereas legislation usually refers to statutory law enacted by the legislator (the legislative branch of government), regulation is adopted and promoted by entities that are supposed to develop a self-regulatory system (in order to introduce certain rights/obligations). In other words, legislations are acts adopted by a state, whereas regulations might be adopted by companies, industry associations, formal or informal bodies. The second distinctive line is about the relationship between general and specific. Legislators often adopt rules that are general and applicable in many perspectives. Thus, the concrete application of the rules would be possible only if generals rules and principles are specified to be used in a certain context. This process is usually carried out by development of regulation, or more specifically, self-regulation. However, legislation might be a subset of a regulation. This would be the case when states or other legislative instances are allowed to adopt documents that are formally promoted as regulations, but they contain principles and general rules. These principles and rules might be specified by legislations adopted by lower legislative instances (Kosti et al., n.d.).

As it is explained, the goal of this document is to present certain regulatory framework designed to contribute to the project objectives. Therefore, this document presents specific regulation tailored for a particular purpose. Nevertheless, the document firstly addresses principles and rules from various, but relevant legislations. In subsequent sections, these principles and rules are 'custom-made' and presented as the AI4HealthSec regulatory framework.

2 Structure of the European data protection regulatory framework

This chapter provides brief overview of the sources that regulate protection of personal privacy, personal data, and data security. The goal of the chapter is to introduce the system and organization of principles and rules that protect privacy, personal data and regulate data security.

In the first section, the chapter describes relevant convention law adopted by the Council of Europe as well as brief overview of the case law developed by European Court of Human Rights. The second section outlines the EU Law and relevant primary and secondary law.

2.1 *The Council of Europe*

The Council of Europe has been created after the Second World War. Its primary objective is to form a greater unity between its members for the purpose of safeguarding and realizing the ideals and principles which are their common heritage and facilitating their economic and social progress. Any European State may become a member of the Council of Europe as far as it accepts the principles of the rule of law and the enjoyment by all persons within its jurisdiction of human rights and fundamental freedoms (Council of Europe, n.d.).

In its so far work, the Council of Europe has adopted many conventions that form and protect human rights and freedoms, including protection of personal privacy and data protection. This chapter sheds a light on the most important sources - European Convention of Human Rights, Convention 108 and the case law of the European Court of Human Rights.

2.1.1 European Convention of Human Rights

European Convention of Human Rights (hereinafter ECHR) was adopted in 1950, and it has been effective since 1953. This convention is essential instrument for protecting human rights and make them binding for signing states. The ECHR establishes the European Court for Human Rights (hereinafter ECtHR) which is one of the most significant guardians of human rights.

The Art 8 of the ECHR enshrines the right to respect for private and family life. This article encompasses a wide range of interests. Apart from private and family life it includes home and correspondence (including communication via mails, emails, phone) (Council of Europe, n.d.). In addition, this article protects against arbitrary interferences by public authorities. However, this right is not absolute and hence the fair balance between the competing interests of the individual on one side and of the community on the other should be found. Therefore, contracting parties of the ECHR must develop mechanisms that balance the interests. The mechanism must be 'in accordance with law' and 'necessary in democratic society'.

The ECtHR has developed the case law based on the Art 8 of the ECHR. The case law prescribes negative and positive obligations upon contracting parties. Concerning the positive obligations, states should take all the necessary measures to protect each citizen against unjustified restriction of their fundamental rights. Negative obligations require that States should not hinder hamper the exercise of fundamental rights including right to respect private life. Therefore, in a case of conflict between two competing fundamental rights, a state must find a fair balance between them.

The ECHR is the source of law that establishes strong foundations for privacy protection and protection of personal data. There are many benefits of this source of law. One of the most significant is that relevant case law, subsequent legislations adopted by the Council of Europe, and other

international and supranational regulatory instances, and national regulatory frameworks have been following the principles promoted by the ECHR.

2.1.2 Convention 108

The Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, known as Convention 108 is opened for signatures since January 1981. It is the first legally binding multilateral instrument on the protection of privacy and personal data. The convention has parties and observers not only from the Council of Europe members but also abroad. The special body that works on the implementation of the convention (Conventional Committee) has produced reference documents in important areas such as artificial intelligence, big data, health-related data, media and privacy, Internet governance and similar.

Convention was adapted in 2018. This modernization was necessary to modify Convention 108 to become the landmark instrument for regulating new realities of an increasingly connected world. Also, modifications empower its effective implementation. New protocol that amends the convention remains based on two objectives: free float data and respect for human dignity. The convention 108 together with new protocol is viewed as international standard on privacy protection in the digital age. Therefore, it has been recommended to all United Nations states to accept Convention 108.

The amended protocol is fully consistent with the EU GDPR and the Police Directive. It sets up high data protection standards and enables better environment for innovation and economic growth.

2.1.3 Case Law

The European Court of Human Rights was established in 1959. Since then, the Court has delivered more than 16,000 judgments. Its case law interprets the ECHR and helps to strengthen the rule of law. The Court provides unique perspective of the ECHR by creating powerful and dynamic instrument capable to response to new challenges and the ongoing promotion of human rights and democracy in Europe. Individuals may sue states that are members of the Council of Europe, alleging that the state violates rights granted by the ECHR. Application can be made by any person, non-governmental organization or group of individuals.

The ECtHR has given rulings on various social issues including protection of personal privacy and personal data. Several dozens of cases decided by the Court has provided a vivid perspective to the article 8 to the ECHR. The significance of the Court's Case Law is about the development of principles and rules for data and privacy protection and their specification in particular contexts. The Case Law does not only solve a particular issue but has formed standards for improvement of the regulatory framework for data and privacy protection in Europe and globally. Also, the regulatory development has helped to secure and lawful international transfer of data. As a result, data exchange has been stimulated and that has positively impacted economic growth.

2.2 *The European Union Law*

All actions taken by the EU institutions are based on the treaties. These binding agreements between the EU Member States set out the EU objectives, rules for the EU institutions, decision-making process and the relationship between the EU and Member States.

Treaties are the starting point for EU law and are known in the EU as primary law. The body of law that comes from the principles and objectives of the treaties is known as secondary law. Secondary law includes regulations, directives, decisions, recommendations and opinions.

2.2.1 Charter of Fundamental Rights of the European Union

The Charter of Fundamental Rights of the European Union (hereinafter the Charter) brings together the most important personal freedoms and rights granted by the EU Law into one legally binding document. The Charter was announced in 2000 and came into force in December 2009 together with the Treaty of Lisbon.

The purpose of the Charter is to promote human rights within the territory of the EU. Many of the rights existing in the Charter were previously set out in:

- The EU Treaties
- The European Convention on Human Rights
- Case law of the Court of Justice of the European Union
- National constitutions

The Charter has the same legal power as the EU Treaty. This means that it is superior to the Member States laws. The Charter applies when EU countries adopt or apply a national law implementing an EU directive or when their authorities apply an EU regulation directly. In cases where the Charter does not apply, the protection of fundamental rights is guaranteed under the constitutions or constitutional traditions of EU countries and international conventions they have ratified. The charter does not extend the scope of the EU to matters not part of its normal remit.

