Cyber-security toolbox
for connected medical devices

D2.1 ANALYSIS OF ETHICAL, LEGAL AND DATA PROTECTION FRAMEWORKS

Revision: v.2.0

Work package	WP 2
Task	Task 2.1
Due date	31/8/2023
Submission date	17/07/2023
Deliverable lead	KUL
Version	2.0
Authors	Dusko Milojevic (KUL)
Reviewers	Maja Nisevic (KUL)
Reviewers	Anton Vedder (KUL)
Reviewers	João Rodrigues (INOV)

Abstract	T2.1 provides an overview of the relevant applicable ethical, legal and regulatory frameworks, with a particular focus on data protection, privacy and cybersecurity in the context of CYLCOMED, in order to identify the key principles and rules of relevance that should be considered in the general setting of the project.

Keywords	Medical devices, Data and privacy protection, Cybersecurity, Artificial intelligence

DOCUMENT REVISION HISTORY

Version	Date	Description of change	List of contributor(s)
V0.1	06/06/2023	1st draft	KUL
V1.0	05/07/2023	Revision	INOV
V2.0	17/07/2023	Final version of the deliverable	KUL

Disclaimer

Copyright notice

Project co-funded by the European Commission in the Horizon Europe Programme		
Nature of the deliverable:	ETHICS, SECURITY	
Dissemination Level		
PU	*Public, fully open, e.g. web*	
SEN	*Sensitive, limited under the conditions of the Grant Agreement*	**x**
Classified R-UE/ EU-R	*EU RESTRICTED under the Commission Decision No2015/ 444*	
Classified C-UE/ EU-C	*EU CONFIDENTIAL under the Commission Decision No2015/ 444*	
Classified S-UE/ EU-S	*EU SECRET under the Commission Decision No2015/ 444*	

* *R: Document, report (excluding the periodic and final reports)*
DEM: Demonstrator, pilot, prototype, plan designs
DEC: Websites, patents filing, press & media actions, videos, etc.
DATA: Data sets, microdata, etc
DMP: Data management plan
ETHICS: Deliverables related to ethics issues.
SECURITY: Deliverables related to security issues
OTHER: Software, technical diagram, algorithms, models, etc.

Executive summary

With the rise of cyber threats addressed at connected medical devices, the need to develop new security solutions is more obvious than ever. CYLCOMED addresses the overall ambitious goal of strengthening the cybersecurity of connected medical devices (CMDs), in vitro diagnostic medical devices (IVDs) and software as medical devices (SaMD).

The development and use of CYLCOMED technology fall under the scope of several legal regimes, such as data protection, cybersecurity, medical devices, and artificial intelligence frameworks. These legal frameworks raise numerous legal requirements and obligations which have to be taken into account in the development and design of CYLCOMED technology. However, it is also crucial to maintain compliance with domain specific requirements of ethics and privacy while simultaneously enhancing security.

This deliverable is the first report on the legal and ethical framework in the CYLCOMED project, covering a relatively wide spectrum of legal domains that are applicable to the project. As this deliverable falls under Task 2.1 (T2.1), ”Identification of Ethical and Legal Frameworks”, which is the first task of Work Package 2 (WP2) “Legal, Ethical and Regulatory Issues”, it aims to provide a preliminary ethical and legal analysis and guidance from the onset of the CYLCOMED. Therefore, this deliverable aims to establish a first rough draft of the relevant ethical and legal framework which needs to be taken into account in the course of the project’s lifetime.

It is important to note that this deliverable will provide the basis for subsequent deliverables within Work Package 2 (WP2) of the CYLCOMED. Bearing in mind that the project is in the initial stage, the following deliverables might extend the legal and ethical analysis to frameworks that are not included in this deliverable in accordance with the development of CYLCOMED technical solutions.

Contents

List of figures

List of tables

Abbreviations

Abbreviation	Definition
AI	Artificial Intelligence
ALTAI	The Assessment List for Trustworthy Artificial Intelligence
CAR	Cyber Resilience Act
CER	Critical Entities Resilience Directive
CTIS	Clinical Trial Information System
CSIRTs	Computer Security Incident Response Teams
CMD	Connected Medical Device
CJEU	Court of Justice of the European Union
CoE	Council of Europe
CSA	Cybersecurity Act
CTD	Clinical Trials Directive
CRT	Clinical Trial Regulation
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
EEA	European Economic Area
EC	European Commission
ECHR	European Convention on Human Rights
ECCRI	European Code of Conduct for Research Integrity
ECtHR	European Court of Human Rights
EHDS	European Health Data Space
EDPB	European Data Protection Board
EEA	European Economic Area
EHDS	The European Health Data Space
EHR	Electronic Health Record
EMA	European Medicines Agency
ENISA	European Union Agency for Cybersecurity
EU	European Union
GCP	Good Clinical Practice
GDPR	General Data Protection Regulation
HE	Horizon Europe
HIS	Health Information System
HLEG AI	High-Level Expert Group on Artificial Intelligence
ICO	UK's Information Commissioner’s Office
IMP	Investigational medicinal products
IVDR	In Vitro Diagnostic Medical Devices Regulation
MDD	Medical Device Directive
MDCG	Medical Device Coordination Group
MDR	Medical Devices Regulation
NIS2	Network and Information Security Directive
RED	Radio Equipment Directive
SaMD	Software as Medical Device
SW	Software
TFEU	Treaty on the Functioning of the European Union

UDHR	Universal Declaration of Human Rights
WP	Work Package
WP29	Working Party 29

1 Introduction

Healthcare technologies have the potential to save and enhance lives. These technologies may range from those providing storage of electronic health records, devices that monitor patients' health condition and deliver medication, to telemedicine technology delivering care remotely.[1] As healthcare technologies continue to advance, they are becoming more and more interconnected and integrated into larger IT networks and systems. While the interconnectedness has multiple advantages (e.g. remote monitoring and cost reduction), it also poses significant challenges. The issue of cyberattacks targeting medical devices and hospital networks is among the major challenges nowadays. Cybersecurity of connected medical devices has become a matter of great significance and pressing concern. Malicious actors have the capability to hack pacemakers and insulin pumps, shut down hospital networks, and steal personal health information.[2] For instance, researchers have demonstrated that it is possible to remotely hack implanted insulin pumps and pacemakers-flooding the body with a deadly dose of insulin or releasing a heart-stopping electric charge.[3] Unsurprisingly, there are growing concerns that cybersecurity within healthcare is not sufficient and this has already resulted in a lack of medical information confidentiality and integrity of data.

CYLCOMED addresses the overall ambitious goal of strengthening the cybersecurity of connected, in vitro diagnostic and software as medical devices, maintaining their performance and safety for patients and preserving or enhancing the confidentiality, integrity and availability of private data they exchange or allow to be remotely accessed and focusing on humans operating the technology as the weakest link in the chain for security and privacy. It does so by enabling adoption by all ecosystem stakeholders of technologically sovereign and trustworthy cybersecurity methodologies and toolboxes for connected medical devices and the environments in which they are managed and operate (platforms), complemented with fit-for-purpose guidance covering identified risks and gaps. For this purpose, a methodological and technical cybersecurity framework designed for healthcare services that use CMDs will be developed. Its performance and applicability will be demonstrated by implementing the developed tools in two dedicated pilots. While Pilot 1 "Cybersecurity in Hospital Equipment for COVID-19 ICU patients", will be carried out as a digital twins simulation without the involvement of any human participants, Pilot 2 "Cybersecurity for Telemedicine Platforms" will be conducted as an observational study.

1.1 Purpose and Scope

Our society is undergoing a rapid digital transformation, due to advancements in technologies such as artificial intelligence, machine learning, robotics, and the internet of things. These emerging technologies pose various legal and ethical challenges. Although law and ethics are closely intertwined, it is important to establish their

relationship at the beginning of this deliverable. While laws stipulate what must, can or cannot be done, ethical notions about good and bad behaviour lie behind these stipulations.[4] According to Rochel, ethics fulfils three important functions, namely: **coordinative** function which provides actors with common principles; a **red-line** function of clarifying practices which should be prohibited; and the **gap-filling function** of providing justification for specific actions. In doubt regarding the legal norms or where the law has no clear answer, “ethics is used to jump in and address the problematic situation”.[5] New technologies are an example of where the law lags behind and where ethics play a crucial role, paving the way to legal norms. The field of artificial intelligence is the most obvious example where ethics (Ethics guidelines for trustworthy AI) shapes legal solutions, on the one hand, and act as the guidance in absence of legally binding norms. Additionally, importance of ethics can be illustrated by the European Data Protection Supervisor’s statement that “In today’s digital environment, adherence to the law is not enough; we have to consider the ethical dimension of data processing”.[6]

Next, this deliverable aims to provide a preliminary ethical and legal analysis and guidance at the onset of the CYLCOMED project. Therefore, the purpose of this document is to inform and guide CYLCOMED Consortium partners of their legal obligations concerning the positive[7] international and EU norms on privacy and data protection, cybersecurity, artificial intelligence and clinical trials. Moreover, this legal and ethical inventory should guide the architects and developers of the CYLCOMED toolbox who are creating the technical and functional specifications of the use cases, so they take into consideration the ethical principles and legal requirements at the early stages of the toolbox design.

It will establish a first rough draft of the relevant ethical and legal framework in order to identify the fundamental principles and rules of relevance that should be considered in the general setting of the project. The jurisdictional scope of this deliverable is international law and law of the European Union (EU). Besides the positive legal framework, this deliverable will provide an overview of the most relevant legislative initiatives which are undergoing through legislative procedure due to its relevance and possible influence at the CYLCOMED design.

It is important to note that while this deliverable will provide a first overview of the requirements for legal and ethical compliance, on the one hand, it will provide the basis for subsequent deliverables within Work Package 2 (WP2) of the CYLCOMED, on the other.

1.2 Structure

The legal and ethical analysis in this document is performed within the five main chapters: Privacy and Data Protection, Cybersecurity of CMD, Artificial Intelligence, Clinical trials and Research ethics. Each chapter lays down the legal framework comprising the principal normative acts relevant to the theme of the chapter, briefly explaining the subject matter and its relevance to CYCOMED.

Chapter 2 covers the principal theme of privacy and data protection. It provides an overview of primary and secondary sources. It is followed by Chapter 3 which provides an overview of cybersecurity framework related to connected medical devices.

Chapter 4 analyses documents related to the AI legal and ethical framework, whereas Chapter 5 provides an overview of the clinical trial regulations. The 6th chapter, Research Ethics, identifies the most important ethical considerations. Chapter 7 presents the concluding remarks.

2 Privacy and Data Protection Legal framework

This chapter will give an overview of the main regulatory instruments applicable to the CYLCOMED technology under the privacy and data protection regime in Europe. The analysis will cover the relevant international treaties, primary and secondary sources of EU legislation in this domain.

However, it is important to firstly distinguish the notion of privacy against that of data protection. Despite the fact that privacy and personal data protection are two interrelated terms that are often used interchangeably, it is important to note that they actually constitute two discrete and different notions.[8] On the one hand, the right to privacy emerged in the Universal Declaration of Human Rights (UDHR), which was adopted in 1948. The European Convention on Human Rights (ECHR), adopted in 1950, which builds upon UDHR, provided that everyone has the right to respect for his or her private and family life, home and correspondence.[9] The idea of privacy derives from concepts such as human dignity and the rule of law and it generally refers to the protection of an individual's "personal space".[10] On the other hand, data protection refers to limitations or conditions on the processing of data relating to an identifiable data individual. Data protection instruments were established at the European level since the 1970s during which some states in Europe started to adopt their own, related legislations.[11] In 2000, the Charter of Fundamental Rights of the EU recognised data protection as an autonomous right, which marked the final point of a long evolution, separating privacy and data protection.[12] The right to personal data concerns situations in which personal data is processed, regardless of the relationship and impact on privacy.

The label "fundamental rights" is commonly used as an umbrella term that mirrors universal values such as human dignity, equality, and solidarity. Fundamental rights can often be understood as providing the justification for concrete legal standards, instruments and mechanisms. While fundamental rights can be understood as moral rights, they are realised in concrete legal arrangements.[13] For instance, the GDPR gives substance to the fundamental right to personal data protection, specifying this fundamental right in a number of detailed rights of the data subject that have legal effects. Likewise, laws concerning the proper conduct of elections can be understood as rooted in a concern to protect the fundamental right to vote and the right to free and fair elections.[14]

2.1 European Convention on Human Rights

The European Convention on Human Rights (ECHR) is the first Council of Europe's[15] convention and the cornerstone of all its activities. It was adopted in 1950 and entered into force in 1953. The ECHR is an international instrument, ratified by the 47 member states of the Council of Europe, which protects human rights and political freedoms in Europe. [16] Contracting Parties that have ratified the ECHR have an international obligation to comply with the he rights stipulated in the Convention.[17]

The right to personal data protection forms part of the rights protected under Article 8 of the ECHR, which guarantees the right to respect for private and family life, home and correspondence. According to Article 8(2), this right can be restricted only 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.

Taking into account that CYLCOMED consortium activities will include processing of special category of personal data, which falls under the Article 8 of the ECHR,[18] CYLCOMED shall fully comply with the ECHR.

2.2 Council of Europe Convention 108

The Council of Europe Convention for the protection of individuals concerning the automatic processing of personal data (Convention 108) entered into force in 1985 and still remains open for signatures.[19] It was the first and the only legally binding international instrument in the data protection domain.[20] The purpose of the Convention is to secure the rights and fundamental freedoms of individuals, in particular, the right to privacy, with regard to the automatic processing of personal data.[21] Convention 108 applies to all data processing carried out by both the private and public sectors, including data processing by the judiciary and law enforcement authorities.

Although Convention 108 dates back to 1982 and has a larger geographical reach than the GDPR, the both legal frameworks more or less follow the same logic.[22] To date, 55 countries are party to the Convention 108.[23] Here it is worth noting that Convention 108 is binding for states that have ratified it. Each Party State is required to apply this Convention to data processing subject to its jurisdiction in the public and private sectors and to take necessary measures in its law to give effect to the provisions of this Convention and secure their effective application. Additionally, the Convention is not subject to the judicial supervision of the European Court of Human Rights (ECtHR) but has been taken into consideration in the case law of the ECtHR within the context of Article 8 of the ECHR.[24]

It is important to note that, in comparison to GDPR, Convention 108 is an International treaty which is legally binding for states that have ratified it, whereas GDPR is an EU data protection law, legally binding for the EU Member States. While GDPR lays down

strict rules regarding the processing of personal data, Convention 108 contains general principles for data protection.[25] In terms of material scope, Convention 108 is consistent with the majority of the GDPR requirements, although in a less perspective form. The GDPR will be elaborated on in section 2.4 of this deliverable.

Convention 108 underwent three amendments. The first occurred in 1999 when the European Communities were allowed to join the treaty, while the second amendment took place in 2001, which incorporated new obligations related to the existence of supervisory authorities and transborder data flow.[26] Due to the significant advancement of technology and the processing of personal data in a digital environment, Convention underwent significant modernisation in 2018,[27] also called Convention 108+. The aim of modernisation was both to address privacy challenges from new technologies and to strengthen enforcement.

The Convention provides a benchmark for CYLCOMED to understand the fundamental rights that all individuals from the Contracting States enjoy with regard to the processing of personal data.

2.3 Charter of Fundamental Rights

The Charter of Fundamental Rights (Charter) is the European Union's bill of human rights which entered into force with the Treaty of Lisbon on 1 December 2009.[28] The Charter applies to EU institutions, bodies, offices and agencies in all their actions, and Member States have a duty to respect the rights guaranteed by the Charter when they are implementing EU law.[29] The right to personal data protection, enshrined in Article 8 of the Charter is of particular importance for the CYLCOMED project.

Article 8(1) stipulates that everyone has the right to the protection of personal data concerning him or her, whereas Article 8(2) prescribes that 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. Additionally, Article 8 (2) grants the right to access data that has been collected concerning a particular individual.

Taking into account the fact that the Charter explicitly raises the level of personal data protection to that of a fundamental right in EU law, the design and deployment of the CYLCOMED technology shall take into consideration the rights and freedoms guaranteed by the Charter, specifically the protection of personal data.

2.4 General Data Protection Regulation (GDPR)

The GDPR entered into force on 25 May 2018, replacing Directive 95/46/EC (the GDPR).[30] The material scope is set out by Article 2, which prescribes that GDPR applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a

filing system or are intended to form part of a filing system. Therefore, in order to ensure a high level of protection, the GDPR applies to any processing of personal data. Regarding the territorial scope, the GDPR applies to the European Economic Area (EEA), including all EU countries and Lichtenstein, Iceland, and Norway. The GDPR applies to processing of personal data in the context of activities of a controller or a processor based in the EU, regardless of where the actual processing takes place[31]. It also applies to a controller or a processor based outside of the EU if they process the personal data of individuals in the EU and offer goods or services to, or monitor the behaviour of individuals within the EU.[32]

By providing cybersecurity solutions to enhance the cybersecurity of connected medical devices, the CYLCOMED project will necessarily engage in processing personal data. Moreover, it is foreseen that special categories of personal data will be processed. More specifically, throughout the project lifespan, it is envisaged that the health-related and children data will be processed. Therefore, in order to enable and facilitate compliance, it is essential that the legal requirements set out by the GDPR are taken into consideration by the developers of the CYLCOMED technical solution from the outset of the design process. As processing special categories of personal data is essential to the design of CYLCOMED, this section will provide a more detailed overview of the relevant regulatory requirements.

The analysis will start with the notion of the personal data, and followed by legal grounds for the processing of personal data. It then moves on to discussing the key actors responsible for compliance and elaborates on the obligations each of the actors has. The data subject rights will be elaborated, while the importance of data protection officer and data protection impact assessment will be described. Elaboration on the rights the data subjects enjoy concerning their data is then put forward. Finally, this chapter ends up with pointing out importance of data protection officer and data protection impact assessment for the CYLCOMED project.

2.4.1 Personal Data

GDPR Article 2(1) sets out that the Regulation applies to *the* ***processing*** *of* ***personal data.*** Therefore, personal data is a threshold concept for the application of data protection law in general. Thus, it is important to introduce these definitions more closely.

- "**'Personal data'** means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."[33]
- "**'Processing'** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or

alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."[34]

The Article 29 Working Party (WP29), which is the predecessor of the European Data Protection Board (EDPB), further provided guidelines which shed more light on the definition of personal data, interpreting that the definition of "personal data" is constituted of four building blocks, namely:

- ***Any information;*** The expression "any information" underlines the intention of the legislator for the broad interpretation of the personal data. Therefore, personal data may include any information. For instance, information can either be "objective" (e.g., the identification of substances in blood samples), as well as "subjective" (e.g., in the form of opinions). It is not important for the information to be true, proven or complete, as long as it relates to a person;[35]
- ***Relating to;*** WP29 clarifies that the "relating to" element is crucial since it provides the relationship between the individual and information. It states that, in general terms, the information relates to an individual if it is about the individual. For instance, the details of a patient's diagnostic examination found in her/his medical history are clearly related to that patient;[36]
- ***Identified or identifiable;*** The person to which the information relates must also be identified or identifiable. A person is "identified" when they can be directly distinguished or "singled out" from a larger group of persons, based on identifiers, such as the name, identification number, locations, or physical, physiological identity of a particular individual;[37]
- ***Natural person;*** This building block means that subjects to the protection of personal data are all living natural persons, whereas data on legal persons (e.g. corporations) and data relating to deceased persons[38] are not protected by the GDPR.

2.4.2 Key roles under the GDPR

Understanding the key roles in relation to the processing of personal data is crucial in ensuring compliance with the GDPR requirements. There are three crucial roles in the processing of personal data under the GDPR:

- data controller,
- data processor, and
- data subject.

Since there are multiple GDPR obligations imposed on the controllers and processors, it is essential to introduce the concepts of “data controller” and “data processor” in more depth. The most important consequence of being a controller or a processor is a legal responsibility for complying with the obligations under GDPR.

2.4.2.1 Controller

Article 4(7) GDPR defines a controller as the “natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data”. GDPR sets no limitation in terms of the legal form of the controller, and everyone with legal capacity can be a controller when processing personal data, including individuals, private legal entities, or government entities.

The essential element and the main building block of the controllership is the determination of the *purpose* and *means* of the processing activity. If an entity has decision-making power over determining the "purpose" of processing it, de facto, constitutes that entity as controller. In order to assess whether someone exercises decision-making power, EDPB Guidelines[39] proposes that questions "Why is this processing taking place?” and “Who decided that the processing should take place for a particular purpose?”, should be taken into consideration.

While the controller typically solely determines the purpose of processing and its essential elements, the means of processing can be delegated to the processor to some extent. The EDPB Guidelines here differentiate the determination of “essential” (e.g. which data shall be processed, length of storage, who shall have access and what security measures need to be taken) and “non-essential means” (e.g. choice of the hardware or software, or the detailed security measures). While the controller must determine the purposes and means of the processing, some more practical aspects of implementation (“non-essential means”) can be left to the processor.[40] In some cases, especially in complex situations where many subjects are involved in the processing, the identification of the controller might bear significant challenges.

2.4.2.2 Joint controllership

The situation in which two or more entities determine the purpose and means of the processing constitutes a “joint” or “co-controllership”. The key element for assessing the existence of joint controllership is the joint participation of two or more entities in the determination of the purposes and means of a processing operation. GDPR Article 26 defines the scope and responsibilities of joint controllers while pointing out that they must have an arrangement in place that specifies their roles and responsibilities for compliance with the GDPR requirements.[41] Failure to conclude such an arrangement may be subject to a severe fine, according to GDPR Article 83 (4)(a).

It is important to note that joint controllership does not necessarily involve equal involvement in determining the purpose and means of processing activities, and, therefore, there are many possible arrangements among the parties involved. The joint controllership may vary from a very close relationship (e.g., sharing all purposes and means of processing) or a more loose relationship (e.g., partially sharing purposes).[42] Moreover, the mutual relationship between joint controllers can occur at different stages and with different degrees of processing. Consequently, responsibility for compliance with GDPR requires a case-by-case analysis and assessment of the involvement of each entity encompassed by joint controllership. However, in regard to data subject rights, it is essential to note that, despite the arrangement among the joint controllers, GDPR Article 26(3) entitles the data subject with the opportunity to exercise its rights against each of the controllers.

2.4.2.3 Processor

Under GDPR Article 4(8) processor is defined as "a natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller". For an entity to be qualified as the processor, it is essential that two crucial criteria are met, namely: the entity must be a *separate* legal entity with respect to the controller and the processing of personal data must be made on the controller's behalf.[43] Therefore, there is a significant distinction between a data controller and a data processor. The former is the natural or legal person who **determines the purposes** and the means of processing, whereas the processor is the natural or legal person **who processes the data on behalf of the controller**. The role of a processor is derived from the controller's decision to outsource the processing to another entity. However, apart from determining the purpose and means of processing, the controller is allowed to process the personal data, in which case he embodies the role of controller and processor at the same time.

The controller may outsource processing activities to multiple processors, for different purposes or separate stages of processing (multiple processors). [44] Besides, the controller may decide to authorise the processor to engage one or more processors ("subprocessor(s)").[45] However, the borders for processing are always set out by the controller (purpose and means), to which the processor must be confined. If the processor steps out of the processing framework determined by the controller (e.g. processor carries out the processing for its own purpose), the processor infringes the GDPR by going beyond the controller's instructions. In such case, the processor shall be considered to be a controller in respect of that processing and may be subject to fines for non-compliance.[46]

2.4.2.4 Relationship between controller and processor

Under GDPR Article 28(1), the controller "shall use processors who are able to provide sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject". In other words, the controller is

responsible for the assessment of whether the processor meets criteria of “sufficient guarantees”. To that end, GDPR Recital 89 states that an approved code of conduct or an approved certification mechanism may be used as an element to demonstrate compliance with the obligations of the controller. Additionally, EDPB recommends that when assessing sufficient guarantees, processors’ expert knowledge, reliability, resources, and market reputation should be taken into consideration.[47]

The relationship between controller and processor, as stipulated by GDPR Article 28(3), shall be governed by a contract or other legal act under Union or Member State law, and such contract or other legal act shall be in writing, including in electronic form (GDPR Article 28(3)). To demonstrate the existence of the contract, as well as facilitate the execution of defined obligations among the interested parties, EDPB recommends ensuring that the necessary signatures are included in the legal act[48]. GDPR Article 28(3)(4) has left at discretion to controller and processor to, either negotiate their own contract or to rely, in whole or in part, on standard contractual clauses in relation to obligations under Article 28(3)(4). However, EDBP recommends that instead of merely restating GDPR Article 28, a legal act between interested parties should be drafted in light of the specific data processing activity, with clearly specified mutual obligations. More specifically, according to EDBP’s interpretation of GDPR Article 28(3), an agreement between the controller and processor must include, at least, the following elements, namely: the **subject matter** of the processing, the **duration** of the processing, the **nature** of the processing; the **type of personal data;** the **categories of data subjects;** the **obligations and rights of the controller.[49]**

2.4.2.5 The obligations of the controller and the processor

Another important distinction among them is the scope of obligations under the GDPR. While the controller is subject to stricter obligations, such as responsibility for GDPR compliance and implementation of the appropriate technical and organisational, the processor is subject to limited compliance responsibilities.

2.4.3 Privacy and data protection principles

A responsible data controller must follow the principles outlined in GDPR to ensure compliance and protect the personal data collected from individuals. The principles provide guidance for everyone who is required to be GDPR compliant.

According to GDPR Article 5(2), the controller is accountable for and must be able to demonstrate compliance with these basic principles. In other words, this means that any processing of personal data through CYLCOMED shall be guided by data protection principles illustrated by the graphic below:

2.4.3.1 Lawfulness, fairness and transparency

Article 5(1)(a) GDPR sets out that data "*shall be processed lawfully, fairly and in a transparent manner in relation to the data subject*". The **lawfulness** principle requires that the data processing is based on legitimate grounds stipulated by GDPR Article 6 for non-sensitive personal data, and Article 9, for special categories of personal data, which will be elaborated in detail in the following sections due to its importance and relevance to CYLCOMED.

The principle of **fairness,** which is enshrined in Article 8(2) of the EU Charter, represents the overall requirement of the GDPR that extends beyond transparency requirements and is closely linked to processing personal data in an ethical manner[50]. Guidelines 4/2019 on Data Protection by Design and by Default provide a non-exhaustive list of some aspects of fairness which should always be respected while processing personal data.[51] The list encompasses, inter alia, elements such as data subject autonomy in controlling the processing, non-discrimination, taking into account ethical considerations such as assessing the broader impact on individuals' rights through processing, and the right to fair algorithms.[52]

The principle of **transparency** imposes an obligation upon the controller to inform data subjects about what data are being collected, how their data are being used, consulted or otherwise processed, and the risks involved in processing. [53] Although GDPR does not explicitly define the principle of transparency, its Recital 39 elaborates that processing operations must be explained to the data subjects in an easily accessible way, ensuring they understand what will happen to their data, while using clear and plain language. The principle of transparency is embedded in GDPR Articles 12, 13, 14 and 34, which give substance to this principle. Furthermore, Guidelines 4/2019 on Data Protection by Design and by Default provide an exemplary list of crucial design and default elements for the principle of transparency which should be respected while

processing personal data.[54] Besides, detailed elaboration on how to understand the concept of transparency can be found in Article 29 Working Party Guidelines on transparency. [55]

2.4.3.2 Purpose limitation

The principle of purpose limitation, also enshrined in Article 8(2) of the EU Charter, requires that any processing of personal data must be done for a specific, well-defined purpose and only for additional purposes that are compatible with the original purpose.[56] It means that the purpose should be defined before processing personal data and unambiguously expressed. Lawful processing is confined to the initially specified purpose, while further processing must be based on separate legal grounds. Any processing of personal data for undefined, unspecified or unlimited purposes shall be regarded as unlawful.

However, when it comes to further processing, GDPR envisages exceptions from the general rule that further processing is not allowed. As set out in GDPR Article 6(1)(b), “further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with GDPR Article 89(1), not be considered to be incompatible with the initial purposes”. Namely, further processing for the aforementioned purposes is considered compatible with the initial purpose if appropriate safeguards are in place (both technical, *e.g. encryption, pseudonymisation*, and organisational, e.g. *appointment of a Data Protection Officer (DPO))*.

2.4.3.3 Data minimisation

GDPR sets out that personal data shall be “adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed”.[57] It can be seen that the data minimisation principle is closely linked to the principle of purpose limitation. It imposes requirements upon the controller to limit the processing of personal data to what is necessary for the purposes for which they are processed. From the technical side, data minimisation principle is implemented through privacy-enhancing technologies or other measures such as pseudonymisation.

2.4.3.4 Data accuracy

Under the GDPR Article 5(1)(d), data controllers must keep personal data accurate and take every reasonable measure to ensure that inaccurate personal data are erased or rectified without delay. The controller has a duty to actively keep records accurate. In case he fails, controllers are liable for the accuracy of the personal data they process, no matter which technology they use. Personal data processed through CYLCOMED must be accurate and up to date and checked regularly.

2.4.3.5 Storage limitation

As set out by Article GDPR Article 5(1)(e), personal data shall 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*”. As soon as personal data are no longer needed for the purposes for which they were collected, controllers are obliged to erase or anonymise collected data.

An exception from the aforementioned general rule that data storage should be proportionate to the data collection’s length and purpose, personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1). In such cases, implementation of the appropriate technical and organisational measures is required by GDPR in order to protect the rights and freedoms of the data subject.

2.4.3.6 Integrity and confidentiality

Personal data must be processed in a manner that ensures their appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.[58] When implementing technical or organisational measures, the “one size fits all” approach should be avoided, and the specific circumstances of each case should be analysed. A risk-based approach should be implemented in order to assess the correlation between the risk likelihood and severity for the rights and freedoms of natural persons.

GDPR Article 32(1) sets out that the state of the art, the costs of implementation and the nature, scope, context and purpose of processing should be taken into account while assessing which technical or organisational measures should be put in place. They may include pseudonymisation and encryption of personal data, regularly testing and evaluating the effectiveness of the measures to ensure the data processing is secure, and implementation of a professional secrecy obligation.[59] Hence, based on an assessment of risks CYLCOMED design must ensure the integrity and confidentiality of the data, as well as regular review of the security measures so that they may be updated as necessary.

2.4.3.7 Accountability principle

As set out by GDPR Article 5(2), the controller is responsible for ensuring compliance with GDPR principles and is obliged to demonstrate such compliance. Although this principle obliges the controller solely, it is essential to note that GDPR, through several norms, holds processors accountable for compliance.[60] While this provision does not specify how a controller is required to demonstrate compliance, it can be done in various ways which will depend on the specific circumstances of each case. Some examples of how controllers can facilitate compliance are the designation of a data protection officer, data protection impact assessments, recording processing activities,

implementation of appropriate technical and organisational measures and ensuring data protection by design and by default, to mention just a few compliance mechanisms.

2.4.4 Lawful grounds for processing personal data

In general, it is not allowed to process any data unless there is at least one legal ground explicitly prescribed by GDPR. Article 6(1) GDPR provides an exhaustive list of six potential legal bases for processing personal data, as illustrated by the graph below:

2.4.4.1 Consent

Article 8 of the Charter, Article 5 (2) of Convention 108+ and Article 6 of the GDPR explicitly define consent as the possible legal basis for processing personal data. GDPR envisages numerous requirements that controllers have to comply with to obtain valid consent. GDPR 4(11) sets out the essential requirements that consent has to meet in order to be a lawful ground for the processing:

- **Freely given;** Consent has to be freely given, which means that the data subjects have genuine choice and control. GDPR Recital 42 stipulates that consent is not considered freely given “if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment”. Likewise, Recital 43 delineates that there is a presumption of consent not being freely given if “it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service is dependent on the consent despite such consent not being necessary for such performance”. Next, there is also a presumption that consent is not freely given if the process/procedure for obtaining consent does not allow data subjects to give separate consent for

personal data processing operations respectively, despite it being appropriate in the individual case.[61] Recital 42 also states that the controller needs to demonstrate that it is possible to refuse or withdraw consent without detriment.

- **Specific;** This requirement stems from the transparency principle, which means that processing purpose or purposes must be explicitly specified, using clear and plain language. In the case when the processing has various purposes, consent should be given for all of them (granularity).[62] Therefore, controllers should provide a separate opt-in for each purpose, to allow users to give specific consent for specific purposes.[63]
- **Informed;** Prior to giving consent, data subjects need to understand what they are agreeing to, and be aware of the fact that they are giving consent and of the scope of that consent. GDPR Recital 42 sets out minimum elements that "informed consent" needs to fulfil, namely controller identity and purpose of each of the processing activities. Furthermore, for consent to be informed, data subjects must also be aware of the consequences of not consenting to the processing and of the right to withdraw consent.[64] Means of providing information to the data subject can include written or oral statements, audio or video message.
- **Unambiguous;** GDPR Article 4(11) states, inter alia, that all consent must be given in an unambiguous way, which means that data subjects must give their consent by an explicit affirmative action. According to the GDPR Recital 32, consent can be given in writing (on paper or by electronic means) or through an oral statement. However, an oral statement as means of giving consent bears some difficulties for the controller to prove that all conditions for valid explicit consent were met.[65] On the other hand, silence, pre-ticked boxes or inactivity are not deemed acceptable.

The GDPR Article 7(1) clearly outlines the explicit obligation of the controller to demonstrate a data subject's consent, meaning that the burden of proof will be on the controller. Recital 42 states "where the processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation." It is equally important to point out that data subjects can withdraw their consent at any time, and data subjects should be made aware of this right before granting consent. This withdrawal should be as easy as giving consent, but will not retroactively affect any processing based on previously obtained consent. Article 7(3) GDPR clarifies that the withdrawal of consent must be as simple as the granting of consent.

2.4.4.2 Contract

According to the GDPR Article 6(1)(b), processing of personal data is also lawful when it is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract. Therefore, this legal ground applies in cases where at least one condition is met:

- the processing in question must be objectively necessary for the performance of a contract with a data subject, or
- the processing must be objectively necessary in order to take pre-contractual steps at the request of a data subject.

EDPB Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR provide further guidance on the matter.[66]

2.4.4.3 Legal obligation

The GDPR recognises that controllers may be obliged to collect, store, and process personal data. Under Article 6(1)(c), such processing operations are considered lawful if they are necessary to fulfil these obligations, whereas the legal obligation must originate directly from the law. The Member State or Union law should determine the purpose of processing to qualify as the lawful ground.

2.4.4.4 Vital interests

GDPR Article 6 (1) (d) prescribes that personal data processing is lawful if it “is necessary in order to protect the vital interests of the data subject or of another natural person”. Recital 46 clarifies that vital interests are ”essential for the life” of the data subject. Therefore, these legal grounds come to the fore only in exceptional cases, such as humanitarian emergencies and pandemics. Consequently, this legal ground for processing should be invoked only if the processing cannot be based on another legal basis.[67]

2.4.4.5 Public task

Article 6(1)(e) of the GDPR sets out that personal data may lawfully be processed if it “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”. This ground is the general basis for the lawful processing of personal data, which may be used by any controller who is exercising official authority or carrying out a specific task in the public interest, as long as the processing is necessary. Just like for personal data processing activities grounded on a “legal obligation”, the GDPR does not require a specific law for each individual processing, but either the EU or Member State law should determine the purpose of processing.[68]

In such a case, there should be a basis in either EU or Member State law (Art. 6 (3)) whether the controller performing such a task in the public interest or in the exercise of official authority should be a public authority or another natural or legal person governed by public law, or, where it is in the public interest to do so by private law. Just like for personal data processing activities based on a legal obligation, the GDPR does not require a specific law for each individual processing, but the law should determine the purpose of processing (Rec. 45).

2.4.4.6 Legitimate interests

GDPR Article 6(1)(f) sets out legitimate interest as a legal ground for the processing of personal data. To rely on this legal basis, the data controller must ensure that 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. While GDPR Article 6(1)(f) does not clarify what could constitute a legitimate interest, Recital 47 provides clarification on where this legal basis could be used. For instance, when processing personal data is strictly necessary to prevent fraud or the processing of personal data for direct marketing purposes. Opinion, 06/2014 of the WP29 on ”legitimate interests” under Directive 95/46/EC[69] provides a non-exhaustive list of some of the most common contexts in which the issue of legitimate interest in the meaning of Article 7(f) may arise, including here, for instance, prevention of fraud, misuse of services, or money laundering, employee monitoring for safety or management purposes and physical security, IT and network security.

In the context of the CYLCOMED project, it is important to point out that IT and network security can constitute legitimate interest as a legal ground for the processing of personal data. The example given for this by the GDPR Recital 49 is preventing unauthorised access to electronic communications networks and malicious code distribution and stopping ‘denial of service’ attacks and damage to computer and electronic communication systems.

However, before any processing activity, it is essential to determine that processing does not override the interests or fundamental rights and freedoms of the data subject. Moreover, how to conduct such a balancing test is not further clarified. Some guidance can be found in the aforementioned Opinion on ”legitimate interests”, which suggests a multi-step procedure. First, controllers ought to verify whether their interest is actually “legitimate”. Second, they need to identify the data subject’s interests, rights and freedoms. Third, they have to establish whether the controller’s interests are overridden by those of the data subject. Likewise, The UK's Information Commissioner’s Office (ICO) produced more detailed guidance[70] on legitimate interests, which proposes the three-part test to assess whether legitimate interest can be a lawful ground for the processing of personal data (purpose test, necessity test and balancing test), and which should be conducted before processing starts. It is important to note that legitimate interest as a legal basis cannot be invoked by public authorities for processing carried out in the performance of their tasks.

Controllers should assess which legal ground is the most suitable for data processing activities taking into account the purpose of processing. It is important to note that there is no hierarchy of legal basis for the lawful processing of personal data: all are equally valid. The GDPR does not give preference to one legal ground over another nor states that one is more suitable or more important than the others. The choice of legal basis will depend on the specific circumstances of each case. While there must be at least

one legal ground for lawful data processing, GDPR does not exclude the possibility of defining more legal grounds.

2.4.5 Processing of special categories of data

Some personal data are more sensitive in nature and, thus, enjoy higher protection under the GDPR. The GDPR refers to these "sensitive" personal data as special categories of personal data. Since the processing of special categories of personal data under GDPR Article 9 is deemed as high-risk processing regarding the rights and freedoms of individuals, these types of personal data merit specific protection, and, therefore, GDPR requires an additional layer of protection. GDPR Article 9(1) sets out that "*processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of 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* ***shall be prohibited***". However, despite this general rule that processing sensitive data is prohibited in principle, GDPR Article 9(2) lays the ground for exceptions if certain conditions are met. More specifically, the abovementioned article defines an exhaustive list of ten exceptional cases in which processing sensitive data is possible. Moreover, it is essential to accentuate that GDPR Article 9(4) allows Member States to maintain or introduce further conditions, including limitations, regarding the processing of genetic data, biometric data or data concerning health. Since the processing of sensitive data is the subject of a much stricter legal regime, it is crucial to assess and determine the legal basis for such processing carefully.

Bearing in mind that the CYLCOMED project will necessarily engage in processing special categories of personal data in its use case, it is essential to establish an additional legal basis for processing such data. Therefore, to ensure the lawful processing of sensitive data within the scope of the CYLCOMED project, apart from legal grounds listed in GDPR Article 6, it is crucial to establish an additional legal basis for processing data relating the health. Given the context in which the CYLCOMED will be conducted, the cumulative legal ground might be found in some of the exceptions under GDPR Article 9(2):

- **Explicit consent** - "*The data subject has given explicit consent to the processing of those personal data for one or more specified purposes"* [GDPR Article 9(2)(a)]. In contrast to "regular" consent defined by the GDPR Article 6(1)(a), for lawful processing of sensitive personal data, explicit consent is required. EDBP Guidelines clarify that the term "explicit" refers to the way consent is expressed by the data subject.[71] How it is expressed will depend on context and case by case basis. Examples of such consent provided by the Guidance may include "written and signed statements", "statement by filling in an electronic form, by sending an email, by uploading a scanned document carrying the signature of the data subject, or by using an electronic signature", or even by telephone (e.g. pressing a button or providing oral confirmation).