The Charter contains all rights granted by the ECHR. However, the Charter addresses some additional freedoms and rights in order to meet reality of newly formed issues. One of the new granted rights relates to protection of personal data. Namely, the Charter ensures that private and family right should be respected granting that 'Everyone has the right to respect for his or her private and family life, home and communications.' In addition, Article 8 regulates protection of personal data by granting that 'Everyone has the right to the protection of personal data concerning him or her'. In addition, the same article lays down that data processing must be carried out fairly, within the specified purposes, and based on consent or other ground laid down by law. Finally, compliance with the 'rules shall be subject to control by an independent authority.'

Despite academic critics and polemics (Sloot, 2017), the Charter separated data protection from protection of personal privacy. Additional significance of the Charter lays in fact that both rights are classified as fundamental rights.

2.2.2 GDPR

The Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and the free movement of such data (hereinafter GDPR) is the core legislative source of the EU Data Protection Law. The GDPR came into force on 25 May 2018, replacing the Directive 95/46/EC. The replacement was necessary to address the challenges regarding the development of new technologies and increasing trend of information transferring. Therefore, the main goal of the GDPR is to deal with the new reality generated by technological development and its effects on the rights and freedoms of individuals. The GDPR protects individuals' personal data from the risks set up

by data processing. In that way, the GDPR strengthens the right to protection of personal data as one of the fundamental rights set up by the Charter of Fundamental Rights of the European Union. Of course, and GDPR laid down that protection of personal data is not an absolute right and it has to be balanced against other fundamental rights.

The GDPR empowers the EU Data Protection Law by promoting a common set of data protection rules that are implementable in all Member States of the EU. The GDPR is Regulation and unlike directives, regulations are directly applicable under EU law. In other words, there is no need for their transposition into national laws, and there is no need for national implementation. For that reason, the GDPR should be a common framework for protecting personal data in the EU.

2.2.2.1 Application of the GDPR

The GDPR applies to the processing of personal data that is wholly or partly carried out by automated means as well as to the processing other than by automated means. Personal data is defined as any 'information relating to an identified or identifiable natural person ('data subject')' that can be identified by revealing 'one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.' Processing of personal data has very broad meaning and it refers to almost everything that could be done with data.

The GDPR does not apply to the processing of personal data regarding activities that fall outside the scope of the EU Law, in certain matters of the EU security and defense policy, in the course of a purely household activities and in cases of data processing carried out by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not. The GDPR applies to the processing of personal data of data subjects who are in the EU. Thus, the GDPR has ex-territorial application and it applies to data processing activities taken by a controller or processor not established in the Union, where the processing activities are related to 'the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or the monitoring of their behavior as far as their behavior takes place within the Union.'

As might be understood, the central entities in charge of processing activities are Data Controllers and Data Processors. Data Controller is 'the natural or legal person, public authority, agency or other body' that determines the purposes and means of the processing of personal data, whereas Data Processor is 'a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller'.

2.2.2.2 The GDPR Principles

The GDPR confirms and additionally develops principles promoted by fair information practices. Therefore, the GDPR does not provide novelties concerning promoted principles but rather organize and specify them in a different way than it has been the case before. The GDPR promotes six principles, plus the accountability principle that is extracted as the separate one.

2.2.2.2.1 Lawfulness, fairness, and transparency principle

Lawfulness means that processing of personal data has to be carried out on the basis of one of the six legal grounds enshrined by the GDPR:

- consent,
- the performance of a contract,
- legal obligation,
- the vital interest of individuals,
- public interest and
- the legitimate interest.

Lawfulness requires that data processing should be allowed and carried out within the constraints of the applicable laws. Applicable laws include not only data protection law but also other applicable laws.

Fairness is a principle that serves to balance potential disbalance of powers between data controllers and data subjects. Application of this principle tends to achieve a 'fair balance' when applying data protection rules. As a result, personal data must not be processed in a manner that prevents unreasonable violation of the fundamental rights and freedoms of data subjects, and particularly their right to the protection of personal data.

Transparency principle is linked to fairness. To meet the transparency requirement, each activity of personal data processing should be conducted transparently. The concrete transparency obligations imposed to data controller are given in articles 12, 13 and 14. These articles enshrine the set of necessary information that should be provided to a data subject by a controller. Also, the GDPR stipulates the ways how information should be presented to data subjects.

2.2.2.2.2 Purpose limitation principle

Purpose limitation principle is embedded in the Art 5(1)b of the GDPR. This article foresees that personal data shall be 'collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes'. In essence, the purpose limitation principle is composed of two sets of requirements. The first one imposes obligation to data controller to identify boundaries within which personal data will be processed. The second set poses obligation to process data only if a processing purpose is compatible with the initial purpose(s) for which data has been collected. To assess compatibility between initial and subsequent purposes, a data controller should examine the following criteria (given in Recital 50):

- The relationship between the purposes for which data have been collected and the purpose that leads the subsequent data processing activities.

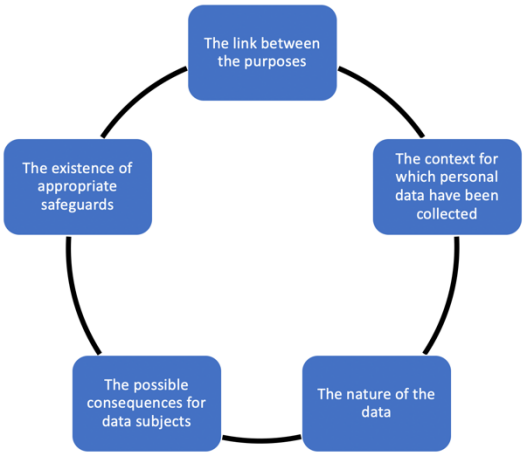

Figure 1 - Secondary Use of Personal Data under GDPR

- The context in which data have been collected and the subsequent expectations of the data subject regarding their further use.
- The nature of personal data and the impact of further use on the data subject.
- Safeguards are put in place by the controller to ensure fair processing.

Nevertheless, it should not be neglected that exceptions from above rules could be acceptable. Exceptions might refer to processing personal data for scientific or statistical analysis and research.

2.2.2.2.3 Data minimization

'Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed'. To satisfy requirements of this principle, data controllers have to pass proportionality and necessity tests. That means data controllers should be able to prove that plans regarding the use of a particular scope and a type of data are reasonable to achieve the specified purpose of data processing. Therefore, data controllers should assess whether the purpose of data processing should be achieved by processing with either fewer data or with properly used measures that will additionally protect personal data. For these reasons, data controllers must adjust the amount of collected data proportionately to the purpose of processing.

2.2.2.2.4 Accuracy principle

The GDPR laid down that 'Personal data must be accurate and, where necessary, kept up to date'. Therefore, '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'. Collection and subsequent processing should be carried out only if data is correct and complete. Data controllers must rectify data whenever they found out that data is inaccurate or incomplete.

2.2.2.2.5 Storage limitation principle

Storage limitation principle is about obligation to keep personal data 'in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.' So, once the purpose of processing is identified, data controllers have to determine the retention period. When the purpose has been fulfilled, data must be deleted. Nevertheless, data might be kept for a longer period if there is a legal ground for further data processing. Also, 'personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.'

2.2.2.2.6 Integrity and confidentiality

The principles of integrity and confidentiality are embedded in the GDPR provision stating that personal data should be 'processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and accidental loss, destruction or damage, using appropriate technical or organizational measures'. Concerning the security of personal data, data controllers should take into consideration several factors when determining appropriate technical and organizational security measures. Also, this principle should be interpreted in the context of data controllers' obligation to report a breach of personal data in a relevant way.

2.2.2.2.7 Accountability principle

Accountability principle is not a new principle in the data protection framework. Nevertheless, the GDPR clearly defines it. In that way, the GDPR significantly contributes the existing data protection framework. The essence of the principle lays in the data controllers' obligation to comply with other principles as well as to be able to demonstrate it.

2.2.2.3 Data subjects' rights

Data subjects have specific rights concerning activities that include processing of their personal data. The rights are regulated by the Chapter 3 of the GDPR.

- The right to be informed - Even though that right to be informed is not explicitly shaped as a separate right, data subjects have a right to know relevant details about activities that include processing of their personal data. The GDPR regulates the type of information that should be presented to data subjects as well as how the information should be communicated.
- The right to access – any data subject has a right to know what information about him/her is processed by a data controller. The importance of this right might be found in the fact that a data subject cannot exercise other rights without knowing what information about him/her is processed. In addition, under this right data subjects have a right to find out not only the category of information processed by data controllers but also other relevant facts such as the purpose of processing, recipients of data, retention period, third parties with whom data is shared, source of data and relevant info about other data protection rights.
- The right to rectification – Considering the purpose of data processing, data subjects have a right to request their data to be completed and/or rectified. This right harmonizes the accuracy principle.
- The right to erasure – This right is also known as 'right to be forgotten'. Under certain circumstances, data subjects might request their data to be deleted. If the erasure conditions are met, data controllers must delete data without undue delay. Also, they have to inform third parties to do so. Nevertheless, data could be kept on several grounds laid down by the GDPR.
- The right to restriction processing - Data subjects also have the right to restrict processing of personal data if the conditions listed in GDPR are met.
- The right to data portability – This right is one more novelty of the GDPR. Data subjects have a right to receive their data from data controllers 'in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided.' This right refers to data processed by automated means. However, exercise of the right is still under question due to several challenges related to technical perspectives of the structured, commonly used and machine-readable format of data.
- The right to object – Data subjects might object processing of their personal data for the reasons specified by the GDPR. However, data controllers could overcome objections if they demonstrate compelling legitimate grounds that override the rights and freedoms of data

subjects, or if data processing is necessary for establishing and/or defending the legal claims.

- The right not to be subject to automated individual decision-making, including profiling - Data subjects have 'the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her'. Nevertheless, exercising right is constrained by specific exceptions as it is regulated by the GDPR.

2.2.3 NIS Directive

The Directive 2016/1148 on the security of network and information system (hereinafter NIS Directive) is the first EU legislative initiative exclusively dedicated to the cybersecurity. NIS Directive was adopted end entered into force in 2016, whereas Member States had to transpose this directive into national laws until November 2018. For effective implementation of the directive, the Member States had at their disposal the "NIS toolkit". This toolkit provides practical information about the best practices, explanations, interpretation of specific provisions, and how they should work in practice.

The general goal of NIS Directive is to provide legal measures to strengthen the overall level of cybersecurity in the EU. For that purpose, Member States should appropriately equip Computer Security Incident Response Team (CSIRT) and a competent national NIS authority. They should cooperation and form 'Cooperation Group' to support and facilitate strategic cooperation and the information exchange. NIS Directive imposes obligation to Member States to effectively cooperate on specific cybersecurity incidents and share information about risks via CSIRT Network. Member States should identify the 'operators of essential services' within business sectors such as energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure. In these sectors operators should take appropriate security measures and notify serious incidents to the relevant national authority.

Figure 2 - The CSIRTs Network is a network composed of EU Member States' appointed CSIRTs and CERT-EU ("CSIRTs Network members").

Article 23 of the directive requires periodical review of the directive by the European Commission. As a result of the review process, the new legislative proposal has been presented in December 2020. Proposal for 'NIS 2.0' contains measures for improvement cybersecurity infrastructure, and particularly the resilience and incident response capacities of public and private entities, competent authorities. The new proposal expands the scope of the directive application and includes medium and large companies.

2.2.4 ePrivacy Directive and proposal for ePrivacy Regulation

The GDPR applies to all sectors, without any differentiation. Therefore, its application is considered horizontal. However, the EU Law also contains legislations with vertical application. It is a word about sector specific application. One of these legislations is ePrivacy Directive.

In order to follow up rapid technological development within electronic communication sector, the EU legislator started developing vertical legislation to regulate 'the processing of personal data in connection with the provision of publicly available electronic communication services in public communications networks in the community'. That was necessary to protect users' rights concerning protection of personal data and privacy. The ePrivacy Directive was approved in 2002 and amended in 2009. This directive was complementary to the Directive 95/46 and it has regulated sectors that were not covered by the Directive 95/46. In essence the ePrivacy Directive should ensure privacy and confidentiality of electronic communications through application of appropriate organizational and security measures.

Even though many of provisions are general (or principle-based), there are also specific rules. The significant importance of the directive is regulation of use of tracking technologies (known as cookies) and regulation of commercial communication, particularly unsolicited communication. The ePrivacy Directive imposes obligations not only on electronic communication providers but also on Member States. It is worth stressing the ePrivacy Directive stipulates use of a user consent (in accordance with Directive 95/46/EC and the GDPR) as the legal ground for lawful data processing. Of course, there are some exceptions when consent is not necessary.

2.2.5 Proposal for ePrivacy Regulation

Due to the enormous development of technology in recent years as well as exponential growth of processed data in the electronic communications environment, the EU legislator has decided to amend the e-Privacy Directive. Therefore, there is ongoing amending of the ePrivacy directive. More precisely, the EU legislator is currently working on a new e-Privacy Regulation (hereinafter ePrivacy Regulation).

The EU legislator tends to extend the scope of the ePrivacy Regulation as well as to replace the current directive by regulation and in that way to unify Member Stets national laws (as it is the case with GDPR). The current proposal for ePrivacy Regulation reinforces the regime of protection for users and subscribers of electronic communications services. This regulation introduces new compliance obligations and sanctions in situations of non-compliance. Also, the current global standards regarding the confidentiality of communications would be updated. Finally, ePrivacy Regulation is supposed to be complementary to the GDPR.

2.2.6 Regulation on Medical Devices 745/2017 (MDR)

EU adopted new Medical Device Regulation 2017/745 (hereinafter MDR) on 5th of April 2017, and it came to force on 25th of May 2017 with a transition period for already approved medical devices till 25th of May 2021. This regulation replaces two EU directives: 90/385/EEC (active implantable devices) and 93/42/EEC (other medical devices). It aims to ensure high quality and safety standards for medical devices on the EU market. In comparison to two replaced EU directives, the MDR improves focus on the cybersecurity topic. In particular, the document requires manufacturers develop their medical devices (software and/or devices included electronic programmable systems) in accordance with state of the art regarding the principles of risk management and IT security.

2.2.7 Medical Device Coordination Group Document (MDCG) 2019-16

Medical Device Coordination Group was established to assist in implementation of MDR according to article 103(1) of MDR and to achieve the objective they released a Guidance on Cybersecurity for medical devices (hereinafter MDCG 2019-16) in December 2019. The goal of the document is to provide guidelines for manufacturers, as well as other actors in the supply chain, to comply with essential requirements of the MDR and IVDR (EU Regulation 746/2016 for in vitro diagnostic medical devices) relevant to cybersecurity.