- **Employment, social security and social protection law** - “Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject”.[72]
- **Protection of vital interests** – “Processing is necessary **to protect the vital interests** of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent”. [73]
- **Association or Non-profit organisations** – “*Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects*”.[74]
- **Manifestly made public data** – “processing relates to personal data which are **manifestly made public** by the data subject**”.[75]**
- **Legal claims** – “*processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity”*.[76]
- **Substantial public interest –** “*processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject*”.[77]
- **Health or social care** – “*Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to a contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3*”.[78] GDPR Article 9(3) contains the additional safeguard if this exception is to be used as the legal basis. It can be lawful ground if the personal data is being processed by (or under the responsibility of) a professional who is subject to an obligation of professional secrecy.
- **Public interest –** “Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular, professional secrecy”.[79]

- **Archiving/ Research or Statistical purposes** – "processing is **for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes** in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject".[80]

It is worth repeating that this is an exhaustive list of exceptions, and each exception must be interpreted restrictively. Equally important, these exceptional cases for processing sensitive data must be additionally supported by the legal ground defined by the GDPR Article 6. More specifically, it is obligatory to determine a lawful basis under GDPR Article 6 and a condition for processing special category data under GDPR Article 9. In the context of the CYLCOMED project, besides the consent, the processing of health data for the purposes of cyber-security in a hospital could be grounded based on art. 6(1)(c) (legal obligation) or art. 6(1)(e) GDPR (task in the public interest) together with art. 9(2)(g) (substantial public interest) or art. 9(2)(i) GDPR (public interest in the area of public health).

Furthermore, it is essential to point out that GDPR Article 9(4) allows Member States to maintain or introduce further conditions, including limitations regarding the processing of data concerning health. Therefore, it is advisable that CYLCOMED partners check their specific legal requirements for processing special categories of data in the health sector.

2.4.6 Data subject's rights

Individuals are granted eight rights under the GDPR to safeguard their privacy. GDPR imposes an obligation on controllers to facilitate the exercise of these data protection rights irrespective of the specific technical circumstances of the processing operation. The controller is required to provide information regarding these rights prior to data collection and upon request from the individual. The GDPR grants data subjects the following rights:

2.4.6.1 Right to be informed

The right to be informed stems from the transparency principle, which empowers individuals, inter alia, to have insight into how their data is processed. GDPR Articles 13 and 14 specify the types of information that the controller needs to provide to the data subject, regardless of whether the data subject shows interest in the information or not. Recital 39 further clarifies that data subjects have the right to be aware that their data are processed and to be informed about the processing activities, the risks, the safeguards, and their data protection rights. Next, GDPR Articles 13 and 14 set out the scope of information that must be provided to the data subject depending on whether they are obtained directly, or indirectly from the data subject, as follows:

- **Identity and contact details of the controller** (and of its representative, where applicable);

- **Contact details of the DPO, where applicable;** The contact details of the DPO should include information allowing data subjects and the supervisory authorities to reach the DPO in an easy way (a postal address, a dedicated telephone number, and/or a dedicated e-mail address).[81]
- **Purposes and the legal basis for the processing;** Apart from the purpose for processing**,** this information needs to include legal ground for processing under Article 6, as well as under Article 9 if the special category of data will be processed.
- **Categories of personal data concerned;** This information is not required if the controller obtained information directly from the data subject.
- **Legitimate interests** pursued by the controller or by a third party, where applicable;
- **Recipients** of the personal data, if any;
- **Details whether the data will be transferred** to a third country/international organisation (and corresponding adequacy decision or safeguards);
- **Storage period**, or criteria used to calculate the storage period;
- **The data protection rights**; This information should be specific to the context of the CYLCOMED project and the data subject must be informed about the rights (access; rectification; erasure; restriction; object; data portability) and how these rights can be exercised;
- If the legal basis is consent, the existence of the right to withdraw consent;
- **Right to lodge a complaint** with a supervisory authority;
- **Information on whether the provision of personal data is a statutory or contractual requirement;** This information is not required if the controller did not obtain information directly from the data subject;
- **Existence of automated decision-making**, including profiling, if any;
- **Information about the further processing of the data**, where applicable;
- **The source of the collected data;** This information is not required if the controller obtained information directly from the data subject.

It is important to note that GDPR Article 13 obliges the controller to inform the data subject about the aforementioned information at the time when personal data are obtained. By contrast, GDPR Article 14 refers to situations in which data are obtained without the knowledge of the data subject, and, therefore, the data subject is unaware of that fact. Hence, when the data have not been directly obtained from the data subject, the controller must provide the information within a reasonable period after obtaining the personal data, and at the latest within a month from the day of the indirect collection. If the obtained personal data are to be used for communication with the data subject, the controller must provide information at the latest at the time of the first communication to that data subject. Eventually, Article 14(3)(c) GDPR sets out that if

the personal data are to be disclosed to another recipient, then the controller must provide all mandatory information under Article 14 GDPR at the latest when the personal data are first disclosed.

The aforementioned information shall be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.[82] Regarding the means of communicating information to data subjects, GDPR Article 12(1) sets out that information shall be provided **in writing**, or **by other means** (cartoons, infographics or flowcharts),[83] including, where appropriate, **by electronic means** (e.g. “just-in-time” contextual pop-up notices, 3D touch or hover-over notices, and privacy dashboards[84]). Information may be provided **orally** if requested by the data subject, in which case the controller must have otherwise verified the data subject’s identity.[85] If the data controller intends to further process the personal data for a purpose other than the initially communicated purpose, the information must be provided prior to that further processing with information on that other purpose.[86] Where the processing is addressed to a child, data controllers should pay particular attention to how they present information to children and be mindful of situations where there are multiple actors and technological complexity.[87]

2.4.6.2 Right of access

GDPR Article 15 embodies the Right to access, which is specifically recognised under the EU Charter of Fundamental Rights.[88] It enables data subjects to access their personal data which have been obtained and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing[89]. Therefore, controllers are obliged to provide access to information with regard to the processing purposes, where possible the period for which the personal data are processed, the recipients of the personal data, the logic involved in any automatic personal data processing and, at least when based on profiling and the consequences of such processing.[90] Hence, the primary goal is to provide data subjects with sufficient, transparent and easily accessible information about the processing of their personal data so that they can be aware of and verify the lawfulness of the processing and the accuracy of the processed data.[91]

Since GDPR does not prescribe any formal requirements in terms of the form of the request, the data subject is free to choose the means of communicating the request to the controller. To facilitate the right to access, controllers are encouraged to develop a user-friendly communication environment, and, where possible direct remote access to personal data.[92] Likewise, EDBP Guidelines provide examples of good practice in regard to the exercise of data subjects' rights, such as autoresponder systems to inform of staff absences and appropriate alternate contact.[93] Under GDPR Article 15 controller is obliged to provide information either by a copy or in a commonly used electronic form if the data subject makes the request by electronic means. If later is the case, EDBP advises that the controller has to consider appropriate technical and organisational measures, including adequate encryption when providing information via e-mail or online self-service tools.[94] Moreover, subject to particular circumstances,

EDBP is of the opinion that it could be appropriate for the controller to provide access through other ways (e.g. oral information or an inspection of files).[95]

GDPR Article12(3) set out that the controller shall provide information to the data subject without undue delay and in any event within one month of receipt of the request. However, taking into account the complexity and the number of requests, the deadline can be extended by a maximum of two months, in which case the data subject must be informed about the reasons causing the delay. Additionally, controllers are allowed to reject the request for access if the request is manifestly unfounded or excessive,[96] if it adversely affects the rights and freedoms of others,[97] or when such restriction is stipulated by the Member States' national law.[98]

2.4.6.3 Right to rectification

Under GDPR Article 16 data subject is entitled to obtain the rectification of inaccurate data and to have incomplete personal data completed, without undue delay. The platform must enable these corrections in an easy and timely manner.

2.4.6.4 Right to erasure ("Right to be forgotten")

GDPR Article 17 entitles data subjects to request from data controllers the erasure of their personal data, in certain circumstances. It imposes an obligation upon the controller to erase personal data without undue delay where one of the following grounds applies:

- the personal data is no longer necessary for the purposes for which they were collected;
- the data subject withdraws consent on which the processing is based, and there is no other legal ground for the processing to continue;
- the data subject objects to the processing based on the legitimate interests of the controller or carried out in the public interest, and there are no overriding legitimate grounds for the processing, or when the data subject objects to the processing of their data for direct marketing purposes;
- processing has been unlawful;
- the personal data have to be erased for compliance with a legal obligation;
- collected in the context of the offer of information society services to children.[99]

Additionally, GDPR Recital 66 extends the right to erasure to the online environment clarifying that the controller has an obligation to inform other controllers of the request to delete all links, copies or replications of the data, through appropriate technical and cost-effective measures.

However, GDPR Article 17 (3) sets out exceptions to the right to erasure, some of which could be particularly relevant for CYLCOMED:

- for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- if the processing is necessary for public health purposes in the public interest (e.g. ensuring high standards of quality and safety of health care and of medicinal products or medical devices);
- if the processing is necessary for the purposes of preventative or occupational medicine; for the working capacity of an employee; for medical diagnosis; for the provision of health or social care; or for the management of health or social care systems or services. This only applies where the data is being processed by or under the responsibility of a professional subject to a legal obligation of professional secrecy (e.g. a health professional).
- archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

2.4.6.5 Right to restriction of processing

Under GDPR Article 18 data subject is entitled to temporarily restrict the processing of their personal data where:

- the accuracy is contested by the data subject,
- the processing is unlawful, and the data subject opposes the erasure of the personal data and requests the restriction of their use instead,
- the data are not necessary for the purpose of processing but must be kept for legal claims,
- the data subject has objected to processing pursuant to Article 21(1) pending the verification of whether the legitimate grounds of the controller override those of the data subject.

If the data subject invokes the right to restriction, apart from storing personal data, the controller is not allowed to share, disclose, erase, or perform any other type of processing operation on them, unless a specific exception applies (e.g. consent of the data subject or public interest of the Union or of a Member State).[100] GDPR Recital 67 states that some of the methods for application of the right to restrict can include temporarily moving the selected data to another processing system, making the selected personal data unavailable to users, or temporarily removing published data from a website.

2.4.6.6 Right to data portability

Right to data portability aims to strengthen the data subject's ownership over the data provided to the controller and empowers data subjects to decide what they want to do with their personal data. More specifically, GDPR Article 20 allows data subjects to receive the personal data that they have provided to a controller, in a structured, commonly used and machine-readable format, and to transmit those data to another data controller.

GDPR enables data subjects to invoke the right to portability only when:

- the lawful basis for processing this information is consent or the performance of a contract

  and

- the processing is carried out by automated means.

Data available only in paper form and manually processed are out of the scope of data portability right. Additionally, the right to have personal data transmitted directly from one controller to another will depend on the technical feasibility. Hence, transmission between controllers could occur when communication between two systems is possible. However, if technical impediments bar direct transmission, the data controller needs to provide information to the data subject regarding the technical impediments.[101] While GDPR does not specify the format of the personal data to be provided, W29 Guidelines recommends that "Where no formats are in common use for a given industry or given context, data controllers should provide personal data using commonly used open formats (e.g. XML, JSON, CSV,…) along with useful metadata at the best possible level of granularity, while maintaining a high level of abstraction". [102]

To accommodate the right to data portability, CYLCOMED partners are encouraged to develop interoperable formats and tools (e.g. download tools and Application Programming Interfaces) which will facilitate the exercise of data subject right to data portability.

2.4.6.7 Right to object

Under GDPR Article 21 data subjects have the right to object to the processing of their data, in certain circumstances. GDPR stipulates four specific cases in which the data subject is entitled to invoke the right to object:

- where personal data are processed for the performance of a task carried out in the public interest or the controller's legitimate interest;[103]
- where personal data are processed for direct marketing purposes;[104]
- where personal data are processed by automated means in the context of information society services;[105]

- where personal data are processed for scientific, historical, or statistical purposes;[106]

In cases where **personal data are processed for direct marketing purposes** data subject is entitled to object processing at any time, in which case the controller is obliged to stop any further processing.[107] In contrast with the objecting to processing for direct marketing purposes which gives the data subject absolute right, under GDPR Article 21(1) controllers may refuse the data subject's objection if they demonstrate compelling legitimate grounds for the processing activity which overrides the data subject's interests, rights, and freedom or the processing is for the establishment, exercise or defence of legal claims. Likewise, if the processing is necessary for the performance of a task carried out for reasons of public interest controllers may refuse the data subject's objection.

2.4.6.8 Right not to be subject to automated decision-making

The GDPR Article 4(4) defines profiling as: "*any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular, to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements*". Generally speaking, profiling entails analysis and predictions based on the gathered information about the data subject (e.g. interests, economic situation, health, behaviour) in order to place them in a certain category, or group.[108] Since profiling carries many risks (e.g. discrimination), GDPR Article 22(1) sets out that data subjects have the right not to be subject to automated decision-making that produces a legal or similarly significant effect. However, GDPR Article 22(2) prescribes exceptions to this general prohibition in cases:

- where the decision is necessary for the entry into contract or the performance of a contract,
- when it is authorised by EU or Member State law applicable to the controller or
- when it is based on the individual's explicit consent.

If automated decision-making involves special categories of personal data, it will be only allowed where the explicit consent of the data subject is given, or where processing is necessary for reasons of substantial public interest.[109] However, under these exceptions controller is obliged to put in place suitable measures to safeguard the data subject's rights and freedoms and legitimate interests.

When designing the CYLCOMED, it is important to consider the data controller's responsibility to comply with data subject rights. This involves developing technical solutions that are in line with the GDPR requirements and make it easy for individuals to exercise their rights. The purpose of the data processing should be clearly defined and communicated to data subjects, especially if it involves automated decision-making or profiling. The data controller must go through several verification stages to

ensure that the processing is based on the proper legal basis for processing personal data, as well as specific data processing and processing for the purpose of automated decision-making or profiling. It is crucial to take these steps to protect the privacy and rights of data subjects from whom data are processed for the purpose of the CYLCOMED project.

2.4.7 Data Protection Officer

GDPR Article 37(1) imposes an obligation on controllers and processors to designate data protection officer in three (3) specific cases:

- where the processing is carried out by a public authority or body;
- where the core activities of the controller or the processor consist of processing operations, which require regular and systematic monitoring of data subjects on a large scale; or
- where the core activities of the controller or the processor consist of processing on a large scale of special categories of data or personal data relating to criminal convictions and offences.

Although GDPR does not specify what constitutes a “public authority or body”, WP29 is of the opinion that public authority or body is to be determined by Member State law.[110] Regarding the notion of the “core activities”, GDPR Recital 97 clarifies that “the core activities of a controller relate to its primary activities and do not relate to the processing of personal data as ancillary activities”, whereas WP29 further states that core activities should be interpreted as “the key operations necessary to achieve the controller’s or processor’s goals”.[111] Moreover, the WP29 has clarified that the “core activities” should not be interpreted in such a way that they exclude processing operations that form an inextricable part of the controller’s or processor’s activities. For example, a hospital that provides medical services is the example used by the WP29 to illustrate core activites. To deliver health care, a hospital would need to process health data. According to the WP29, processing data in this situation should be regarded as one of a hospital's essential functions, and the hospital would be required to designate a DPO.[112]

While the term “large-scale processing” is not explicitly defined in the GDPR, Recital 91 briefly clarifies which operations should be deemed large-scale processing.[113] On the other hand, WP29 Guidelines shed more light on what should be considered as large-scale processing by recommending the four (4) factors that should be taken into consideration when assessing whether the processing is large-scale:

- The number of data subjects concerned - either as a specific number or as a proportion of the relevant population,
- The volume of data and/or the range of different data items being processed,
- The duration, or permanence, of the data processing activity,
- The geographical extent of the processing activity.

One of the examples given for large-scale processing by the WP29 is the processing of patient data in the regular course of business by a hospital. In contrast, processing personal data by an individual physician, other health care professional or lawyer should not be considered large-scale processing.[114]

Since the processing activities performed through CYLCOMED will fall under the specific cases defined by the GDPR Article 37(1), designation and oversight of a DPO will be required.

2.4.8 Data Protection Impact Assessment

To be able to demonstrate compliance with GDPR controllers are in some cases obliged to carry out a Data Protection Impact Assessment (DPIA). GDPR Article 35(1) states that controllers must carry out a DPIA before any processing that is "likely to result in a high risk to the rights and freedoms of natural persons". Next, in accordance to the GDPR Article 35(3) DPIA is particularly necessary where:

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

  or
- systematic monitoring of a publicly accessible area on a large scale."

The Article 29 Working Party is of the view that these cases do not constitute an exhaustive list, and a DPIA may also be required for other types of processing which are not explicitly mentioned by the cited article.[115] Moreover, in order to further clarify operations that require a DPIA due to their inherent high risk, WP29 developed a set of ten (10) criteria to help to determine whether a data protection impact assessment is required in a specific case.[116]

The most relevant criteria in the context of the CYLCOMED project are:

- Evaluation or scoring, including profiling and predicting, especially from "aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements";
- Sensitive data, as set out by GDPR Article 9;
- Data processed on a large scale;
- Data concerning vulnerable data subjects, in particular processing personal data of children;[117]
- Innovative use or applying technological or organisational solutions;

The WP29 recommends that in each case where more than two criteria are met, DPIA is required, as well as in cases where it is not possible to determine whether data protection impact assessment is required.[118] Regarding the content of the data protection impact assessment, GDPR Article 35(7) sets out minimum requirements for the scope of the DPIA as follows:

- A systematic description of the purposes and envisaged processing operations and, where applicable, the legitimate interest pursued by the controller;
- An assessment of the necessity and proportionality of the processing in relation to the purpose;
- An assessment of the risks to the rights and freedoms of the data subjects;

  and
- The measures envisaged to address the risks.

If the DPIA results reveal that the data processing could result in a high risk in the absence of measures taken by the controller to mitigate the risk, the controller must seek the advice of the national data protection authority before proceeding with the processing of data.[119]

2.4.9 Notification of a personal data breach

GDPR Article 4(12) defines “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”. If not addressed promptly and appropriately, a data breach may cause severe damage to data subjects, such as discrimination, financial loss, identity theft or fraud.[120]

Hence, GDPR Article 33(1) sets out that “in the case of a personal data breach, the controller shall **without undue delay** and, where feasible, **not later than 72 hours after having become aware of it**, **notify the personal data breach to the supervisory authority** competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.”

While GDPR does not provide further clarification at which moment the controller becomes “aware”, WP29 is of the opinion that “a controller should be regarded as having become “aware” when that controller has a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised.”[121] GDPR Article Art. 33 (3) outlines the minimum information that must be encompassed in the notification to enable the supervisory authority to take appropriate action:

- description of the nature of the personal data breach;

- name and contact details of the data protection officer or other contact point where more information can be obtained;
- consequences of the personal data breach;
- measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

In addition to notifying the supervisory authority, when a data breach is likely to result in a high risk to the rights and freedoms, controllers are also obliged to inform the data subject without undue delay.[122]

The CYLCOMED design must facilitate compliance with the described obligations and, in particular, enable the controller (or processor) to collect all the information detailed under GDPR Article 33 in a timely manner.

2.5 Regulation for the European Health Data Space Proposal

In May 2022, the European Commission published the legislative proposal for a Regulation for the European Health Data Space (EHDS), one of the central building blocks of a strong European Health Union.[123] The EHDS builds upon legislation such as the GDPR, the Regulation (EU) 2017/745 on medical devices (Medical Devices Regulation) and the Regulation (EU) 2017/746 on in vitro diagnostic medical devices (In Vitro Diagnostics Regulation), and the proposed Artificial Intelligence Act, with the aim to complete the regulatory canvas for the use of health data in the European Union.[124] The aforementioned legislative acts will be subject to analysis in this deliverable. The EHDS's general objective is to ensure that natural persons in the EU have increased control over their electronic health data, while at the same time ensuring a legal framework allowing researchers, innovators, policymakers and regulators to access relevant electronic health data.[125] In order to attain the general objective, the proposal establishes a set of rules and infrastructures to support the primary and secondary use of health data, as well as an European governance framework. More specifically, the EDHS:

- strengthens the rights of natural persons in relation to the availability and control of their electronic health data;
- lays down rules for the placing on the market, making available on the market or putting into service of electronic health records systems ('EHR systems') in the Union;
- lays down rules and mechanisms supporting the secondary use of electronic health data;
- establishes a mandatory cross-border infrastructure enabling the primary use of electronic health data across the Union;

- establishes a mandatory cross-border infrastructure for the secondary use of electronic health data.[126]

Electronic health data is in the current proposal defined as “personal and non-personal electronic health data”.[127] Personal electronic health data means “data processed in electronic form, concerning health and genetic data as defined by the GDPR, as well as data referring to determinants of health, or data processed in relation to the provision of healthcare services”.[128] Next, the EDHS defines the ‘primary use of electronic health data’ as “the processing of personal electronic health data for the provision of health services to assess, maintain or restore the state of health of the natural person to whom that data relates, including the prescription, dispensation and provision of medicinal products and medical devices, as well as for relevant social security, administrative or reimbursement services”.[129] Secondary use of electronic health data is defined as “the processing of electronic health data for purposes set out in Chapter IV of this Regulation. Generally speaking, secondary use concern the re-use of health data that were collected initially in the context of providing care but which may later be re-used for another purpose.[130] The data used may include personal electronic health data initially collected in the context of primary use, but also electronic health data collected for the purpose of the secondary use”.[131] Chapter IV of the Proposal is devoted to the secondary use of health data. It introduces a governance regime for health data exchanges among entities.