Figure 3 - Safety vs Security

The document points out the importance of the relationship between safety and security during risk assessment of medical devices. A security issue can have safety impacts, whenever the security is too week (e.g., making a malicious modification in a system is too easy) or is too restrictive (e.g., in an emergency medical personnel should be able to access implantable medical device easily, but in normal operating conditions it needs strong security measures).

2.2.8 Case Law of the Court of Justice of the European Union

The Court of Justice of the European Union (hereinafter the CJEU) reviews the legality of the acts of the institutions of the European Union, ensures that the Member States comply with obligations under the Treaties, and interprets European Union Law at the request of the national courts and tribunals. The Court thus constitutes the judicial authority of the European Union and, in cooperation with the courts and tribunals of the Member States, it ensures the uniform application and interpretation of EU Law (Court of Justice of the European Union, n.d.).

The CJEU has an important role in harmonizing national regulatory frameworks on data protection. Before the GDPR became fully effective, Directive 95/46 regulated data protection principles and rules at the EU level. Principles laid down by the Directive were frequently interpreted by national regulators in non-harmonized ways. The CJEU interventions were valuable to harmonize standards as well as to maintain and develop data protection principles and rules by deciding the cases referred by national courts. In era of the GDPR, the Court issues several important decisions (e.g. Scherms case, Planet 49 case) that significantly affect the regulatory landscape of data protection. The CJEU interpretations of rules and principles decreases the level of legal certainty but impose additional challenges for application of relevant principals and rules in practice.

2.2.9 European Data Protection Board and national data protection authorities

The European Data Protection Board (hereinafter the EDPB) is an independent European body. This body has been established by the GDPR and might be consider as a successor of the Article29 Working Party (established by the Directive 96/46). The EDPB contributes to the consistent application of data protection rules throughout the European Union. It also promotes cooperation between the EU's data protection authorities.

Figure 4 - EDPB Logo

The EDPB is composed of representatives of the national data protection authorities, and the European Data Protection Supervisor (EDPS). The EDPB closely cooperates with the European Commission in the matters regulated by the GDPR. The EDPB can adopt general guidance, recommendations, and best practices to clarify the terms of European data protection laws, providing a consistent interpretation of data protection principles, rights, and obligations. This body may adopt binding decisions towards national supervisory authorities to ensure a consistent application of data protection regulation. Also, the EDPB may adopt consistency findings in cross-border data protection cases and ensure effective exchange of information and best practice between national supervisory authorities (European Data Protection Board, n.d.).

National data protection authorities are independent public authorities with investigative and corrective powers that might be engaged to supervise application of the data protection law. Data protection authorities provide expert advice on data protection issues and handle complaints lodged against violations of the General Data Protection Regulation and the relevant national laws. There is one in each EU Member State.

3 European data protection regulatory framework and its ethical aspects

Law prescribes what must, can or cannot be done. However, ethics goes beyond what is stipulated by law. Data protection law is based on certain ethical values and it supports fundamental right and freedoms (Hijmans & Raab, 2018, 1). Moreover, 'laws come and go; the ethics stays' (Taleb, 2018).

There is an increasing trend of ethical discussions on protection of personal privacy and personal data. It comes as no surprise due to rapid technological development. New technologies could improve security measures that protects personal privacy. However, aspirations toward high security might also jeopardize privacy – for example, application of surveillance system at public place might be at cost of our personal privacy. So, it would not be wrong that two opposite conclusions could be both correct.

Privacy is an elusive concept and there are many definitions for it. Nevertheless, it seems that there is no universal and omni-accepted one (Solove, 2008). Privacy can be seen as a social value and public good as well as an individual value (Warren & Brandeis, 1890). If we take into consideration access theories of privacy, we may conclude that privacy is about isolation and solitude. However, isolation and solitude could be unwanted, and this fact generates weakness of access theories. These weaknesses are little wonder due to reason that these theories are quite old. Some of them have been created at the end of XIX century by Warren and Brandeis (Warren & Brandeis, 1890).

Modern theories give particular attention to individuals' right to choose and decide whether a situation is unwanted loneliness or just private. Modern theories such as control theories, introduced the idea of an individual's self-determination concerning personal privacy. However, in era of data-sharing industry, it is quite questionable whether individuals might use effective mechanism to determine environment that protects their privacy in a way they would expect to. Even though those theories have their weak sides, it cannot be denied that they extract privacy as a concept that differs from others due to its authentic value. What is similarly important is that theories form foundations for development of the system of rights that protect privacy.

Challenges related to outlining the ethical dimension of privacy also lay in diversity of protected objects. Protection of home and places, protection of property, protection of computers, protection of family right, protection of social relations, protection of communications, protection of documents, protection of the person (body, mind, identity), and protection of personal data might belong (cumulatively or separately) to protection of personal privacy. Some of these objects belongs to personal zone (e.g., body, thoughts), some to intimate zone (e.g., family life), some to semi-private zone (e.g., social relations) whereas there are those that belong to public zone (e.g., property). Also, there are physical things such as properties, computers or documents. On the other side there are non-physical such as personal data (Koops et al., 2017). Due to substantial diversity of protecting objects, it is not an easy task to extract the system of values that promotes and protects the concept of privacy.

If we turn back to the regulatory framework that protects personal privacy, we may easily conclude that many provisions are principle-based and not rules-based. Each principle has its own ethical dimension and value. After consideration of these aspects and for the sake of project objectives, we decided to focus on three of them, namely fairness, transparency, and accountability.

3.1 *Fairness*

Fairness might be views ad a value that enables equal treatment in accordance with accepted social standards. This value is related to justice and it should provide treatment without biases or discrimination. In that way, fairness ensures access to equal opportunities.

Fairness stays behind the idea that individuals should be aware of facts related to processing their personal data. This is necessary to make an informed decision about personal data processing. However, there are situations that individuals cannot decide on processing their personal data due to reasons that override their freedoms and rights. Fairness requires an assessment on how processing will affect individuals. If processing negatively affects individual, then processing will be unfair. However, there are situations when processing generates negative effects, but processing is still considered fair (Ustaran, 2018, 106). For instance, personal data may be collected by tax authorities about an individual who has not paid taxes. Processing information about previously received multiple fines and/or sanctions for tax evasion should be used to issue stronger penalties. However, regardless negative effects to the person, processing his/her data should be considered also fair. Justification might be found in the application of relevant tax law, and therefore the processing should be considered as fair.

Even though that fairness enables equal treatment, this value has a crucial role in the selection of privacy intrusion. For instance, special categories of data are processed more restrictively than those that are not sensitive. Nevertheless, it is quite fair to process more data about some individuals such as public figures, politicians and so on. More liberal disclosure of this type of data relies of the freedom of expression grounds.

Regarding the interaction of cybersecurity with fairness, there are several considerations. Firstly, cybersecurity threats and application of protective measures might have different effects on different protected values. For instance, data breach might concern financial data and ultimately may provoke measurable financial loss. However, reputational damage generated by data breach or violation of personal privacy might be very difficult to quantify. Therefore, these values (reputational damage and violation of personal privacy) might be considered less important than financially measurable loss. This could open a Pandora's box of ethical questions, particularly if a risk assessment regarding potential cybersecurity threats gives higher value to financial considerations (Knockaert et al., 2020, 11).

The fact is that many entities need to implement cybersecurity measures. The second ethical consideration is about justification for/of use of a particular measure to protect a particular property. It is well known that decision of this kind is usually based on risk assessment. In other words, damages and harms should be evaluated before a measure is decided. However, it is quite legitimate to wonder whether (for instance) national security as a protective property is more valuable than citizens' rights and freedoms. This dilemma is solved using prevalent ethical discourse in a society (or country) and application of decided methodology. However, whatever is applied, it raises polemics about the fairness of the decision.

Finally, the third consideration is about a decision-maker. Cybersecurity measures might come at the expense of some values or may jeopardize certain properties. Therefore, a state or a company decision to protect certain entity or value (e.g. company's property or national security) might be at the cost of rights and freedoms of individuals. Simply, some social groups are authorized to make

decisions that primarily protects the interest of that group. Nevertheless, this potentially subjective assessment might lead to discrimination and fairness (re)considerations.

It would not be wrong to claim that fairness does not only enable equality but also treats different individuals and situations in different manners. This could be explained by close relations of fairness with justice. Rawls claims that 'justice denies that the loss of freedom for some is made right by a greater good shared by others. It does not allow that the sacrifices imposed on a few are outweighed by the larger sum of advantages enjoyed by many. (…) 2An injustice is tolerable only when it is necessary to avoid an even greater injustice' (Rawls, 1999, 3-4).

3.2 *Transparency*

There are various academic explanations about transparency. Transparency might refer to forms of information visibility, which is increased by reducing or eliminating obstacles. It provides possibility to access information, intentions or behaviors (Turilli & Floridi, 2009, 105). Also, Vaccaro and Madsen define transparency as a 'degree of completeness of information, provided by each company to the market, concerning its business activities' whereas DiPiazza and Eccles as the 'obligation to willingly provide to shareholders the information needed to make decisions'. These definitions emphasize the perspective of those who enable access to information transparency. An entity that generates availability of information forms accessibility to the information, makes them transparent and thereby affects user's decision-making process. In other words, information providers configure elements regarding information disclosure. Choices and decisions regarding information disclosure should be in accordance with relevant regulation but also depend on business, and ethical factors (Turilli & Floridi, 2009, 106).

There are strong links between fairness and transparency (Ustaran, 2018, 106). Transparency involves openness and clearness regarding activities that may encroach someone's privacy. Individuals whose data is processed should be informed about activities that may encroach into personal privacy, including those that relate to personal data processing. How much information will be considered sufficient will depend on the particular circumstances (such as regulation, decisions of an information provider, business and ethical factors). Therefore, it would not be wrong to claim that transparency is not an ethical principle per se. It might be considered ethically neutral principle but it can easily become 'proethical condition, when the disclosed information has an impact on ethical principles. Such an impact depends on at least two types of relationships that occur between disclosed information and ethical principles. One is dependence: some amount of information is required in order to endorse ethical principles. The other is regulation: ethical principles regulate information flow by constraining its access, usage, dissemination and storage.' (Turilli & Floridi, 2009, 107).

Transparency contains the feature of graduality. If we refer to relevant legislation, we may see that data processing activities that are likely to result in a high risk to the rights and freedoms of natural person by virtue of their nature, scope, context and purpose should be reported to data protection authorities. That is not the case with less risky data processing activities. In other words, transparency imposes obligations to engage stricter controlling mechanism when risks for personal privacy are greater. Nevertheless, we should not forget that exposer of privacy might be useful for upgrading other domains. For instance, access to health-related data may contribute life-saving research, even though someone's privacy could be violated.

The dilemma of picking the type of information that should be disclosed requires understanding the features of the audience that should be informed. In other words, an information provider should consider who should be informed about information processing activities. For instance, processing children information collected via a website supplied by children-related content forms a context that is substantially different than one in which an employer collects and processes employee's data.

Transparency is not only about the providing access to information. It also refers to ways how information is provided. Delivering info about data processing before processing starts affects individuals' choice concerning the protection of their personal privacy. Therefore, one of the foundations regarding transparency refers to providing information about data processing in a timely manner. A timely manner is quite general construction, and its specification is context-based. Finally, transparency means that information about processing activities should be clear, concise, easy to understand and provided in an accessible manner. Again, and these requirements are general, and their practical form will depend on a particular context.

3.3 *Accountability*

Distinctions among concepts such as liability, accountability, ethics and responsibility have raised academic discussions. There are various conceptualizations and subsequent reconceptualization of these concepts (Mulgan, n.d.). Accountability is one of key values within European data protection regulatory framework. There are tendencies for stronger embedding of accountability within the framework. Accountability was outlined in OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Nevertheless, unlike Directive 95/46, the GDPR explicitly regulates accountability as a separate principle.

The essence of accountability principle lies in obligation to be compliant with all other data protection principles and to be able to demonstrate it. These requirements are part of the legal responsibility, and it is important to underline that accountability goes beyond legal responsibility. Legal responsibility concerns who is supposed to do what, and it may include legal consequences for the performance or non-performance of duties and tasks that are regulated by certain legislation (such as GDPR). Accountability implies that a responsible agent attempts to respect other principles and demonstrates its compliance, even when this is not explicitly required by law (Hijmans & Raab, 2018, 10). Therefore, accountability imposes both - obligation to behave in a certain way; and preparedness to explain the behavior to relevant stakeholders (e.g. public bodies in a form of regulatory instances as well as individuals). Being capable to explain the behavior relies on (inter alia) requirements deriving from transparency principle.

Accountability includes a risk-based approach. Whoever processes someone's data should assess risks related to the processing. By doing so, data controllers and/or processor should make ethical judgements. The GPDR contains explicit requirement for risk assessment formed in so-called Data protection impact assessment (DPIA). Having in regard, the lack of clear rules for conducting DPIA, the accountability plays a crucial role in ethical assessment of risks generated from activities that might affect someone's privacy.

Accountability is closely linked to corporate social responsibility (Hijmans & Raab, 2018, 11). Societal concerns should be integral part of business (and not only business) practice. In era of emerging technologies, particular attention should be given to innovations. Responsible innovation should have ethical dimensions that would not raise societal concerns (and privacy protection is one of the

greatest concerns). In his work, Koops notes that authors have several different opinions regarding what responsible innovation is. It has been described as a 'concept', a 'notion', a 'discourse', an 'approach', an 'ideal', an 'aspiration', a 'new field of study', an 'emerging discipline', a 'trend in a scholarship', a 'policy' or a 'hype'. He sums up responsible innovation as a combination of two things. 'It is, first, an ideal: something we strive for even though we realize it can never be fully attained. Second, it is also a project, a joint enterprise of an increasingly large community of people who want to bring us closer to this ideal' (Koops, 2015, 5). If we would like to get closer to this ideal, then we need specific instruments for building and stimulate ethical dimensions. Some academics have developed the concept of 'ethics by design' for this purpose. (Hijmans & Raab, 2018, 11).