The proposal includes provisions that introduce, not only legal, but also institutional, and technical-infrastructural rules. For instance, Member States can establish one or more Health Data Access Bodies. These Health Data Access Bodies are responsible for granting access to electronic health data for secondary use. The Health Data Access Bodies may be either new public sector bodies, or existing public sector bodies or internal services of public sector bodies.[132] The proposal also includes provisions on health data quality and utility for secondary use. This entails that health data access bodies inform the data users about the available datasets and their characteristics through a metadata catalogue.[133]

The EHDS covers a wide range of goods, including medical devices, and services, such as remote care delivery tools, health data and information management solutions, and patient management, including telemonitoring and diagnosis. Once it is adopted, the EHDS will have an impact on electronic health records, medical devices, and telemedicine. For instance, healthcare providers will be required to ensure that data can be shared/made accessible and that electronic health records, medical devices and other systems are interoperable. Another example is that the EDHS introduces new rules for manufacturers of electronic health record systems that wish to place their products and services in the EU market, thereby complementing the existing rules established by Regulation 2017/745 on medical devices and the Regulation (EU) 2017/746 on in vitro diagnostic medical devices.[134]

The EHDS contains important provisions related to CYLCOMED, in particular on access to data for research and facilitating the establishment of infrastructures for data

sharing. However, the proposal is currently still in the legislative process. Therefore the provisions might still change considerably and will be analysed accordingly.

3 The Cybersecurity Framework

The health sector is among the most targeted sectors when it comes to cyberattacks.[135] The increasing digitalisation of healthcare service providers has enabled cyberattack techniques toward them to become more liquid, flexible, and able to exploit all the possible paths of entry rapidly. Cyberattacks on the IT infrastructure of hospitals, electronic health records, or medical devices that have taken place during the COVID-19 pandemic reaffirmed the importance and urgency of ensuring cybersecurity in the healthcare sector.[136] Therefore, ensuring cybersecurity in the health care sector is a growing concern.

It is important to note that regulating cybersecurity is a complex task. The same can be said for medical device regulation which is characterized by regulatory specialization and fragmentation.[137] Consequently, regulating cybersecurity of medical devices bears complexities of both legal frameworks.[138]

It is noteworthy to point out that the EU cybersecurity framework is comprised of several pieces of legislation that cover aspects linked to cybersecurity or some of its elements. When it comes to the legal requirements for the cybersecurity of medical devices relevant to CYLCOMED technical solution, the EU laws establishes a set of different requirements enshrined in the Medical Devices Regulation (MDR), In vitro diagnostic medical devices (IVDR), the Cybersecurity Act (CSA), the Network and Information Systems Directive (NIS2), the General Data Protection Regulation (GDPR), and the Radio Equipment Directive (RED).

Furthermore, the two legislative proposals that the EU legislator currently discusses are likely to apply to medical devices: the EU AI Act proposal and the Cyber Resilience Act (CRA). These legislative acts will be subject of analysis under this section. Additionally, although not explicitly related to cybersecurity, due to interconnectedness and importance, the Critical Entities Resilience Directive (CER) will be briefly elaborated in this section.

3.1 The Cybersecurity Act

Over the last decade, cybersecurity has become one of the top priorities for the European Union. In order to increase the cybersecurity of the European Union, in light of the increased cybersecurity challenges, European Parliament and the European Council approved the Cybersecurity Act,[139] repealing Regulation (EU) 526/2013. Cybersecurity Act (CSA) entered into force in June 2019 and became directly applicable in all EU Member States. As set out by Cybersecurity Act Article 1, CSA lays down:

- objectives, tasks and organisational matters relating to the European Union Agency for Cybersecurity (ENISA) and
- a framework for the establishment of European cybersecurity certification schemes for the purpose of ensuring an adequate level of cybersecurity for ICT products, ICT services and ICT processes in the Union, as well as for the purpose of avoiding the fragmentation of the internal market with regard to cybersecurity certification schemes in the Union."

In order to reach a common understanding, it is important to clarify the main definition used for the purposes of CSA. Hence, CSA Article 2 defines the terms "*cybersecurity certification", "ICT products", "ICT services" and "ICT processes", as follows:*

- '**European cybersecurity certificate'** means a document issued by a relevant body, attesting that a given ICT product, ICT service or ICT process has been evaluated for compliance with specific security requirements laid down in a European cybersecurity certification scheme;
- "**ICT product** means an element or a group of elements of a network or information system";
- "**ICT service** means a service consisting fully or mainly in the transmission, storing, retrieving or processing of information by means of network and information systems";
- "**ICT process** means a set of activities performed to design, develop, deliver or maintain an ICT product or ICT service';

3.1.1 The Role of ENISA

The Cybersecurity Act aims to **strengthen** the role of **ENISA** by granting the agency a permanent mandate, reinforcing its financial and human resources and overall enhancing its role in supporting the EU to achieve common and high-level cybersecurity. Cybersecurity Act gives ENISA a pivotal role in the EU cybersecurity domain. The tasks delegated to ENISA may be summarised as follows:

- Development and implementation of Union policy and law;[**140**]

ENISA is positioned as a centre of expertise in the field of cybersecurity in order to enhance the development of Union policy and law in the field of cybersecurity through, inter alia, the provision of independent opinions and analysis, providing advice, exchange of best practices between competent authorities, issuing guidelines on various topics such as risk management, incident reporting, and information sharing, especially concerning the NIS2 Directive.[141] Another important role is assisting in the annual review of Union policy activities by creating a yearly report on the status of implementation of the cybersecurity legal framework.

- Capacity-building;[142]

ENISA assists Member States in strengthening their cyber resilience and response capabilities, while also fostering competencies and skills in cybersecurity. This is achieved by providing expert knowledge to prevent, detect, analyse, and respond to cyber threats and incidents. Additionally, ENISA may assist in developing national cybersecurity strategies and policies, as well as in developing national Computer Security Incident Response Teams (CSIRTs).

- Operational cooperation at the Union level;[143]

Under this task, ENISA is called to enhance collaboration and coordination at the Union level by facilitating information sharing among Member States, Union institutions, bodies, offices, and agencies, as well as relevant private and public stakeholders on cybersecurity matters. Additionally, ENISA shall contribute to cooperation with third countries and international organisations on matters related to cybersecurity.[144]

- Cybersecurity certification and standardisation;[145]

In order to strengthen trust in the internal digital market and its competitiveness, ENISA is tasked to contribute to the establishment and maintenance of a European cybersecurity certification framework. ENISA shall monitor developments in areas of standardisation and recommend appropriate technical specifications for use in the development of European cybersecurity certification schemes, as well as prepare candidate European cybersecurity certification schemes. Besides, ENISA shall compile and publish guidelines and develop good practices, concerning cybersecurity requirements and contribute to capacity-building related to evaluation and certification processes.

- Awareness-raising and education;[146]

One of ENISA's tasks is to enhance cybersecurity awareness, which entails promoting cyber-hygiene and cyber-literacy among citizens, organisations, and businesses. Performance of this task will include, inter alia, the organisation of regular outreach campaigns to increase cybersecurity awareness, as well as coordination and exchange of best practices among Member States on cybersecurity awareness and education.

3.1.2 Certification Framework

CSA establishes the first EU wide cybersecurity certification framework to ensure a common cybersecurity certification approach in the European internal market and ultimately improve cybersecurity in a broad range of digital products and services. Certification is seen as vital for increasing the trust and security of ICT products, ICT services or ICT processes.[147] Besides, cybersecurity certification aims to overcome the fragmentation and overlapping of national cybersecurity certification schemes. Furthermore, it strives to enable a harmonised approach at the Union level to European cybersecurity certification schemes, with a view to creating a digital single market for ICT products, ICT services and ICT processes.[148]

Strategic priorities for European cybersecurity certification schemes shall be defined by the Union's rolling work programme for European cybersecurity certification, which will include at least a list of ICT products, services and processes or categories thereof that are capable of benefiting from being included in the scope of a European cybersecurity certification scheme.[149] The Union Rolling Work Programme should serve as a strategic document that enables industries, national authorities, and standardisation bodies to prepare ahead for upcoming European cybersecurity certification schemes.[150]

Cybersecurity certification schemes may be requested by the European Commission to ENISA on the basis of the Union work rolling plan for ICT Standardisation, and adopted by the Commission by means of implementing act.[151] This Act has to be endorsed by all Member States.

As set out by CSA Article 51, the European cybersecurity certification scheme needs to achieve at least the following security objectives:

- to protect stored, transmitted or otherwise processed data against accidental or unauthorised storage, processing, access or disclosure during the entire life cycle of the ICT product, ICT service or ICT process; to protect stored, transmitted or otherwise processed data against accidental or unauthorised destruction, loss or alteration or lack of availability during the entire life cycle of the ICT product, ICT service or ICT process;
- that authorised persons, programs or machines are able only to access the data, services or functions to which their access rights refer;
- to identify and document known dependencies and vulnerabilities; to record which data, services or functions have been accessed, used or otherwise processed, at what times and by whom;
- to make it possible to check which data, services or functions have been accessed, used or otherwise processed, at what times and by whom; to verify that ICT products, ICT services and ICT processes do not contain known vulnerabilities; to restore the availability and access to data, services and functions in a timely manner in the event of a physical or technical incident;
- that ICT products, ICT services and ICT processes are secure by default and by design;
- that ICT products, ICT services and ICT processes are provided with up-to-date software and hardware that do not contain publicly known vulnerabilities, and are provided with mechanisms for secure updates."

Furthermore, based on the risk level associated with the intended use of the ICT product, service or process in terms of the probability and impact of an incident, the cybersecurity certification scheme will have to specify one or more levels of assurance, namely: basic, substantial or high.[152] For instance, a high assurance level would mean that the certified product passed the highest security tests. According to Recital 86, assurance level serves as the basis for confidence that certified ICT products, services

or processes fulfil the security requirements of a specific European cybersecurity certification scheme.

European cybersecurity certification schemes will define a minimum set of elements concerning the subject matter, scope and functioning of the individual scheme, such as the scope and object of the cybersecurity certification, the detailed specification of the cybersecurity requirements and the intended assurance level (‘basic’, ‘substantial’ or ‘high’).[153]

It is important to note that 3 cybersecurity certification schemes are under development:

- The European Cybersecurity Certification Scheme on Common Criteria “EUCC”,
- The European Certification Scheme for Cloud Services “EUCS”

  and
- The European Cybersecurity Certification Scheme for 5G networks “EU5G”[154].

As required by the Cybersecurity Act Article 58, each Member State shall appoint one or more cybersecurity certification authorities at the national level that will be tasked to supervise, certify and monitor EU cybersecurity certification at the national level and to exchange at the EU level. National accreditation bodies, under certain conditions, may accredit the conformity assessment bodies (CABs), which then may act as evaluators (by auditing/testing) and/or as certifiers under the Cybersecurity Certification Scheme.

An EU cybersecurity certificate attests that an ICT product, process or service has been certified in accordance with cybersecurity certification schemes and that it complies with the specified cybersecurity requirements and rules. However, it is important to note that **cybersecurity certification is voluntary** unless otherwise specified by EU or Member State regulations.[155] Providers that want their ICT solution to be certified can apply for a certificate via a CAB, according to the rules defined in the particular certification schemes.

If ICT products, services or processes present a low risk corresponding to assurance level “basic”, the European cybersecurity certification scheme may allow for the conformity self-assessment under the sole responsibility of the manufacturer or provider of ICT products, services or processes.

One of the main ambitions of the CYLCOMED project is development of technical cybersecurity framework designed for healthcare services that use CMDs. Hence, if Consortium partners opt for cybersecurity certification of its technical solutions, the CA is of explicit relevance for the CYLCOMED project.

3.2 The NIS 2 Directive

The Network and Information Security Directive (NISD) 2016/1148/EU[156] is considered to be the first piece of EU-wide cybersecurity legislation which aimed, inter alia, to build cybersecurity capabilities across the Union and mitigate threats to network

and information systems.[157] Despite its significant achievements, such as a positive shift in the cybersecurity framework and improved cyber resilience of public and private entities, the impact assessment on the NIS Directive[158] has demonstrated its limitations over time.

The incoherent application of the NIS Directive due to the divergent Member State methodologies for identifying Operators of Essential Services (OES) was recognised as the most crucial issue.[159] For instance, in some Member States hospitals have not been recognised as the OES, thus not falling within the scope of the NIS Directive, whereas in another Member State, almost every single hospital in the country is covered by the NIS security requirements, which has led to fragmentation and uneven application of NIS rules and to fragmentation in the EU internal market.[160] Additionally, ineffective supervision, limited enforcement of the Directive and a lack of systematic information sharing among Member States are some of the identified shortcomings in the implementation of the Nis Directive. [161] Eventually, in order to address recognised weaknesses in December 2022, Directive (EU) 2016/1148 (NIS Directive) was repealed by The Directive (EU) 2022/2555 on measures for a high common level of network and information security across the Union (NIS 2 Directive). To strengthen the cybersecurity level across the Union, NIS 2 Directive lays down the following:

- obligations that require Member States to adopt national cybersecurity strategies and to designate or establish competent authorities, cyber crisis management authorities, single points of contact on cybersecurity (single points of contact) and computer security incident response teams (CSIRTs);
- cybersecurity risk-management measures and reporting obligations for entities of a type referred to in Annex I or II as well as for entities identified as critical entities under Directive (EU) 2022/2557;
- rules and obligations on cybersecurity information sharing;
- supervisory and enforcement obligations on Member States.

The NIS 2 Directive introduces significant changes in comparison to the repealed NISD. It differentiates two categories of entities that fall within the scope of the Directive, namely “essential entities” and “important entities”, which are listed in Annexes I and II of the NIS 2 Directive. The distinction between them is based on the criticality of “essential entities” and “important entities” with regards to their sector or the type of service they provide, their size as well as a compliance obligation. According to Article 3 of the NIS 2 Directive, the following entities are deemed **essential**:

- Entities of a type referred to in Annex I which exceed the ceilings for medium-sized enterprises provided for in Article 2(1) of the Annex to Recommendation 2003/361/EC.[162] Article 2(1) of the aforementioned recommendation sets out that the category of micro, small and medium-sized enterprises (SMEs) is made up of enterprises which employ **fewer than 250 persons** and which have an **annual turnover not exceeding EUR 50 million**, and/or an annual balance sheet total

not exceeding EUR 43 million. Hence, if these ceilings are exceeded by the entities of a type referred to in Annex I, they will be regarded as essential.

- Qualified trust service providers and top-level domain name registries as well as DNS service providers, regardless of their size;
- Providers of public electronic communications networks or of publicly available electronic communications services which qualify as medium-sized enterprises, as explained above;
- Public administration entities of central government as defined by a Member State in accordance with national law;
- Any other entities of a type referred to in Annex I or II that are identified by a Member State as essential entities pursuant to Article 2(2), points (b) to (e);
- Entities identified as critical entities under Directive (EU) 2022/2557 on the resilience of critical entities,[163] regardless of their size.
- Entities which Member State have identified as the operators of essential services before 16 January 2023, in accordance with Directive (EU) 2016/1148 or national law, if the Member State so provides.

Entities of a type referred to in Annex I or II which do not qualify as essential entities shall be considered to be **important entities**. NIS 2 Directive requires Member States to establish a list of essential and important entities as well as entities providing domain name registration services, by 17 April 2025.[164]

In the context of the CYLCOMED project, it is important to note that the Directive is applicable to healthcare providers who are classified under the sector of high criticality (**Annex I**), whereas manufacturers of medical devices and in vitro diagnostic medical devices are listed within the other critical sectors (**Annex II**), as it is presented below in tables 1 and 2.

Table 1

Sectors of high criticality (Annex I)	
Sector	**Type of entity**
Energy	
Transport	
Banking	
Financial market infrastructures	
Drinking water	
Waste water	

Digital infrastructure	
ICT service management (business-to-business	
Public administration	
Space	
Health	**Healthcare provider** - any natural or legal person or any other entity legally providing healthcare on the territory of a Member State[165]
	EU reference laboratories[166]
	Entities carrying out research and development activities of medicinal products[167]
	Entities manufacturing basic pharmaceutical products and pharmaceutical preparations
	Entities manufacturing medical devices considered to be critical during a public health emergency (public health emergency critical devices list)[168]

Source: Adapted for the purposes of Deliverable D2.1 from Annex I NIS 2 Directive

Table 2

Other critical sectors (Annex II)	
Sector	**Subsector**
Postal and courier services	
Waste management	
Manufacture, production and distribution of chemicals	
Production, processing and distribution of food	
Digital providers	
Research	
Manufacturing	**Manufacture of medical devices and in vitro diagnostic medical devices**
	Manufacture of computer, electronic and optical products
	Manufacture of electrical equipment
	Manufacture of machinery and equipment n.e.c.
	Manufacture of motor vehicles, trailers and semi-trailers
	Manufacture of other transport equipment

Source: Adapted for the purposes of Deliverable D2.1 from Annex II NIS 2 Directive

In order to ensure a high level of cybersecurity across the Union, NIS 2 Directive imposes many obligations upon the Member States, which may be summarised as follows:

- The adoption of a national cybersecurity strategy;[169]
- Designation or establishment of competent authorities and single points of contact responsible for cybersecurity and for the supervisory tasks;[170]
- Designation of cyber crisis management authorities and adoption of a national large-scale cybersecurity incident and crisis response plan;[171]
- Designation or establishment of one or more computer security incident response teams (CSIRTs);[172]

  and

- Cooperation among the Member States.[173]

Besides the aforementioned requirements, NIS 2 Directive mandates the Member States to establish a set of cybersecurity risk-management measures for the entities under its personal scope. More specifically, pursuant to NIS Directive Article 21(1) Member States are required to ensure that "essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services*".*

Prior to defining which measures will be taken, essential and important entities will evaluate whether they correlate to the risk posed. In that vein, responsible entities will take into account, inter alia, the level of exposure to the risk, its size, risk probability and overall risk influence on society. NIS 2 Directive Article 21(2) defines a list of elements that must be included in the cybersecurity risk-management measures while pointing out that these measures should be based on an all-hazards approach. As examples of measures, the aforementioned article includes, amongst others, policies on risk analysis and information system security, incident handling and measures to ensure human resources security, access control policies and asset management.

Another important obligation imposed upon the Member States relates to the **reporting obligations.** Member states are required to ensure that essential and important entities without undue delay notify the responsible national bodies of any incident that has a significant impact on the provision of their services.[174] To be regarded as a significant incident, NIS Directive Article 23(3) stipulates two specific conditions, namely:

- It has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned;
- It has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.

In such cases, entities affected by the significant incident are required to notify security breaches to responsible national authorities as follows:

- **Without undue delay** and in any event **within 24 hours** of becoming aware of the significant incident, **an early warning**;
- **Without undue delay** and in any event **within 72** hours of becoming aware of the significant incident, **an incident notification**;
- **A final report not later than one month** after the submission of the incident notification.

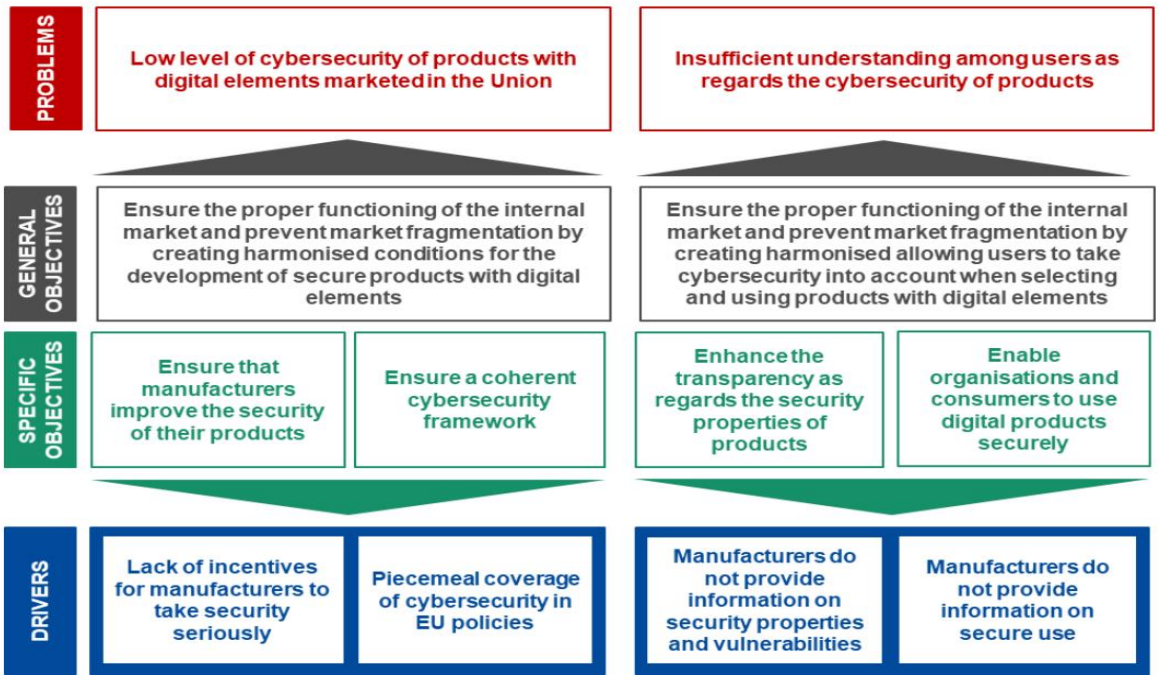
Essential and important entities which infringe legal obligations regarding the reporting of significant incidents may be subject to severe administrative fines.[175]

Since health care provider and manufacturers of medical devices and in vitro medical device are recognised as “essential entities” and “important entities”, the CYLCOMED project design shall comply with legal requirements laid out by the NIS2.

3.3 Cyber Resilience Act (CRA)

The EU Commission presented on 15th September 2022 the proposal for a Regulation on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act, CRA).[176]
Impact assessment on the CRA supports the standpoint that the adoption of CRA will fulfil the missing link in the cybersecurity legislative framework that will specifically address cybersecurity in products with digital elements.[177]
The main issues recognised by Commission’s Impact assessment are the low level of cybersecurity of products with digital elements and insufficient understanding among users as regards to the cybersecurity of products. To address these issues, CRA aims to create conditions for the development of secure products with digital elements by ensuring that hardware and software products are placed on the market with fewer vulnerabilities and that manufactures take security seriously throughout a product’s life cycle. The second main objective aims to create conditions allowing users to take cybersecurity into account when selecting and using products with digital elements.[178]
Identified issues and the CRA objectives are illustrated in the following Figure.

Figure 1 CRA Objectives



Source: Impact assessment report on the Cyber Resilience Act (CRA), p.20.

To increase the overall level of cybersecurity of all products with digital elements placed on the internal market, the CRA lays down the following:

- Rules for placing products with digital elements on the market to ensure the cybersecurity of such products;
- Essential requirements for the design, development and production of products with digital elements, and obligations for economic operators in relation to these products with respect to cybersecurity;
- Essential requirements for the vulnerability handling processes put in place by manufacturers to ensure the cybersecurity of products with digital elements during the whole life cycle, and obligations for economic operators in relation to these processes;
- Rules on market surveillance and enforcement of the above-mentioned rules and requirements.[179]

According to the CRA proposal, 'product with digital elements' means any software or hardware product and its remote data processing solutions, including software or hardware components to be placed on the market separately.[180] From this definition, it can be seen that CRA applies to a broad range of products. For instance, the CRA will be applicable to end devices (e.g., laptops, smartphones, sensors, routers) including software (e.g. mobile apps, desktop applications, video games) as well as both hardware and software components. Additionally, the CRA proposal addresses artificial intelligence systems and establishes a link with the AI Act proposal. For instance, Products with digital elements considered as high-risk AI systems under the proposed Artificial Intelligence Act must comply with the essential requirements set out by the CRA proposal.[181] However, It is important to note that the CRA proposal

excludes from its scope of applicability products with digital elements that are considered to be medical devices or in vitro diagnostic medical devices under the scope of the MDR and IVDR.[182] On the other hand, subject to its applicability, CRA imposes various obligations upon manufacturers, such as conducting mandatory security assessment requirements, implementing vulnerability-handling procedures, and providing necessary information to users.

Due to its relevance to CYLCOMED architecture and toolbox, the CRA proposal will be covered in the upcoming deliverables, since it is rather unclear how the final draft of the Regulation will look like.

3.4 The Critical Entities Resilience Directive (CER)

The Directive on the resilience of critical entities (CER)[183] was adopted in December 2022, and became legally binding in January 2023, repealing the Directive 2008/114/EC.

CER Directive, alongside with NIS 2 Directive, reflects the Union's effort to strengthen the EU's resilience against online and offline threats.[184]

One of the key goals of CER Directive, as set by Recital 43, is to reduce vulnerabilities and strengthen the physical resilience of critical entities in the EU in order to ensure the uninterrupted provision of services that are vital for the economy and society. According to Recital 43, CER Directive establishes a comprehensive framework that focuses on enhancing the resilience of critical entities against all types of hazards whether natural or man-made, accidental or intentional.[185]

It is important to note that CER Directive excludes from its scope matters covered by NIS 2 Directive since cybersecurity is adequately addressed by the NIS 2 Directive, which imposes comprehensive requirements on a large set of entities to ensure their cybersecurity.[186] However, CER Directive highlights the importance of cooperation and information exchange among relevant authorities on cybersecurity risks, cyber threats and cyber incidents and non-cyber risks, threats and incidents affecting critical entities, especially due to the hybrid nature of threats to critical entities[187]. Moreover, Member States are called to ensure that obligations imposed by CER Directive and NIS 2 Directive are implemented in a complementary manner in order to avoid duplication, as well as to avoid exposing critical entities to additional administrative burdens.[188]

On the other hand, in the context of the CYLCOMED project, particularly use case 2, it is noteworthy to address the main requirements imposed by the CER Directive since it addresses healthcare providers as subjects of compliance with CER Directive obligations. However, it is important to first introduce some of the main definitions provided by the Directive.

Pursuant to CER Directive Article 2(1), a **critical entity** may be public or private entity identified by a Member State in accordance with a number of criteria, and belonging to one of the sectors listed in the Annex.[189]

Critical **infrastructure** is defined as “an asset, a facility, equipment, a network or a system, or a part of an asset, a facility, equipment, a network or a system, which is necessary for the provision of an essential service”.[190] In turn, an **essential service** is “a service which is crucial for the maintenance of vital social functions, economic activities, public health and safety, or the environment”.[191]

CER Directive lays down various obligations that Member States and critical entities must comply with. Requirements imposed upon Member States may be summarised as follows:

- Adopt a national strategy[192] and carry out regular risk assessments[193];
- Identify entities that provide essential services to society, the economy, public health and safety or the environment, taking into account the outcomes of the risk assessment;[194]
- Support the identified critical entities in enhancing their resilience with, for instance, advice and training;[195]
- Designate or establish one or more competent authorities responsible for the correct application and, where necessary, enforcement of the rules set out in the CER Directive;[196]
- Ensure that national authorities have the powers, resources and means to carry out their supervisory tasks, including conducting on-site inspections of critical entities and introducing penalties for non-compliance as part of an enforcement mechanism;[197]

  and

- Cooperation between the Member States;[198]

In regard to critical entities, CER Directive requires that they carry out risk assessments to identify risks that could disrupt their ability to provide essential services, within nine months after being notified that they have been identified as critical entities.[199]Next, critical entities are obliged to take technical, security and organisational measures to enhance their resilience.[200] These measures should be appropriate and proportionate to the risks they face so as to prevent, protect against, respond to, resist, mitigate, absorb, accommodate and recover from an incident, including measures necessary to, inter alia, ensure adequate physical protection of their premises and critical infrastructure and ensure adequate employee security management, duly considering measures such as setting out categories of personnel who exercise critical functions, establishing access rights to premises, critical infrastructure and sensitive information.[201]

Critical entities are required to notify the competent authority, without undue delay, of incidents that significantly disrupt or have the potential to significantly disrupt the provision of essential services. Additionally, critical entities must submit an initial notification within 24 hours of becoming aware of an incident, unless they are

operationally unable to do so. A detailed report should be submitted within one month.[202]

At this stage, it is rather unclear how the final draft of the Regulation will look like. It will have to be further analysed what are the practical implications of the upcoming Regulation on CYCOMED project. Eventually, it is important to note that CER Directive has to be transposed into national law by 17 October 2024.

Healthcare providers, as operators of essential services, must take security measures to comply with CER Directive security requirements, especially taking into account the duration of the CYLCOMED project.

3.5 Medical Devices Regulation (MDR)

The Medical device regulation (MDR) was adopted in April 2017 and became legally binding on 26th May 2017.[203] In addition, MDR is a vertical legislative act, directly applicable to all Member States, without the need to be transposed into national laws, thus contributing to the harmonisation of medical device legislation in Europe.

MDR Recital 2 points out that the Regulation aims to ensure the smooth functioning of the internal market as regards medical devices, taking as a base a high level of protection of health for patients and users, and taking into account the small and medium-sized enterprises that are active in this sector. Additionally, MDR establishes rules regarding the placing on the market, making available on the market or putting into service of medical devices for human use and accessories for such devices in the Union.[204]

Prior to proceeding with the most relevant legal MDR requirements in the context of the CYLCOMED project, it is noteworthy to introduce the definition of medical devices. Pursuant MDR Article 2(a), a medical device is any instrument, apparatus, appliance, software, implant, reagent, material or other article intended by the manufacturer to be used, alone or in combination, for human beings for one or more of the specific medical purposes, such as follows:

- Diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease;
- Diagnosis, monitoring, treatment, alleviation of, or compensation for, an injury or disability;
- Investigation, replacement or modification of the anatomy or of a physiological or pathological process or state;
- Providing information by means of in vitro examination of specimens derived from the human body, including organ, blood and tissue donations, and which does not achieve its principal intended action by pharmacological, immunological or

metabolic means, in or on the human body, but which may be assisted in its function by such means.

The scope of items classified as medical devices is extensive and encompasses nearly all diagnostic or therapeutic devices and materials, with the exception of those primarily utilising pharmacological, immunological, or metabolic methods. For instance, under the scope of the definition falls everything from plaster, and disposable gloves to pacemakers and radiation systems.[205] Additionally, it can be seen that MDR applies to **software** that is intended by the manufacturer to be used, alone or in combination, for human beings for one or more purposes listed above. It is important to note that not all types of software are classified as medical devices. MDR Recital 19 provides brief clarification in which cases software should not be regarded as a medical device. It states that software for general purposes, even when used in a healthcare setting, or software intended for life-style and well-being purposes is not a medical device. Medical Device Coordination Group (MDCG) Guidance sheds more light on this matter.[206]

According to the Guidance document, software qualifies as a medical device if it:

- Directly controls a medical device (e.g. radiotherapy treatment software),
- Provides decision-advancing information (e.g. blood glucose meter software)

  or

- Provides support to healthcare professionals (e.g. ECG interpretation software).

It can be seen that MDR illustrates the focus of legislators on ensuring that devices placed on the EU market are fit for the new technological challenges linked to cybersecurity risks. However, it is interesting to note that the MDR does not expressly refer to cybersecurity.[207]

One of the important initial considerations which need to be taken into account at the onset of the CYLCOMED project relates to whether the CYLCOMED solution falls under the scope of the MDR.

The mobile application tool developed in the CYLCOMED project is likely to qualify as a “medical device” under the MDR, therefore it is useful to briefly mention its security-related provisions.

Furthermore, in order to be compliant with MDR, manufacturers are obliged to meet various legal and ethical requirements throughout the entire lifecycle of a device prior to the market release of a medical device.

MDR defines manufacturers as “the natural or legal person who manufactures or fully refurbishes a device or has a device designed, manufactured, or fully refurbished and markets that device under its name or trademark”.[208] Pursuant to MDR Article 5(1) manufacturer is obliged to ensure that the device is compliant with the MDR obligations when used in accordance with its **intended purpose.**[209] According to Article 5(2) of the MDR, “a medical device shall meet the general safety and performance requirements set out in **Annex I** taking into account the intended purpose’’.

MDR Annex I sets out 23 general safety and performance requirements that medical devices must comply with, taking into account the intended purpose.[210] Broadly speaking, these requirements refer to general medical device requirements, design and manufacturing requirements and requirements regarding the information supplied with the device.

According to Annex I, some of the general obligations that need to be fulfilled by the manufacturer include:

- Devices shall achieve the performance intended by their manufacturer;
- Devices shall be designed and manufactured in such a way that they are suitable for their intended purpose;
- Device shall be safe and effective, and associated risks shall be acceptable when weighed against the benefits of the patients and level of protection of health and safety while taking into account the state of the art;
- The risk management system shall be established, implemented, documented, and maintained;
- Risks must be reduced as much as possible, but not so much that they negatively affect the risk-benefit ratio;
- Device manufacturers must implement and maintain a thorough, well-documented, and evaluative risk management system that continues to be updated throughout the life cycle of a device;
- Device designed to be used with other devices/equipment as a whole (including the connection system between them) has to be safe and should not impair the specified performance of the device;
- Devices shall be designed and manufactured in a way to remove, as far as possible, risks associated with possible negative interaction between software and the IT environment within which they operate;
- Device incorporating electronic programmable systems, including software or standalone software as a medical device, “shall be designed to ensure repeatability, reliability, and performance according to the intended use;
- Devices should be developed and manufactured according to the state of the art and by respecting the principles of the development lifecycle, risk management, verification, and validation;
- For devices that incorporate software or for software that are devices in themselves, the software shall be developed and manufactured in accordance with the state of the art taking into account the principles of development life cycle, risk management, including information security, verification and validation;
- Manufacturers shall set out minimum requirements concerning hardware, IT network characteristics, and IT security measures, including protection against unauthorised access;

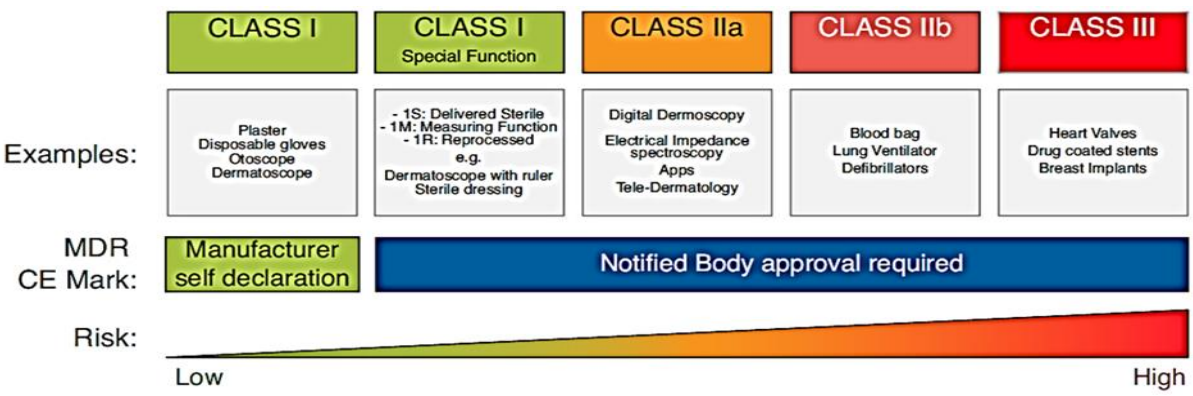
Device shall be accompanied by the information needed to identify the device and its manufacturer, and by any safety and performance information relevant to the user, or any other person, as appropriate. Such information may appear on the device itself, on the packaging or in the instructions for use, and shall, if the manufacturer has a website, be made available and kept up to date on the website.

Apart from Annex I, the MDR has significant effects on **clinical data** and evaluation requirements, reclassification of some device types and post-market requirements. The classification of medical devices in use by the EU medical device legislation is a risk-based system taking into account the vulnerability of the human body and the potential risks associated with the devices. According to Article 51 (1) MDR, based on the intended purpose and their inherent risks, medical devices shall be divided into the following classes:

- Class I—low-risk medical devices;
- Class IIa—medium risk;
- Class IIb—medium/high risk;
- Class III—high risk.

Each of these risk classes requires a different conformity assessment route, which will determine the steps that manufacturers are required to take for CE marking. Devices classified as Class I are subject to minimal regulatory control and are not designed to provide significant support or aid in preserving human life or preventing health impairment. On the other hand, Class III devices are deemed high-risk and typically serve to sustain human life. Medical Device Coordination Group (MDCG) provides detailed Guidance criteria that can be used in order to determine medical device classification.[211] Figure 2. provides an illustration of medical devices' classes, examples, requirements and risks.

Figure 2 Medical Devices Classes



Source: Malvehy, J., Ginsberg, R., Sampietro-Colom, L., Ficapal, J., Combalia, M. and Svedenhag, P. (2022), New regulation of medical devices in the EU: impact in dermatology. J Eur Acad Dermatol Venereol, 36: 360-364. https://doi.org/10.1111/jdv.17830

To achieve CE marking for a product under MDR, manufacturers must meet stringent conditions such as a quality management system, extensive technical documentation

of the development and manufacturing of a product, risk management for the product in clinical use, clinical evaluation that shows the safety and performance of the product and that the benefits of using the device outweigh any risks.

It is worth noting that one key aspect in meeting MDR objectives is the creation of a European database on medical devices (EUDAMED) that should integrate different electronic systems to collate and process information regarding devices on the market and the relevant economic operators, certain aspects of conformity assessment, notified bodies, certificates, clinical investigations, vigilance and market surveillance. The objectives of the database are to enhance overall transparency, including through better access to information for the public and healthcare professionals, to avoid multiple reporting requirements, to enhance coordination between Member States and to streamline and facilitate the flow of information between economic operators, notified bodies or sponsors and the Member States as well as between Member States among themselves and with the Commission.[212]

In particular, EUDAMED is organised into the following three electronic systems:

- On clinical investigations;
- On vigilance;

  and
- On market surveillance.

It is also important to mention that, pursuant to MDR Article 87(1), manufacturers of medical devices are obliged to report, to the relevant competent authorities, **any serious incident** involving devices made available on the Union market, except expected side-effects which are clearly documented in the product information and quantified in the technical documentation and are subject to trend reporting in accordance to MDR. A serious incident is defined as any incident that directly or indirectly led, might have led or might lead to any of the following:

- the death of a patient, user or other person;
- the temporary or permanent serious deterioration of a patient's, user's or other person's state of health;
- a serious public health threat. [213]

The period for the reporting will depend on the severity of the incident. For instance, manufacturers shall report any serious incident **immediately** after they have established the causal relationship between that incident and their device or that such causal relationship is reasonably possible and **not later than 15 days** after they become aware of the incident. However, in the event of a serious public health threat[214] the report must be provided immediately, and not later than 2 days after the manufacturer becomes aware of that threat.

If CYLCOMED technical solution falls under the scope of the MDR, manufacturers are obliged to meet various legal and ethical requirements throughout the entire lifecycle of a device prior to the market release of a medical device.

3.6 In vitro diagnostic medical devices (IVDR)

Regulation (EU) 2017/746 on in vitro diagnostic medical devices (IVDR) was adopted on April 5, 2017, and entered into force on May 26, 2017, repealing the EU Directive 98/79/EC on in vitro diagnostic medical devices, which had been in force since 1998.[215]

As same as MDR, IVDR regulation is a valid and binding legislative act that all EU Member States must apply in its entirety. Hence, in contrast to the now superseded EU Directive, it does not first have to be transposed into national law.