If we turn back to the European data protection regulatory framework, we may easily notice that the regulator has integrated the concept of 'privacy by design' into the framework. This concept established by former Information and Privacy Commissioner of Ontario Ann Chavoukian, is principle-based concept that advocates embedding data protection into the specific design of new systems and technologies (Ustaran, 2018, 200). 'Privacy by design' reflects ethical dimension of accountability whenever planning and execution of new developments are conducted. Moreover, this concept should be addressed in ongoing operations and management of entire life cycle of personal data processing.

If we consider the distinction between accountability and responsibility concerning the context of 'privacy by design' we may easily infer that this concept has an important role for legal responsibility. There are legal provisions that impose certain obligations that should be met to fulfill the legal requirements. However, the normative structure of 'privacy by design' leads us toward conclusion that this concept is the essence of accountability. There is no obvious solution or 'one-size-fits-all' approach to satisfy all requirements from seven principles that create this concept. Ethical choices are left to those that create innovation, develop technologies, or already use them. However, these choices might be the subject of civil procedure and liability discussed in an appropriate forum (e.g. competent court).

3.4 *Ethics Guidelines for Trustworthy Artificial Intelligence*

On 8 April 2019, the High-Level Expert Group on AI presented Ethics Guidelines for Trustworthy Artificial Intelligence (hereinafter the Guidelines). The goal of the Guidelines is to promote Trustworthy AI. The Guidelines are composed of three chapters. The first one is the most general and focuses on foundations (components) of Trustworthy AI. The second explains requirements of Trustworthy AI and methods to realise Trustworthy AI. The final one is about assessing Trustworthy AI.

Figure 5: Ethics Guidelines for Trustworthy Artificial Intelligence Cover

3.4.1 Components of the AI

According to the Guidelines, trustworthy AI is based on three components that should be met during the entire lifecycle of the AI:

- Lawful AI - respecting all applicable laws and regulations
- Ethical AI - respecting ethical principles and values
- Robust AI - both from a technical perspective while taking into account its social environment

3.4.1.1 Lawful AI

There is a duty of any natural or legal person to comply with laws when develop, deploy and use artificial intelligence. Therefore, lawful artificial intelligence means that its' development, deployment and use should comply with various legally binding rules and laws. Legal sources that should be taken in consideration might be international, supranational and the national laws. The legal sources such as EU primary law, EU second reload, international conventions and numerous national legislations might impose both negative and positive obligations. These sources impose what cannot be done, what should be done, and what may be done. In other words, they enable certain actions but also prohibit some of them.

The lawful artificial intelligence fosters the second and third components of Trustworthy AI (ethical and robust AI). However, we should be aware that some reflections of ethical and robust artificial intelligence exist within the first component of Trustworthy AI (lawful AI). Nevertheless, realization of ethical and robust AI goes beyond legal obligations.

3.4.1.2 Ethical AI

Laws usually do not speed up technological developments. Conservative legislative techniques very often cannot create a law that follows the rapid progress of technology. Also, valid legal sources might not reflect the prevalent ethical discourse. However, Trustworthy AI must be aligned with certain ethical norms.

Taking into account that AI should improve individual and collective wellbeing, it would not be wrong to claim that applied ethical principles for Trustworthy AI are rooted in fundamental rights. Fundamental rights are ethical imperatives and hence all AI practitioners should tend to adhere to them. The Guidelines refers to principles set up by the Charter as a mirror to fundamental rights. Therefore, the principles of Trustworthy AI are:

- Respect for human autonomy
- Prevention of harm
- Fairness
- Explicability

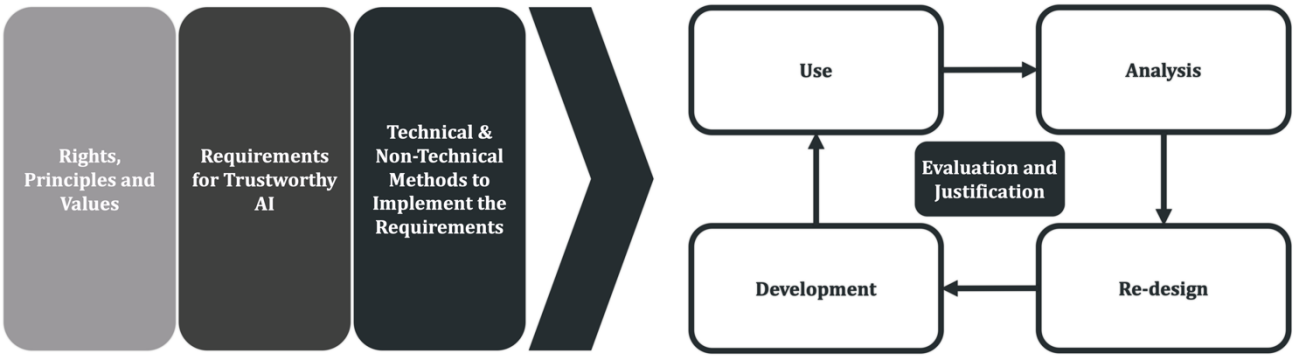

Figure 6 - Realizing Trustworthy AI throughout the system's entire life cycle

3.4.1.3 Robust AI

Robust artificial intelligence is a system that performs in a safe, secure and reliable manner. It contains safeguards that serve to prevent any unintended adverse impact. Therefore, when AI system is robust individuals and society must be confident that AI will not cause any unintentional harm. Robustness complements ethical AI and vice versa. Together with Lawful AI, they compose Trustworthy AI.

3.4.2 Requirements of Trustworthy AI

The Guidelines provide more concrete requirements to achieve trustworthy AI. These requirements apply to various stakeholders such as developers, deployers, end-users, and broader society. The Guidelines proposes a set of seven key requirements that AI systems should meet to be regarded as trustworthy:

- Human agency and oversight (Including fundamental rights, human agency and human oversight)
- Technical robustness and safety (Including resilience to attack and security, fall back plan and general safety, accuracy, reliability and reproducibility)
- Privacy and data governance (Including respect for privacy, quality and integrity of data, and access to data)
- Transparency (Including traceability, explainability and communication)
- Diversity, non-discrimination and fairness (Including the avoidance of unfair bias, accessibility and universal design, and stakeholder participation)
- Societal and environmental wellbeing (Including sustainability and environmental friendliness, social impact, society and democracy)
- Accountability (Including auditability, minimisation and reporting of negative impact, trade-offs and redress).

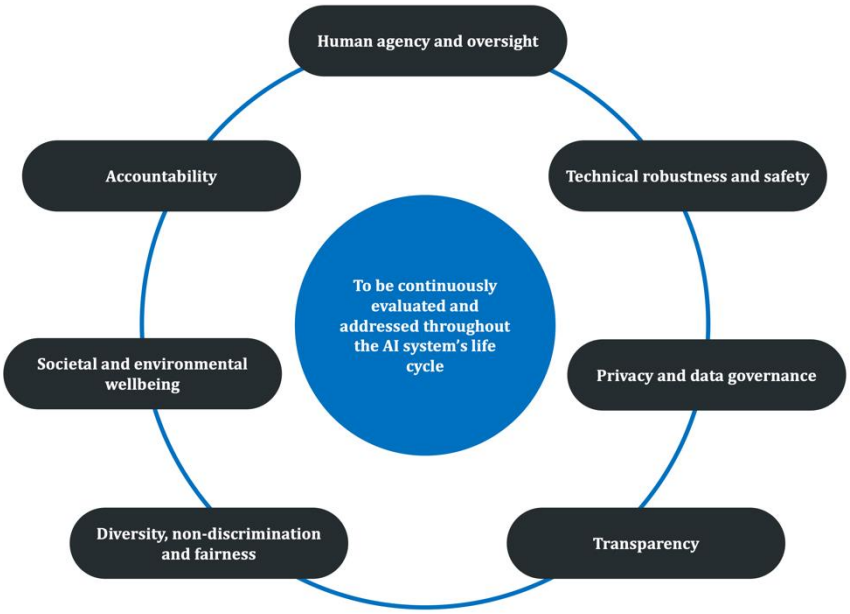

Figure 7: Interrelationship of the seven requirements: all are of equal importance, support each other, and should be implemented and evaluated throughout the AI system's lifecycle

3.4.3 Assessment of Trustworthy AI

Assessment of Trustworthy AI is a context-based process. The Guidelines stresses that there is a non-exhaustive list of factors and criteria that might be used for assessment purposes. Therefore, it would be necessary to create the assessment list created accordingly to specific use case and context in

which the system operates. The assessment list should take into account the governance structure of a particular entity (or entities) which engagement relate to the system (development, deployment, use). Cooperation among relevant stakeholders is necessary for this purpose. Assessment of trustworthy AI primarily observes Ethical AI and Robust AI. That does not mean that assessment should not contain questions useful to assess compliance with relevant legislation (e.g. data protection legislation). Nevertheless, it must be emphasized that the Guidelines do not provide instructions on how to assess the compliance state of the system with relevant legislative requirements.

4 AI4HealthSec regulatory framework

The AI4HealthSec regulatory framework is perceived to be composed of five integral parts:

- Data governance
- Data security
- Risk-based approach
- Privacy by design
- Incident response

These parts are not separate units. Moreover, they permeate and supplement each other. Data governance is an integral part of the framework since it refers to the process of managing the availability, usability, integrity and security of the data. Rules for data security determine methodology for setting up appropriate security controls. The methodology is based on assessment of the risks that might be materialized and consequently compromise data. Therefore, it is necessary to apply privacy and security preserving approaches through whole data lifecycle. For that reason, concepts of Privacy by design and by default are inseparable parts of AI4HealthSec regulatory framework. Finally, when security controls are failed and data is compromised, appropriate response to the security incident should be conducted.

In the following sections more details on each part of the regulatory framework are included. Also suggestions on provision that should be taken into consideration to outline each part of proposed regulatory framework are extracted.

Table 2 - Data governance

Data governance	
Protection of personal data (in clinical investigations)	A clinical investigation may be conducted only if the rights of the subject to physical and mental integrity, to privacy and to the protection of the data concerning him or her are in accordance with the GDPR are safeguarded. Relevant provisions: - MDR: Article 62(4)(h)
Data security	Data should be processed in manner that ensures appropriate security and confidentiality of the personal data including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. Relevant provisions: - GDPR: Recital 39 and Article 5(1)(f)

Data minimization and storage limitation	Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimization'). Personal data should be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Relevant provisions: - GDPR - Article 5(1)(c) and Article 5(1)(e) - ePrivacy Regulation – Article 7(1) and Article 7(2)
Purpose limitation	Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Relevant provisions: - GDPR - Article 5(1)(b) - ePrivacy Regulation – Recital 19, Recital 20, and Article 8(1)
Roles and responsibilities	The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processors, also in relation to the monitoring by and measures of supervisory authorities, requires a clear allocation of the responsibilities. Relevant provisions: - GDPR - Recital 79
Data Processor guaranties	To ensure compliance with the requirements of the GDPR in respect of the processing to be carried out by the processor on behalf of the controller, when entrusting a processor with processing activities, the controller should use only processors providing sufficient guarantees, in particular in terms of expert knowledge, reliability and resources. Relevant provisions: - GDPR - Article 28 and Recital 81
Metadata of personal data and monitoring of data processing (inventory of processed data)	Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. Relevant provisions: - GDPR: Article 30
Code of Conduct and certification	It is stipulated to develop code of conducts and/or certification mechanism that would contribute implementation of the data protection regulation

	Relevant provisions: - GDPR: Article 40 and Article 42

Table 3 - Data security

Data security	
Security of processing	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 risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk. Relevant provisions: - GDPR: Recital 83, and Article 32 - MDR: Annex I
Implementation of appropriate technical and organizational measures	The appropriate measure that the controller and the processor should implement may include inter alia the pseudonymization, encryption of personal data; any measure that ensures the ongoing confidentiality, integrity, availability and resilience of processing systems and services; measures that ensure the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and carry our regular testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. Relevant provisions: - GDPR: Recital 28, Article 32 - NIS Directive: Recital 49, Article 14, Article 16 - MDR: Annex I
Confidentiality of data	Data shall be confidential. Any interference with data, such as by listening, tapping, storing, monitoring, scanning or other kinds of interception, surveillance or processing of data, by persons other than authorized users, shall be prohibited, except when permitted by relevant regulation. Relevant provisions: - GDPR: Recital 39 and Article 5(1)(f) - ePrivacy Regulation: Recitals 1, 6, 11, 12, 13, 15, 16, and 17 and Article 5

	- MDR: Annex I
Security of network and information system	Network and information systems should be able 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. Relevant provisions: - NIS Directive: Article 4

Table 4 - Risk-based approach

Risk-based approach	
Data Processing Impact Assessment	Where data processing is based on the use of new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. Relevant provisions: - GDPR: Recital 84, Recital 90 and Article 35 - ePrivacy Regulation: Recital 17, Article 6(b), Article 6(c) - ePrivacy Directive: Article 4(2) - MDR: Annex I

Table 5 - Privacy by design

Privacy by design	
Privacy by design and by default	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 organizational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimization, in an effective manner and to

	integrate the necessary safeguards into the processing in order to meet the requirements of GDPR and protect the rights of data subjects. Relevant provisions: - GDPR: Recital 78 and Article 25

Table 6 - Incident response

Incident response	
Breach notification requirements, Business continuity, Disaster recovery, and Resilience	In the case of a data breach, the controller when become aware of the breach shall without undue delay notify the personal data breach to the supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay. The controller should take measures to mitigate its possible adverse effects. Relevant provisions: - GDPR: Recital 85, 86, 87, 88 and Article 33, 34, - NIS Directive: Recital 69, Article 14 and Article 16 - MDR: Article 87

The identified regulatory framework is composed of relevant principles and legal rules applicable to the AI4HealthSec project. Concerning that the project is at an early phase of technical developpements, the applicability of these principles and rules may require re-assessment as the project evolves towards the piloting phase. All relevant updates concerning the processing of personal data within the project as well as concerning the project outcomes, on which the identified legal framework applies – must be updated by responsible partners and reported within the Data Management Plan. Based on this reporting, additional legal and ethical requirements may be identified and applied thruought the project life cycle.

5 Conclusion

This deliverable has the form of the report presenting regulatory sources relevant for the creation of the AI4HealthSec regulatory framework. Therefore, the document presents the most important the Council of Europe and the EU Law sources related to the domain of privacy, data protection and data security. Due to specificities of the overall project goal, regulation of the medical devices has been also given.