As same as the MDR, IVDR aims to increase patient safety by improving the quality, safety and performance of medical devices. According to IVDR Recital 2, the Regulation aims to ensure the smooth functioning of the internal market as regards in vitro diagnostic medical devices, taking as a base a high level of protection of health for patients and users, and taking into account the small and medium-sized enterprises that are active in this sector. At the same time, this Regulation sets high standards of quality and safety for in vitro diagnostic medical devices in order to meet common safety concerns as regards such products. IVDR lays down rules concerning the placing on the market, making it available on the market or putting into service of in vitro diagnostic medical devices for human use and accessories for such devices in the Union.[216]

IVDR Article 2(2) defines “in vitro diagnostic medical device” as any medical device which is a reagent, reagent product, calibrator, control material, kit, instrument, apparatus, piece of equipment, software or system, whether used alone or in combination, intended by the manufacturer to be used in vitro for the examination of specimens, including blood and tissue donations, derived from the human body, solely or principally for the purpose of providing information on one or more of the following:

- Concerning a physiological or pathological process or state;
- Concerning congenital physical or mental impairments;
- Concerning the predisposition to a medical condition or a disease;
- To determine the safety and compatibility with potential recipients;
- To predict treatment response or reactions;
- To define or monitor therapeutic measures. Specimen receptacles shall also be deemed to be in vitro diagnostic medical devices.

Broadly speaking, IVDR follows the same logic as the MDR. For instance, manufacturers that are seeking market access throughout the EU must comply with Annex I - General Safety and Performance Requirements in terms of meeting these requirements. IVDR Annex I follows the same structure as the MDR.

General Safety and Performance Requirements are divided into three (3) chapters in Annex I, as follows:

- General requirements;

- Requirements regarding design and manufacture;

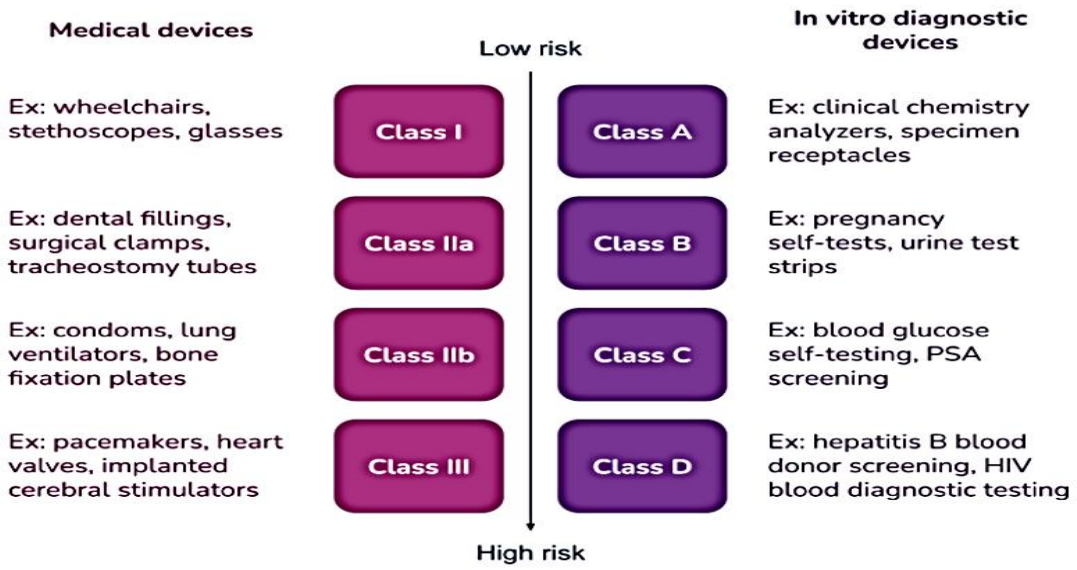
  and

- Requirements regarding the information supplied with the device.

As same as MDR, IVDR outline General Safety and Performance Requirements in great detail for medical device designers and manufacturers, while the general requirements for each are almost identical.

Likewise, IVDR Article 47(1) divides devices into classes subject to the intended purpose and their inherent risks. The similarity is shown in the following figure.

Figure 3 General Safety and Performance Requirements



Source: The ultimate guide to the EU MDR and IVDR general safety and performance requirements (GSPR); available at https://www.rimsys.io/blog/the-ultimate-guide-eu-mdr-gspr

As can be seen, IVDR and MDR follow the same logic in order to increase patient safety by improving the quality, safety and performance of medical and in vitro diagnostic devices. Therefore, in order to avoid duplication in this deliverable, all content elaborated in the section relevant for the MDR section applies to this section.

3.7 Guidance on Cybersecurity for medical devices (MDCG)

The Medical Device Coordination Group of the European Commission endorsed Guidance on Cybersecurity for Medical Devices (MDCG Guidance) in December 2019, which focuses on cybersecurity for medical devices and addresses the relevant provisions in the MDR and IVDR.[217]

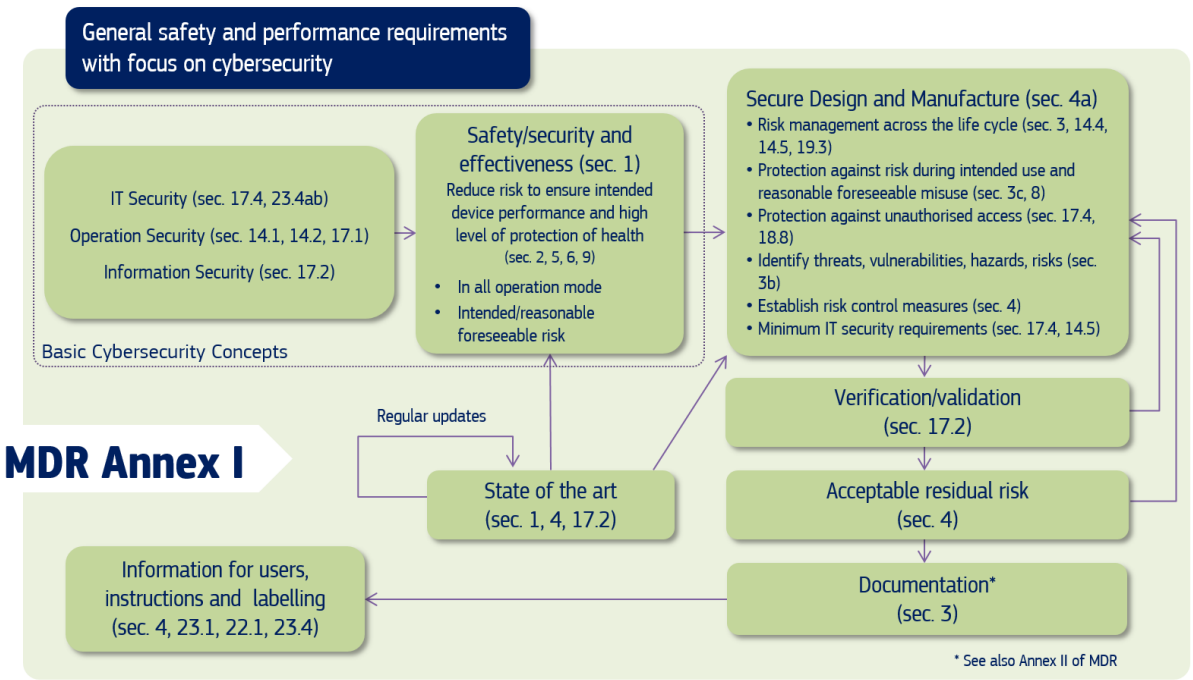
As the MDCG guidance, at the beginning of the document, sets out that “any views expressed in this document are not legally binding”, it is important to note that MDCG

Guidance is not a legally binding document.[218] At the same time, it is the first and most relevant source of information related to cybersecurity.

The main goal of MDCG Guidance is to provide device manufacturers with guidance on how to meet all the relevant essential requirements of Annex I to the MDR and IVDR with regard to cybersecurity.

Figure below provides a visual summary of these requirements, which deal with both pre-market and post-market aspects.

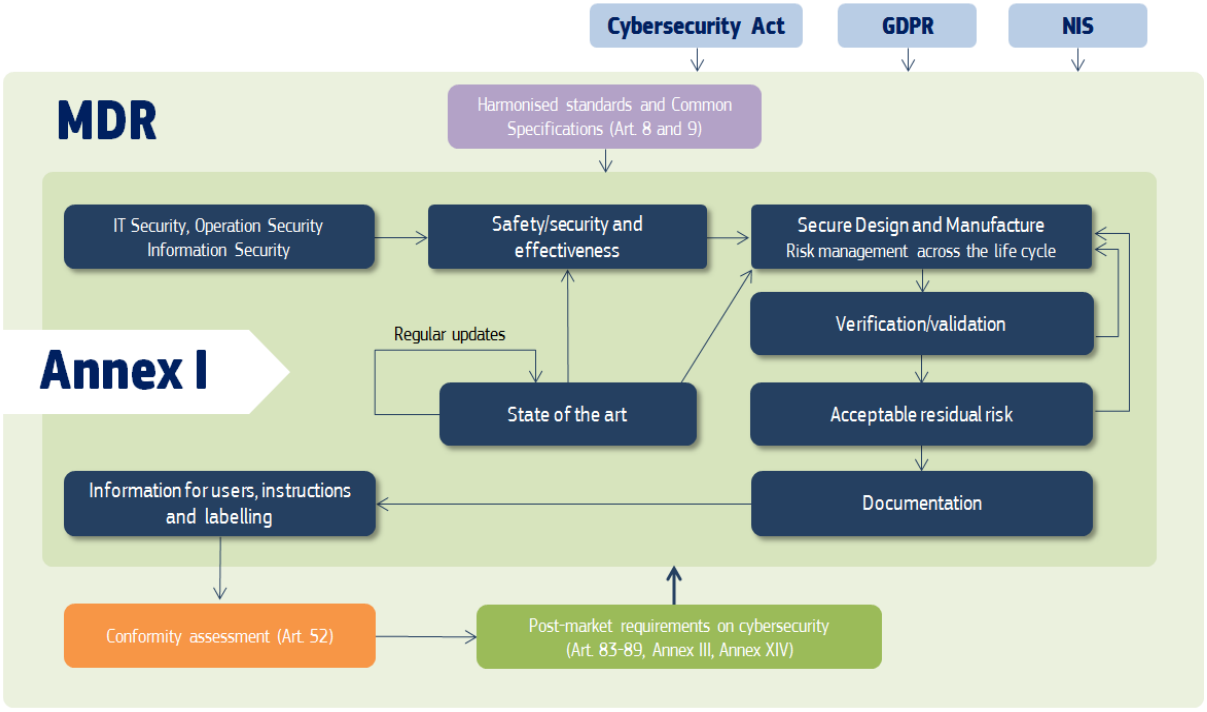
Figure 4 Cybersecurity Requirements Contained in MDR Annex I



Source: MDCG Guidance, p5.

Although outdated to some extent in light of the recent EU legislative activities, the following figure depicts the requirements covering cybersecurity that the manufacturers should be particularly aware of, as well as its relation with other legal frameworks.

Figure 5 Cybersecurity Requirements in the MDR



Source: MDCG Guidance, p6.

Although the MDCG guidance covers a broad range of topics applicable to all stakeholders in the medical device supply chains, and to end-users, it is worth noting that MDCG guidance states that all stakeholders, such as manufacturers, suppliers, healthcare providers, patients, integrators, operators and regulators share responsibilities for ensuring a secure environment for the benefit of patients' safety.

The MDCG is currently the most relevant guidance providing precise cybersecurity requirements for the medical devices that manufacturers need to fulfil prior to placing them on market, and fully apply to CYLCOMED.

3.8 Radio Equipment Directive (RED)

The Radio Equipment Directive (RED) entered into force in June 2014 and is applicable as of June 2016.[219] The RED establishes a regulatory framework for placing radio equipment on the Single Market,[220] and under its scope falls electrical and electronic equipment that can use the radio spectrum for communication and/or radio determination purposes.

The RED defines "radio equipment" as "an electrical or electronic product, which intentionally emits and/or receives radio waves for the purpose of radio communication and/or radiodetermination, or an electrical or electronic product which must be completed with an accessory, such as antenna, so as to intentionally emit and/or receive radio waves for the purpose of radio communication and/or radiodetermination".[221] Hence, all internet-connected radio equipment, including Internet of Things (IoT) with a radio (wireless) function and wearables (i.e., smart

watches) fall under the Directive's scope. A wide range of electronic products that are Wi-Fi, Bluetooth, LTE, 5G, or GPS enabled are under the RED scope. Additionally, **medical devices such as pacemakers or implantable cardioverter defibrillators** are likely to fall under the scope of the Directive and thus be subject to its security requirements.[222]

Pursuant to the RED Article 1(2), the Directive is not applicable to:

- **radio equipment used by radio amateurs** within the meaning of Article 1, definition 56, of the International Telecommunications Union (ITU) Radio Regulations, unless the equipment is made available on the market;
- **marine equipment** falling within the scope of Council Directive 96/98/EC;[223]
- **airborne products**, parts and appliances falling within the scope of Article 3 of Regulation (EC) No 216/2008;[224]
- **custom-built evaluation kits** destined for professionals to be used solely at research and development facilities for such purposes.

The RED excludes from its scope radio kits for assembly and use by radio amateurs, radio equipment modified by and for the use of radio amateurs and equipment constructed by individual radio amateurs for experimental and scientific purposes related to amateur radio, as they are not regarded as being made available on the market. Additionally, it is not applicable to radio equipment exclusively used for activities concerning public security, defence, State security, including the economic well-being of the State in the case of activities pertaining to State security matters, and the activities of the State in the area of criminal law.[225]

To achieve compliance under the RED, radio equipment must be constructed to meet essential requirements in terms of health and safety, electromagnetic compatibility, efficient use of the radio spectrum and avoiding harmful interference[226].

It is important to note that RED does not explicitly refer to cybersecurity, although some of the essential requirements set out in Article 3(3) aim to ensure that radio equipment placed on the EU market is fit for the new technological challenges linked to cybersecurity risks. Pursuant to the RED Article 3(3), radio equipment within certain categories or classes shall be so constructed that it complies with the following essential requirements:

"(a) radio equipment interworks with accessories, in particular with common chargers;

(b) radio equipment interworks via networks with other radio equipment;

(c) radio equipment can be connected to interfaces of the appropriate type throughout the Union;

(d) radio equipment does not harm the network or its functioning nor misuse network resources, thereby causing an unacceptable degradation of service;

(e) ***radio equipment incorporates safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected;***

(f) radio equipment supports certain features ensuring protection from fraud;

(g) radio equipment supports certain features ensuring access to emergency services;

(h) radio equipment supports certain features in order to facilitate its use by users with a disability;

(i) radio equipment supports certain features in order to ensure that software can only be loaded into the radio equipment where the compliance of the combination of the radio equipment and software has been demonstrated."

However, the Commission Impact assessment report with regard to the application of the essential requirements referred to in Article 3(3),[227] points (d), (e) and (f), of RED highlighted that certain radio equipment lacks basic cybersecurity requirements related to, inter alia, protecting privacy or minimising the risks of fraud or preventing harms to the networks. For instance, GDPR sets out rules on data protection and privacy protection. However, it is important to note that **GDPR is specifically aimed at those who control and process personal data, rather than device manufacturers themselves.**[228]

To address above mentioned issues, Commission adopted delegated act to the RED which lays down new legal requirements for cybersecurity safeguards, which manufacturers will have to take into account in the design and production of the radio equipment.[229] For instance, a delegated act pursuant to Article 3(3)(e) of the RED requires that **internet-connected radio equipment[230]**, which is placed on the Union market, incorporate safeguards to ensure that personal data and privacy are protected when they are capable of processing personal data as defined in GDPR Article 4(1).[231]

Although medical devices might fall under the scope of the RED, it is important to note that MDCG Guidance does not even refer to the RED. However, to facilitate compliance with the RED, the European Commission developed the Guide to the Radio Equipment Directive (RED Guide),[232] which states that "when RED is applicable simultaneously with any other EU legislation covering the same hazard (safety or EMC), the issue of overlap might be resolved by giving preference to the more specific EU legislation".[233]

4 Legal and Ethical frameworks governing artificial intelligence

The CYLCOMED project will include the development and use of artificial intelligence (AI)-based systems or techniques. Pilot 1 "Cybersecurity in Hospital Equipment for COVID-19 ICU patients" will be carried out as a digital twins simulation without the involvement of any human participants. No personal data processing by these AI-based tools is envisaged, and there is no potential risk or ethical concern identified regarding the development and use of these tools. However, due to its relevance with

CYLCOMED design, it is of significant importance to briefly elaborate on legal and ethical frameworks governing artificial intelligence.

This section will provide an outline of the relevant legal and ethical frameworks relevant to the CYLCOMED project, focusing on governance at the European Union level. However, since the AI Act proposal is still subject to legal scrutiny according to the EU legislative procedure, and therefore possible adjustments, this deliverable aims to capture the essence of the proposed act, while the next deliverable will analyse the AI Act in more detail.

4.1 Artificial Intelligence Act (AI Act) proposal

In April 2021, the European Commission published the first ever proposal for a regulation on artificial intelligence (AI Act Proposal).[234] The primary goal of the AI Act is to ensure the proper functioning of the single market by creating the conditions for the development and use of trustworthy artificial intelligence in the Union[235]. As provided by the Explanatory Memorandum, the Regulation has the following specific objectives:

- ensure that AI systems placed on the Union market and used are safe and respect existing law on fundamental rights and Union values;
- ensure legal certainty to facilitate investment and innovation in AI;
- enhance governance and effective enforcement of existing law on fundamental rights and safety requirements applicable to AI systems;
- facilitate the development of a single market for lawful, safe and trustworthy AI applications and prevent market fragmentation.[236]

In order to achieve these objectives, the AI Act lays down harmonised rules for the development, placement on the market and use of AI systems in the Union following a proportionate risk-based approach[237]. Pursuant to the AI Act Article 3(1) **artificial intelligence system (AI system)** is defined as "*software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with*".

Annex I of the proposal provides a list of AI techniques and approaches to develop AI, such as "machine learning", "logic knowledge based" systems and "statistical" approaches.

Regarding its **material scope**, AI Act Article 2 sets out that Regulation applies to two categories of subjects:

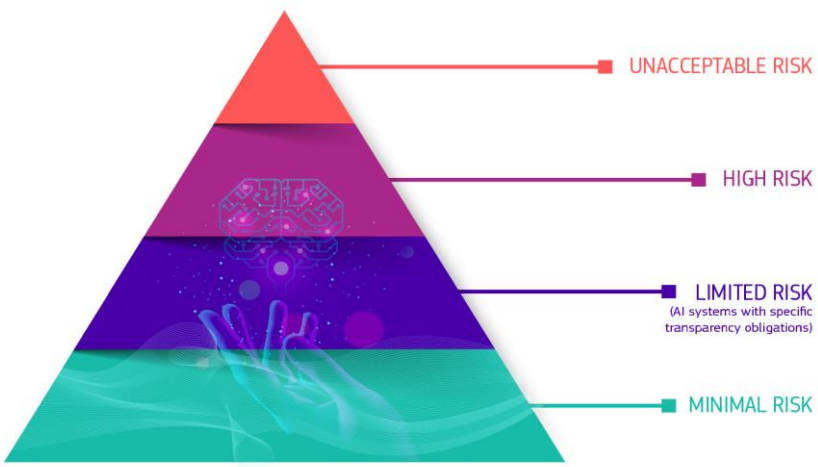
- **"provider"**- which is defined as "any natural or legal persons, public authorities, agencies or bodies that develop or own AI systems to place them on the market or put them into service, whether against payment or for free"[238] and

- **“users”**- which is defined as “any natural or legal persons, public authorities, agencies or bodies that use AI systems under their authorities, unless they are carrying out a non-professional activity”.[239]

In terms of its **territorial scope**, AI Act applies to providers of AI systems established within the EU or in a third country placing AI systems on the EU market or putting them into service in the EU, as well as to users of AI systems located in the EU.[240] The proposed AI Act excludes from its scope AI systems developed or used exclusively for military purposes.[241] Additionally, the proposed Regulation shall not apply to public authorities of a third country and international organisations when acting in the framework of international agreements concluded at national or European level for law enforcement and judicial cooperation with the Union or with its Member States.[242]

The AI Act proposal contains a different set of requirements tailored on a risk-based approach for the development, placing on the market and use of AI systems in the EU. More specifically, the AI Act distinguishes between four categories of risks that AI systems might pose, as illustrated in the figure below:

Figure 6 Risk Levels Specified Under the AI Act Proposal



Source: European Commission, ‘Regulatory Framework Proposal on Artificial Intelligence’ (Shaping Europe’s Digital Future). Available at https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

Depending on the category of risk identified, the stakeholder’s obligations will significantly vary, from complete prohibition in case of unacceptable risk, to permission with no restrictions in case of minimal risk. For instance, AI Act Article 5 explicitly prohibits harmful AI practices that bear “unacceptable risks”. Thereof, it is banned to place on the market, put into services or use in the EU:

- AI systems that deploy harmful manipulative “subliminal techniques”;
- AI systems that exploit specific vulnerable groups (physical or mental disability);

- AI systems used by public authorities, or on their behalf, for social scoring purposes;
- “Real-time” remote biometric identification systems in publicly accessible spaces for law enforcement purposes, except in a limited number of cases (e.g. targeted search for specific potential victims of crime).

Likewise, in accordance with AI Act Article 6, an AI system is considered to be a High-Risk AI system if two cumulative conditions are met:

- the AI system is intended to be used as a safety component of a product, or is itself a product, covered by the Union harmonisation legislation listed in Annex II;
- the product whose safety component is the AI system, or the AI system itself as a product, is required to undergo a third-party conformity assessment with a view to the placing on the market or putting into service of that product pursuant to the Union harmonisation legislation listed in Annex II.

Annex II entails a wide range of products or safety components that are covered by EU legislation, such as toys, medical devices, and radio equipment. In addition to the above high-risk AI systems, eight specific areas listed in Annex III shall also be considered high-risk, such as biometric identification and identification of natural persons, management and operation of critical infrastructures, AI for recruitment purposes, law enforcement, or education and vocational training. If recognised as a high-risk AI system, it will be subject to stringent legal requirements throughout the entire AI lifecycle, from its design to its implementation. The most important obligations refer to risk management, testing, technical robustness, data training and data governance, transparency, human oversight, and cybersecurity.[243] For instance, providers are obliged to establish, implement, document and maintain a risk management system, which shall include the following steps:

- Identification and analysis of the known and foreseeable risks;
- Estimation and evaluation of the risks that may emerge from both normal use and foreseeable misuse;
- Evaluation of other possible risks, on the basis of information collected after the placing on the market; and
- Adoption of suitable risk management measures, taking into account the state of the art.[244]

It is important to note that the use of AI in healthcare per-se is not proposed to be high-risk. However, all certified medical devices that utilise AI would be classified as high-risk AI systems.[245]

Providers that are putting into service or using AI systems in the EU that are not recognised as high-risk AI systems are subject to less stringent conditions. In a scenario where AI systems pose “limited risk”, such as systems that interact with humans (i.e. chatbots), providers are required to comply with transparency obligations.[246] On the other hand, if the AI system is recognised as an AI system with

minimal risk AI Act does not impose any legal obligations for providers and users of such systems. However, they are encouraged to develop codes of conduct to ensure that their AI systems are trustworthy and voluntarily apply the mandatory requirements for high-risk AI systems.[247]

It is important to note that infringement of legal obligations may lead to severe administrative fines, up to 30M EUR or 6% of global annual turnover.[248]

4.2 Ethics Guidelines for Trustworthy AI

In its Communication of 25 April 2018 and 7 December 2018, the European Commission set out its vision for artificial intelligence (AI), which supports "ethical, secure and cutting-edge AI made in Europe".[249]
One of the main pillars that underpin the Commission's vision is ensuring an appropriate ethical and legal framework to strengthen European values. To support the implementation of this vision, on the 1st of June 2018, European Commission appointed a High-Level Expert Group on Artificial Intelligence (AI HELG) mandated to present two deliverables to guide the ethical development and use of AI based on EU fundamental rights. The HLEG AI presented the "Ethics Guidelines for Trustworthy AI" in April 2019, as practical guidance on how developers, implementers and end-users of AI systems can comply with ethical principles. [250]

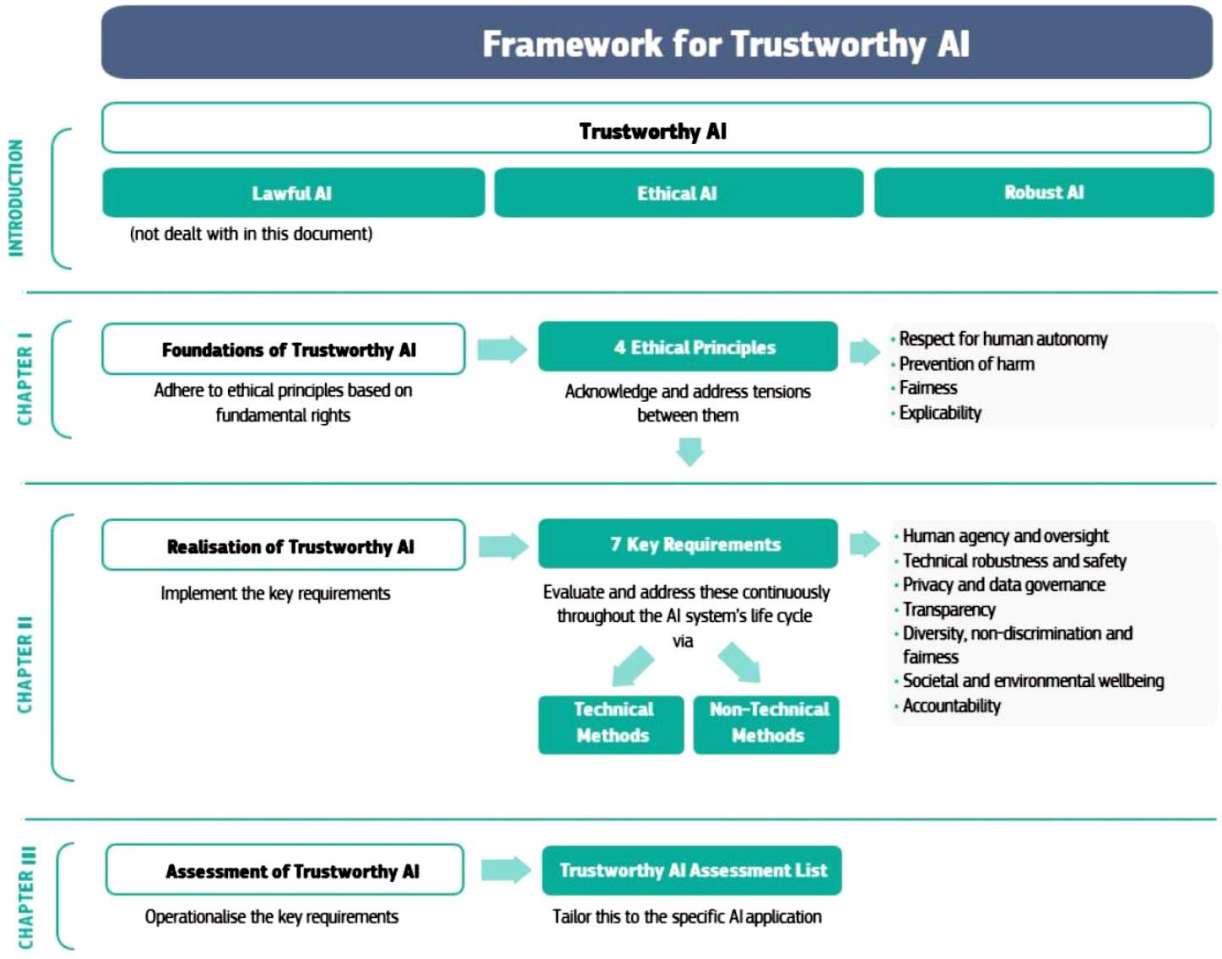
The introductory part of the Guidelines points out that AI should not be seen as an end to itself, but as a means to "increase human flourishing, thereby enhancing individual and societal well-being and the common good, as well as bringing progress and innovation".[251] Additionally, the Guidelines acknowledge that AI systems must adhere to the ethical principles of respect for human autonomy, prevention of harm, fairness and explicability, whereas particular attention should be given to contexts involving vulnerable groups, including children, persons with disabilities and others that have been disadvantaged or at risk of exclusion. The Guidelines revolve around trustworthiness as its main idea and foundational ambition. Trustworthiness is defined as "a prerequisite for people and societies to develop, deploy and use AI systems".[252]
The trustworthiness of an AI system is based on the three main building blocks, which should be met throughout the system's entire life cycle:

- *it should be **lawful**, complying with all applicable laws and regulations*; This pillar refers to compliance with legally binding rules governing the development and use of AI on international, European and national level. According to the Guidelines, these legal sources include, but are not limited to, *EU primary law* (e.g. Charter of Fundamental Rights), *EU secondary law* (e.g. General Data Protection Regulation), the *UN Human Rights treaties and the Council of Europe conventions* (e.g. the European Convention on Human Rights), and *Member State* laws. Additionally, sector-specific rules that apply to particular AI applications should be taken into account (e.g. Medical Device Regulation).

- *it should be **ethical**, ensuring adherence to ethical principles and values*; It is important for AI systems to adhere to ethical standards in order to be considered trustworthy. This is particularly important in scenarios where positive law might encounter difficulties adapting to technological advancements. One example of this can be observed in AI systems where ethics play a crucial role in bridging the gap.
- it should be **robust**, both from a technical and social perspective, since, even with good intentions, AI systems can cause unintentional harm. AI systems are expected to be both technically and socially robust. The Guidelines accentuate that AI should perform in a safe, secure and reliable manner, and safeguards preventing any unintended adverse impacts of AI applications should be put in place.

The schematic overview of the AI HLEG Framework for Trustworthy AI is illustrated in the figure below.

Figure 7 AI HLEG Framework for Thrustworthy AI



Source: Ethics Guidelines for Trustworthy AI p.10

Additionally, the Guidelines set out that fundamental rights enshrined in the EU Treaties, the EU Charter and international human rights law constitute the foundations of Trustworthy AI. According to the Guidelines, the following families of fundamental rights are particularly apt to cover AI systems:

- **Respect for human dignity;** It is crucial that AI systems are developed with the utmost consideration for human well-being, including their physical and mental health, personal and cultural identity, and fulfilment of essential needs.
- **Freedom of the individual;** In an AI context, it is important to ensure that the individual's freedom is not compromised through illegitimate coercion, threats to mental autonomy and health, unjustified surveillance, deception, or unfair manipulation.
- **Respect for democracy, justice and the rule of law;** It is important that AI systems promote and uphold democratic processes, while also showing respect for the diverse range of values and life choices held by individuals. Additionally, it is essential that AI systems do not pose a threat to democratic processes, human deliberation, or democratic voting systems.
- **Equality, non-discrimination and solidarity** - including the rights of persons at risk of exclusion; AI systems should not generate unfairly biased outputs.
- **Citizens' rights**; AI systems should not negatively impact citizens' rights, such as the right to petition the administration.[253]

Furthermore, to ensure the trustworthy development, deployment, and use of AI systems, Guidelines outline four **ethical principles** based on fundamental rights.

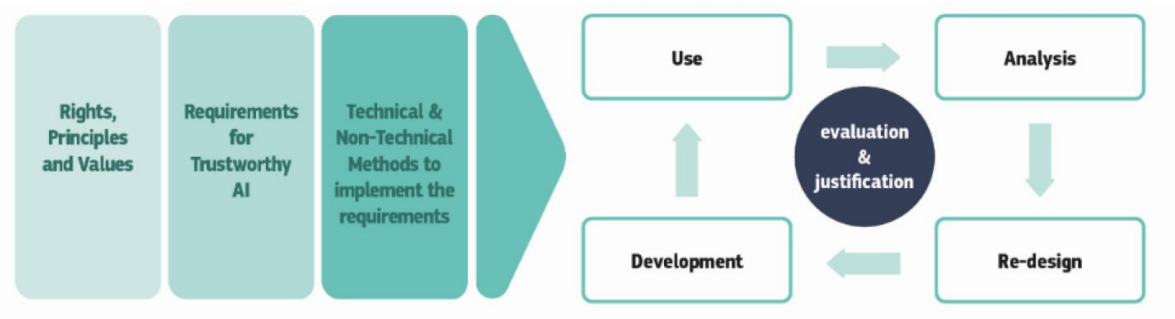
- **Respect for human autonomy;** The principle of respect for human autonomy means that AI systems must not be developed in a manner that can unjustifiably subordinate, coerce, deceive, or manipulate humans. The human-centric design principle must be implemented which will allow effective self-determination.
- **Prevention of harm;** The principle of prevention of harm requires that AI systems are secure and safe. Its design must be technically robust and secured from malicious use that might have an adverse effect on humans.
- **Fairness;** The principle of fairness requires that the development, deployment and use of AI systems must be fair and that AI systems should generate unfairly biased outputs.
- **Explicability;** The principle of explicability is marked as essential in building and maintaining trust in AI systems. It is imperative that transparency is maintained in processes, and that the capabilities and objectives of AI systems are clearly communicated. Whenever possible, decisions should be explained to those who are directly or indirectly impacted.[254]

Building upon these principles, The Guidelines propose a non-exhaustive list of requirements that need to be fulfilled in order to implement Trustworthy AI. These concrete requirements entail systemic, individual and societal aspects:

- **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.[255]

In addition, Chapter II covers technical and non-technical methods worth considering to ensure Trustworthy AI that can be incorporated in the design, development and use phases of an AI system. The implementation and realisation of Trustworthy AI is a continuous process, as illustrated in Figure 8.

Figure 8 Trustworthy AI Life Cycle



Source: Ethics Guidelines for Trustworthy AI p.20.

Examples of technical methods are the architecture for Trustworthy AI, Ethics and rule of law by design (X-by-design), explanation methods (XAI), testing and validation, and quality service indicators. On the other hand, non-technical methods include, inter alia, standardisation, codes of conduct and certification. Chapter III provides a non-exhaustive Trustworthy AI assessment list intended to operationalise the key requirements set out in Chapter II and to help assess whether the AI systems that is being developed, deployed, and used, adheres to the seven requirements of Trustworthy AI.

Following the publication of the Ethics Guidelines for Trustworthy AI, in 2020, AI HLEG published the Assessment List for Trustworthy Artificial Intelligence (ALTAI).[256]

ALTAI builds upon the Ethics Guidelines and provides a practical self-assessment tool that translates the Ethics Guidelines into a checklist, intended for flexible use, meaning that organisations can draw on elements relevant to the particular AI system or add elements to it as they see fit, taking into consideration the sector they operate in. Furthermore, to demonstrate the capability of such an assessment, AI HLEG developed a prototype web-based tool, to practically guide developers and deployers of AI through an accessible and dynamic checklist.[257]

Eventually, it is noteworthy that European Commission developed a guidance note on Ethics By Design and Ethics of Use Approaches for Artificial Intelligence, which provides guidance for adopting an ethically-focused approach while designing, developing, and deploying and/or using AI-based solutions. It explains the ethical principles which AI systems must support and discusses the key characteristics that an AI-based system/application must have in order to preserve and promote ethical principles.

Despite the fact that there is currently no legally enforceable framework that regulates AI, it would be wrong to conclude that there is a legal vacuum for AI. The Ethics Guidelines explicitly recognise the critical importance of lawfulness. It is based on the fundamental rights approach placing the protection of human rights guaranteed by the EU Treaties and the EU Charter at its core. The Ethics Guidelines Recital 12 explicitly points out that “fundamental rights lie at the foundation of both international and EU human rights law and underpin the legally enforceable rights guaranteed by the EU Treaties and the EU Charter. Being legally binding, compliance with fundamental rights hence falls under trustworthy AI's first component (lawful AI).” Hence, although not legally binding, being rooted in legally enforceable rights, Guidelines provide the benchmark for all AI developers, which makes this soft law instrument fully applicable to the CYLCOMED project. This is also supported by the fact that, at this moment, Ethics Guidelines constitute the only regulatory instrument specific for AI in the EU.

5 Clinical Trials

The advancement of medical science largely depends on investigations in humans intended to discover or verify the effects of one or more investigational medicinal products. Clinical trials aim to attain generalised knowledge that can be used to advance healthcare. However, involving human subjects in clinical research, although critical for the welfare of future patients, may not directly benefit the involved patient. In situations where patients may not directly benefit from the research, they are faced with the risk of being exploited or harmed. Therefore, every clinical study must be conducted with the utmost respect for ethical standards. Since Pilot 2 “Cybersecurity for Telemedicine Platforms”, will be conducted as an observational study by processing personal data of patients, including pediatric patients, it is essential to provide initial legal and ethical considerations that are relevant for the CYLCOMED design.

5.1 Declaration of Helsinki

The World Medical Association (WMA) has developed the Declaration of Helsinki as a statement of ethical principles for medical research involving human subjects, including research on identifiable human material and data.[258] Declaration of Helsinki provides guidelines for medical research on human beings. It aims to promote the ethical conduct of research and to protect human subjects from associated risks. The Declaration of Helsinki highlighted two aspects of ethical considerations: that all of the participants have the right to be informed about the study, by giving informed consent, and that an ethics committee approval should have got to ensure the appropriateness of design before initiating a research.[259] The Declaration of Helsinki was the first set of international research guidelines that required research participants to provide informed consent.

The Declaration defines that it is generally the duty of the physician to promote and safeguard the health, well-being and rights of all patients, including those who are involved in medical research. Physicians who are performing medical research have the duty to protect the life, health, dignity, integrity, right to self-determination, privacy, and confidentiality of personal information of research subjects. While the primary purpose of medical research is to generate new knowledge for the benefit of patients, this goal can never take precedence over the rights and interests of individual research subjects.

In medical research involving human subjects capable of giving informed consent, each potential subject must be adequately informed of the aims, methods, the anticipated benefits and potential risks of the study and the discomfort it may entail, post-study provisions, sources of funding, any possible conflicts of interest, institutional affiliations of the researcher, and any other relevant aspects of the study. The potential subject must be informed of the right to refuse to participate in the study and the right to withdraw consent at any time during the study, without reprisal. Special attention should be given to the specific information needs of individual potential subjects as well as to the methods used to deliver the information. Particular attention must be given to the information and consent process of vulnerable patients. It is important to note that the Helsinki Declaration principles concern all types of medical research.[260]

5.2 Declaration of Taipei

The World Medical Association adopted the Declaration of Taipei on Ethical Considerations regarding Health Databases and Biobanks in 2002.[261] This Declaration provides guidance for the protection of research subjects who allow their health data and/or body tissues to be used for future research or other uses. The Declaration of Taipei aims to strike a balance between the rights of individuals and the public interest of research, based on confidentiality and privacy rules. It is noteworthy

that in comparison to the Declaration of Helsinki, it has broadened the scope of application to all public and private entities that use a biobank or health database, including for non-research purposes, non-health-related purposes and commercial purposes.

The Declaration entails rules that address the individuals' rights as donors of samples and data, as well as rules that relate to the governance of health databases and biobanks. The Declaration points out that data and biological material should only be collected, stored or used when the individuals concerned have given their informed consent and the consent is voluntarily given, collected from individuals capable of giving consent, specific, freely given and informed. Additionally, the Declaration sets out several extra informational requirements whenever data or biological material is collected and stored for multiple and indefinite uses. The Declaration of Taipei adopts as a general principle that research should contribute to the benefit of society, in particular public health objectives. Moreover, the Declaration accentuate the role of the independent ethics committees within its scope of application, pointing out that, for instance, an independent ethics committee must approve the establishment of Health Databases and Biobanks used for research and other purposes.[262]

Although not a legally binding document, as same as the Declaration of Helsinki, it provides ethical principles for physicians and other participants in medical research gathering health information, record health-related events and samples collection.

5.3 Clinical Trials Directive (CTD)

The Clinical Trials Directive aims to standardise the conduction of interventional clinical trials in the EU and ensure equality in safeguarding public health.[263] According to CTD Article 1(2), "good clinical practice is a set of internationally recognised ethical and scientific quality requirements which must be observed for designing, conducting, recording and reporting clinical trials that involve the participation of human subjects. Compliance with this good practice provides assurance that the rights, safety and well-being of trial subjects are protected and that the results of the clinical trials are credible".