The AI4HealthSec regulatory framework presented in the section 4 encompasses the elements necessary to achieve material compliance of project outcomes with relevant requirements of relevant regulation. The framework should be perceived as the compliance guidelines composed of applicable principles and rules in the project-related context. It contributes to the design of a manageable approach needed to operationalize the controls necessary to properly handle and protect personal data within (and related to) the context of AI4HealthSec. The regulatory framework serves as a valuable source for the development, implementation and realization of privacy program including information security management tailored for AI4HealthSec.

The document does not only present regulatory sources but also the presentation of relevant ethical discourse. Presented ethics focuses on principles and values that promote and protect the privacy, data protection and data security.

6 Bibliography

- *Charter of Fundamental Rights*. (n.d.). Citizen Information. Retrieved December 17, 2020, from https://www.citizensinformation.ie/en/government_in_ireland/european_government/eu_law/charter_of_fundamental_rights.html#l0b797
- Council of Europe. (n.d.). *Convention 108 and Protocols*. The Council of Europe portal. Retrieved December 22, 2020, from https://www.coe.int/en/web/portal/disclaimer
- Council of Europe. (n.d.). *Details of Treaty No.001*. The Council of Europe portal. Retrieved December 22, 2020, from https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/001
- Council of Europe. (n.d.). *Privacy and data protection*. The Council of Europe portal. Retrieved December 22, 2020, from https://www.coe.int/en/web/freedom-expression/privacy-and-data-protection-explanatory-memo
- The Council of Europe. (1950). *Convention for the Protection of Human Rights and Fundamental Freedoms*. Rome.
- The Council of Europe. (1981). *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*. Strasbourg.
- Court of Justice of the European Union. (n.d.). *General Presentation*. Court of Justice of the European Union. Retrieved December 23, 2020, from https://curia.europa.eu/jcms/jcms/Jo2_6999/en
- Densmore, R. (Ed.). (2019). *Privacy Program Management; Tools for Managing Privacy Within Organization* (Second ed.). IAPP Publication.
- DiPiazza, S. A., & Eccles, R. G. (2002). Building public trust: The future of corporate reporting. https://www.semanticscholar.org/paper/Building-Public-Trust%3A-The-Future-of-Corporate-Eccles-DiPiazza/8130b8b2492850709c754646265704e234a9e901
- *The Directive on security of network and information systems (NIS Directive)*. (2020, December 16). An official website of the European Union. Retrieved December 18, 2020, from https://ec.europa.eu/digital-single-market/en/directive-security-network-and-information-systems-nis-directive
- European Commission; High-level Expert Group on Artificial Intelligence. (2019). *Ethics guidelines for trustworthy AI*. European Commission.
- European Data Protection Board. (n.d.). *About EDPB*. An official website of the European Union. Retrieved December 23, 2020, from https://edpb.europa.eu/about-edpb/about-edpb_en
- The European Parliament and The Council of The European Union. (2016). *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*. Luxembourg: Office for Official Publications of the European Communities.
- The European Parliament and The Council of The European Union. (2016). *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*. Luxembourg: Office for Official Publications of the European Communities.

- The European Parliament and The Council of The European Union. (2018). *Directive (EU) 2016/680 — protecting individuals with regard to the processing of their personal data by police and criminal justice authorities, and on the free movement of such data*. Luxembourg: Office for Official Publications of the European Communities.
- The European Parliament., & Office for Official Publications of the European Communities. (2000). *Charter of fundamental rights of the European Union*. Luxembourg: Office for Official Publications of the European Communities.
- European Union Agency for Fundamental Rights & Council of Europe. (2014). *Handbook on European data protection law*. Council of Europe. 10.2811/69915
- *General presentation*. (n.d.). European Court of Human Rights. Retrieved December 21, 2020, from https://echr.coe.int/Pages/home.aspx?p=home
- *General Presentation*. (n.d.). Court of Justice of the European Union. Retrieved December 21, 2020, from https://curia.europa.eu/jcms/jcms/Jo2_6999/en/
- Hijmans, H., & Raab, C. (2018). Ethical Dimensions of the GDPR. In *Commentary on the General Data Protection Regulation*. Edward Elgar. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3222677
- Knockaert, M., Van Gyseghem, J.-M., Friedewald, M., & Lindner, R. (2020). Report on ethical, legal and societal aspects. In *Strategic programs for advanced research and technology in Europe*. Sparta.
- Koops, B.-J. (2015). The Concepts, Approaches, and Applications of Responsible Innovation. In *Responsible Innovation 2: Concepts, Approaches, and Applications*. Springer International.
- Koops, B.-J., Clayton Newell, B., Timan, T., Skorvanek, I., Chokrevski, T., & Galic, M. (2017). A Typology of Privacy. *Penn Law: Legal Scholarship Repository*. https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1938&context=jil
- Kosti, N., Levi-Faur, D., & Mor, G. (n.d.). Legislation and regulation: three analytical distinctions. *The Theory and Practice of Legislation*, *7*(3). https://www.tandfonline.com/doi/full/10.1080/20508840.2019.1736369
- Mantelero, A., Monte, N., Christodoulaki, M., & Hölbl, M. (2020). *Legal Framework - CyberSec4Europe*.
- Mulgan, R. (n.d.). 'Accountability': An Ever-Expanding Concept? *Wiley Online Library*. https://doi.org/10.1111/1467-9299.00218
- Organisation for Economic Cooperation and Development (OECD). (1980). *Guidelines Governing the Protection of Privacy and Transborder Flow of Personal Data*.
- *Proposal for directive on measures for high common level of cybersecurity across the Union*. (2020, December 16). An official website of the European Union. Retrieved December 18, 2020, from https://ec.europa.eu/digital-single-market/en/news/proposal-directive-measures-high-common-level-cybersecurity-across-union
- Rawls, J. (1999). *A Theory of Justice* (Revised ed.). Harvard University Press.
- Sloot, B. (2017). Legal fundamentalism: is data protection really a fundamental right? In *Data Protection and Privacy: (In)visibilities and Infrastructures* (pp. 1-24). Springer. https://www.springer.com/gp/book/9783319507958
- Solove, D. J. (2008). Understanding Privacy. *Harvard University Press*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1127888

- *Statute of the Council of Europe*. (n.d.). Council of Europe. Retrieved December 21, 2020, from https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/001
- Swire, P., & Kennedy-Mayo, D. (2020). *U.S. Private-Sector Privacy; Law and Practice for Information Privacy Professionals* (Third ed.). IAPP Publication.
- Taleb, N. N. (2018). *Skin in the Game*. Random House.
- Turilli, M., & Floridi, L. (2009). The ethics of information transparency. *Ethics and Information Technology*, *11*, 105-112. 10.1007/s10676-009-9187-9
- *Types of EU law*. (n.d.). An official website of the European Union. Retrieved Decenber 21, 2020, from https://ec.europa.eu/info/law/law-making-process/types-eu-law_en
- Ustaran, E. (Ed.). (2018). *European Data Protection Law; Law and Practice*. IAPP Publication.
- Vaccaro, A., & Madsen, P. (2006). Firm Information Transparency: Ethical Questions in the Information Age. In *An information society for all? In remembrance of Rob Kling* (pp. 145–156). New York: Springer.
- Warren, S. D., & Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review*, *4*(5), 193-220.
- *When does the Charter apply?* (n.d.). An official website of the European Union. Retrieved December 17, 2020, from https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/eu-charter-fundamental-rights/when-does-charter-apply_en