Besides, CTD sets out rules on, inter alia, the responsibility of the sponsor for the clinical trial, the requirement of clinical trial authorisation, the role of ethical committees, data collection, investigative materials, quality control, ethical guidelines, and the safety of subjects. It applies to all academic and commercial interventional clinical trials with an investigational medicinal product EU. It is important to note that, although CTD has enabled the harmonisation of trial conditions, the fact that the principles of the CTD had to be implemented in national laws led to partly substantial differences in trial approval and safety reporting conditions.

Although CTD has been repealed by the Clinical Trials Regulation[264] In January 2022, it will still apply until 30 January 2025 to:

- All Clinical trials applications submitted before 31 January 2022;

- Clinical trials applications submitted between 31 January 2022 and 30 January 2023 if the sponsor opted for the legal regime of the Directive[265].

5.4 Clinical Trials Regulation (CTR)

Clinical Trials Regulation aims at achieving an internal market as regards clinical trials and medicinal products for human use, taking as a base a high level of protection of health. At the same time, this Regulation sets high standards of quality and safety for medicinal products in order to meet common safety concerns as regards these products.[266] Although the Regulation entered into force on 16 June 2014, its application depended on the development of a fully functional EU clinical trials portal and database. European Medicines Agency (EMA) Management Board confirmed to the European Commission on 21 April 2021 that the EU Portal and Database were fully functional. The publication of the subsequent Commission notice on 31 July 2021 fixed the date of applicability of the Clinical Trials Regulation on 31 January 2022.[267]

CRT lays out the rules for the coordinated clinical trial assessment and national approval procedure, the structure of the application dossier, the IT infrastructure of the underlying EU database Clinical Trial Information System (CTIS), the ongoing and final reporting obligations of the sponsor on the trial process and safety data, the manufacturing and handling requirements of investigational medicinal products (IMP), the quality management system including the document management and archiving requirements.

It is noteworthy that CTR simplifies the procedures for the submission of an application dossier for the authorisation of a clinical trial. In contrast to CTD, the multiple submissions of largely identical information will be avoided and replaced by the submission of one application dossier to all the Member States concerned, through a single submission portal. Furthermore, one of the key advantages of the CRT is a unified IT portal and a clinical trial information system. The web-based platform facilitates trial applications to the European Medicines Agency (EMA), communication between governments, and notifications of the involved parties. Additionally, the framework has embedded tools to grant citizens access to the ongoing trials.

5.5 ICH Guideline for Good Clinical Practice (E6)

ICH Guideline for Good Clinical Practice (GCP) is an international ethical and scientific quality standard for designing, conducting, recording and reporting trials that involve the participation of human subjects.[268] Compliance with this standard provides public assurance that the rights, safety and well-being of trial subjects are protected, consistent with the principles that have their origin in the Declaration of Helsinki and that the clinical trial data are credible. The objective of GCP is to provide a unified standard within the European Union (EU), Japan and the United States to facilitate the

mutual acceptance of clinical data by the regulatory authorities in these jurisdictions.[269]

GCP should be followed when generating clinical trial data that are intended to be submitted to regulatory authorities. The principles established in this guideline may also be applied to other clinical investigations that may have an impact on the safety and well-being of human subjects.[270] It enforces tight guidelines on ethical aspects of a clinical study. High standards are required in terms of comprehensive documentation for the clinical protocol, record keeping, training, and facilities, including computer hardware and software. Quality assurance and inspections ensure that these standards are achieved. GCP aims to ensure that the studies are scientifically robust and that the clinical properties of the investigational product are properly documented. GCP also provides clear guidance on the informed consent requirements that need to be signed by the study participant. As this is the basic human protection and research/data quality standard it is fully applicable to the CYLCOMED project.

6 Research Ethics in CYLCOMED project

Ethics is regarded as the cornerstone of all projects funded by the European Commission. This can be illustrated through an EC statement which highlights that "ethics is an integral part of research from beginning to end, and ethical compliance is seen as pivotal to achieve real research excellence".[271] Therefore, EC requires that all research activities carried out under the Horizon 2020 Framework Programme are conducted in compliance with fundamental ethical principles.

Horizon 2020 Framework was established by EU Regulation no. 1291/2013.[272] The rules applicable to participation and dissemination in Horizon 2020 are set out in Regulation 1290/2013/EU.[273]

Regulation 1291/2013 lays out the ethical principles with which all actors in Horizon 2020 projects need to comply. It sets out that "*all research and innovation activities carried out under Horizon 2020 need to comply with ethical principles set out in this article and with relevant legislation*". Additionally, it obliges all actors in Horizon 2020 projects to pay particular attention "*to the principle of proportionality, the right to privacy, the right to protection of personal data, the right to the physical and mental integrity of a person, the right to non-discrimination and the right to ensure high levels of human health protection*".[274] Regarding the research ethics under the Horizon 2020 framework, it is important to emphasize the rules laid down by the four EC guidelines, which has been briefly touched below.

Guidance on how to complete the ethics self-assessment has been developed by EC aiming at facilitating the identification of any ethical issues that may arise, including the Ethics Checks and Audits.**[275]**

Ethics and data protection has the objective to ensure that all projects are guided by ethical considerations and the values and principles on which the EU is founded.**[276]**

It highlights that **data protection** is the cornerstone for research ethics in EU, as well as a fundamental human right. It is intimately linked to **autonomy and human dignity**, and the principle that everyone should be valued and respected[277]. The guidance note places particular attention on the research that involves the **processing of special categories of data and processing of personal data concerning children, which is the particular case in the Cylcomed environment**. As mentioned above, Cylcomed Pilot 2 "Cybersecurity for Telemedicine Platforms" will be conducted as an observational study by processing the personal data of patients, including pediatric patients, whereas no experiments will be conducted on them. Therefore, it is imperative to test the technologies developed in real-life, operational settings.

The **informed consent** is also one of the main elements of the guidance note, which states that "***Informed consent is the cornerstone of research ethics***".[278] Accordingly, it is essential to clearly communicate to participants the purpose of the study, the nature of their involvement, and any potential risks involved. Only after this information is conveyed to the participants, subject to the condition that information is fully understood by participants in the research, is it allowed to seek and obtain the participants' express permission to include them in the project.[279]

In other words, **individuals should not be the subject of a research project without being informed, while their informed consent must meet the minimum requirements stipulated by the GDPR.**

Further guidance on "informed consent" is provided by the **EC Guidance note on informed consent**.[280] This document lays down rules on, inter alia, obtaining the consent of a parent/legal representative and, where appropriate, the assent of the child. For instance, it is imperative that any information addressed to a child is in age-appropriate and plain language that they can easily understand. Besides, it is mandatory to apply the principle of protection by design to research data concerning children and minimise the collection and processing of their data as far as possible. According to the EC Guidance note on informed consent, "***Informed Consent*** *is the decision, which must be written, dated and signed, to take part in a clinical trial, taken freely after being duly informed of its nature, significance, implications and risks and appropriately documented, by any person capable of giving consent or, where the person is not capable of giving consent, by his or her legal representative; if the person concerned is unable to write, oral consent in the presence of at least one witness may be given in exceptional cases, as provided for in national legislation*".[281]

It is important to differentiate informed consent as an ethical standard from consent as a legal ground. Therefore, the consent requirements in the GDPR and the informed consent requirement in the CTR must not be confused. The former presents a legal ground for processing personal data, whereas the latter serves as an ethical standard and fundamental condition under which an individual can be included in an interventional clinical trial with a medicinal product.

Ethics in Social Science and Humanities serves as a crucial guide for social sciences and humanities (SSH) researchers to effectively identify and address ethical

considerations when participating in EU Framework Programme research and innovation initiatives. [282]

It sets out an overarching ethical principles that must be followed whenever research includes humans, which is the case with the CYLCOMED project. These overarching ethical principles in the context of EU-funded research include:

- respecting human dignity and integrity;
- ensuring honesty and transparency towards research subjects;
- respecting individual autonomy and obtain free and informed consent;
- protecting vulnerable individuals;
- ensuring privacy and confidentiality;
- promoting justice and inclusiveness;
- minimising harm and maximising benefit;
- sharing the benefits with disadvantaged populations, especially if the research is being carried out in developing countries;
- respecting and protecting the environment and future generations.[283]

European Code of Conduct for Research Integrity outlines the various professional, legal, and ethical obligations, while also recognising the crucial role of the institution in which the research takes place.[284] For instance, the European Code of Conduct for Research Integrity Article 1 lays down four ethical principles to which the consortium ought to adhere as they lie at the core of ethical research. These are:

- Reliability in ensuring the quality of research, reflected in the design, the methodology, the analysis and the use of resources;
- Honesty in developing, undertaking, reviewing, reporting and communicating research in a transparent, fair, full and unbiased way;
- Respect for colleagues, research participants, society, ecosystems, cultural heritage and their environment;
- Accountability for the research from idea to publication, for its management and organisation, for training, supervision and mentoring and for its wider impacts.

As the CYLCOMED project seeks to develop complex technical solutions concerning connected medical devices based on personal data processing, most notably sensitive data, the CYLCOMED project must uphold the highest ethical standards to achieve the balance between the research objectives and the means used by project partners to attain these goals. Therefore, it is crucial to ensure that the project does not compromise ethical principles. This will ensure the integrity of the research and maintain the trust and credibility of the proposed CYLCOMED technical solutions. It is worth mentioning that while the above is a preliminary overview of the ethical requirements that need to be met, the foundation of ethical requirements will be

developed further for the subsequent deliverables following the final definition of the use cases in the CYLCOMED project.

7 Conclusion

The purpose of the D2.1(T2.1) deliverable was to provide an overview of the applicable legal and ethical framework in the context of CYLCOMED design. The deliverable demonstrated how numerous and various the EU policy initiatives are when it comes to the CYLCOMED ecosystem. The Ethical and Legal Inventory is centred around six themes of relevance to CYLCOMED, namely: privacy and data protection, regulatory frameworks governing cybersecurity of medical devices, Artificial intelligence, clinical studies, and finally, research ethics.

Firstly, Chapter 2 has introduced, inter alia, requirements applicable to the processing of personal data stemming from the GDPR. This chapter explained the conditions for processing personal data such as the legal bases for processing data and the situations where processing of health-related data is allowed. CYLCOMED project should adhere to GDPR requirements. Furthermore, Chapter 3 tried to capture the essence of the regulatory frameworks governing the cybersecurity of medical devices. The complexity of the CYLCOMED project stems exactly from the fact that various legislative frameworks might fall into its scope and vice versa.

Chapter 4 has provided the current state of AI governance in the EU. It could be seen that Rules concerning AI mainly arise from soft law instruments, meaning that there is still no binding legal text. Nevertheless, these soft law recommendations are of great importance and have a significant impact in practice. A considerable part of the existing framework comprises of ethical principles and guidelines. Ethical principles, including human oversight, transparency and accountability should be fully respected in the design and development of AI-based technologies.

Last but not least, ethics are fundamental for successfully completing the CYLCOMED project. As such, throughout the development of CYLCOMED technical solutions, consortium members should always strive to uphold fundamental norms of ethical research. In Chapters 5 and 6 the main sources of EU guidance and requirements regarding clinical trials and research ethics are set out. CYLCOMED project should adhere to ethical principles, including human dignity, protection of health and environment and research integrity, satisfying all relevant compliance requirements for each specific activity. This is an integral part of all the research activities under the Horizon 2020 framework, from the outset to the end.

In order to provide both targeted guidance to partners and to be able to draw legal and regulatory conclusions from the interdisciplinary research in CYLCOMED, WP2 will extend this work in the context of Tasks 2.2 and 2.3. Considering the ever-changing legal landscape, as well as the development of CYLCOMED technical solutions, this deliverable is not a one-off exercise. It provides a first step in our legal research and serves as a solid basis for the upcoming in-depth ethical and legal study (Task 2.2).

References

[1] Coventry L, Branley D. Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. Maturitas. 2018 Jul;113:48-52. doi: 10.1016/j.maturitas.2018.04.008. Epub 2018 Apr 22. PMID: 29903648.

[2] Katherine Wellington, Cyberattacks on Medical devices and Hospital Networks: Legal Gaps and Regulatory Solutions, 30 Santa CLARA HIGH TECH. L.J. 139 (2014).

[3] Christine Hsu, *Many Popular Medical Devices May Be Vulnerable to Cyber Attacks,* **MEDICAL** DAILY. Available at: https://www.medicaldaily.com/many-popular-medical-devices-may-be-vulnerable-cyber-attacks-240096

[4] Hijmans, Hielke and Raab, Charles D., Ethical Dimensions of the GDPR (July 30, 2018). in: Mark Cole and Franziska Boehm (eds.), Commentary on the General Data Protection Regulation, Cheltenham: Edward Elgar (2018, Forthcoming) , Available at SSRN: https://ssrn.com/abstract=3222677

[5] Johan Rochel, Ethics in the GDPR: A Blueprint for Applied Legal Theory, International Data Privacy Law, Volume 11, Issue 2, April 2021, Pages 209–223, https://doi.org/10.1093/idpl/ipab007

[6] European Data Protection Supervisor, Opinion 4/2015, Towards a New Digital Ethics, p4. Available at https://edps.europa.eu/sites/default/files/publication/15-09-11_data_ethics_en.pdf

[7] In this connection, “positive” means existing.

[8] Politou, E., Alepis, E., Virvou, M., Patsakis, C. (2022). Privacy and Personal Data Protection. In: Privacy and Data Protection Challenges in the Distributed Era. Learning and Analytics in Intelligent Systems, vol 26. Springer, Cham. https://doi.org/10.1007/978-3-030-85443-0_2

[9] González Fuster, G. (2014). Privacy and the Protection of Personal Data Avant la Lettre . In: The Emergence of Personal Data Protection as a Fundamental Right of the EU. Law, Governance and Technology Series(), vol 16. Springer, Cham. https://doi.org/10.1007/978-3-319-05023-2_2

[10] Politou, E., Alepis, E., Virvou, M., Patsakis, C. (2022). Privacy and Personal Data Protection. In: Privacy and Data Protection Challenges in the Distributed Era. Learning and Analytics in Intelligent Systems, vol 26. Springer, Cham. https://doi.org/10.1007/978-3-030-85443-0_2

[11] González Fuster, G. (2014). The Beginning of EU Data Protection. In: The Emergence of Personal Data Protection as a Fundamental Right of the EU. Law, Governance and Technology Series(), vol 16. Springer, Cham. https://doi.org/10.1007/978-3-319-05023-2_5

[12] Rodotà, S. (2009). Data Protection as a Fundamental Right. In: Gutwirth, S., Poullet, Y., De Hert, P., de Terwangne, C., Nouwt, S. (eds) Reinventing Data Protection?. Springer, Dordrecht. https://doi.org/10.1007/978-1-4020-9498-9_3

[13] Smuha, N., Ahmed-Rengers, E., Harkens, A., Li, W., Maclaren, J., Piselli, R., & Yeung, K. (2021, Aug 5). How the EU can achieve legally trustworthy AI: a response to the European Commission’s proposal for an Artificial Intelligence Act. SSRN.

[14] Ibid.

[15] The Council of Europe is an international organisation established in 1949 to promote common and democratic principles across Europe. It currently has 46 member countries and is headquartered in Strasbourg. It should be differentiated from the European Council and the Council of the European Union which are the main EU institutions. The Council of Europe and the European Union share the same fundamental values – human rights, democracy and the rule of law – but are separate entities which perform different, yet complementary, roles. For more see https://coe.int/en/web/portal/european-union

[16] Member state of the Council of Europe: Albania, Andorra, Armenia, Austria, Azerbaijan, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Monaco, Montenegro, Netherlands, North Macedonia, Norway, Poland, Portugal, Moldova, Romania, Russian Federation, San Marino, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey, Ukraine, and the United Kingdom.

[17] Handbook on European data protection law - 2018 edition, p23.

[18] S.and Marper v UK App no 30562/04 (ECtHR 4 December 2008).

[19] Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS No. 108, 1981.

[20] de Terwangne, Cécile, 'Council of Europe Convention 108+: A Modernised International Treaty for the Protection of Personal Data', Computer Law and Security Review, 40.July 2013 (2021).

[21] Convention 108 Article 1.

[22] T. Mulder & M. Tudorica (2019) Privacy policies, cross-border health data and the GDPR, Information & Communications Technology Law, 28:3, 261-274, DOI: 10.1080/13600834.2019.1644068

[23] https://coe.int/en/web/data-protection/convention108/parties

[24] Handbook on European data protection law - 2018 edition, p25.

[25] Jorg Ukrow, Data Protection without Frontiers: On the Relationship between EU GDPR and Amended CoE Convention 108, 4 EUR. DATA PROT. L. REV. 239 (2018).

[26] Bertoni, Eduardo (2021): "Convention 108 and the GDPR: Trends and perspectives in Latin America", en Computer Law & Security Review (Vol. 40).

[27] The amending Protocol (CETS No. 223) to Convention 108 was adopted by the Committee of Ministers of the Council of Europe on 18 May 2018 on the occasion of its 128th session held in Elsinore, Denmark.

[28] EU Charter of Fundamental Rights | European Union Agency for Fundamental Rights (europa.eu)

[29] Ibid, 51(1).

[30] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data Official Journal L 281.

[31] Article 3(1) GDPR.

[32] Article 3(2) GDPR.

[33] Article 4(1) GDPR.

[34] Article 4(2) GDPR.

[35] WP29, "Opinion 4/2007 on the concept of personal data", 20 June 2007, p6.

[36] Ibid, p9.

[37] Ibid, p12.

[38] Recital 27 GDPR.

Funded by Horizon Europe Framework Programme of the European Union

[39] EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Guidelines 07/2020 on the concepts of controller and processor in the GDPR | European Data Protection Board (europa.eu)

[40] Ibid.

[41] Article 26 GDPR.

[42] Article 29 Data Protection Working Party, WP 169 (2010), p. 19.

[43] EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, p24.

[44] Ibid.

[45] Ibid.

[46] Article 28(10) GDPR.

[47] EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, p30.

[48] Ibid, p32

[49] Ibid, p33

[50] EU Agency for Fundamental Rights, Handbook on European Data Protection Law, 2018, section 3.1.2.

[51] EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, p19. available at https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf

[52] Ibid, p12.

[53] Recital 39 GDPR.

[54] EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, p15.

[55]WP29 Guidelines on transparency under Regulation 2016/679. Available at file:///C:/Users/u0161701/Downloads/20180413_article_29_wp_transparency_guidelines_7B894B16-B8B9-B044-ED400A6DBAA4FA60_51025%20(4).pdf

[56] Article 5(1)(b) GDPR.

[57] Article 5(1)(c) GDPR.

[58] Article 5(1)(f) GDPR.

[59] Explanatory Report of Modernised Convention 108, para. 56; Article 32(1) GDPR

[60] Art. 28, 29 and 32 GDPR.

[61] Recital 42 GDPR.

[62] Recital 32 GDPR

[63] EDPB Guidelines 5/2020 on consent under Regulation 2016/679.

[64] Article 7(3) GDPR.

Funded by Horizon Europe Framework Programme of the European Union

[65] EDPB Guidelines 05/2020 on consent under Regulation 2016/679.

[66] EDPB, 'Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects', 8 October 2019 (Version 2.0).

[67] Recital 46 GDPR.

[68] Recital 45 GDPR.

[69] WP29, 'Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC' 844/14/EN WP 217, 9 April 2014

[70] ICO's Guide "Lawful basis for processing: Legitimate interest'' (2018) legitimate-interests-1-0.pdf (ico.org.uk)

[71] EDPB, "Guidelines 05/2020 on consent under Regulation 2016/679", 4 May 2020 (Version 1.1), p. 20

[72] GDPR Article 9(2)(b).

[73] GDPR Article 9(2)(c).

[74] GDPR Article 9(2)(d).

[75] GDPR Article 9(2)(e).

[76] GDPR Article 9(2)(f).

[77] GDPR Article 9(2)(g).

[78] GDPR Article 9(2)(h).

[79] GDPR Article 9(2)(i).

[80] GDPR Article 9(2)(j).

[81] WP29, Guidelines on Data Protection Officer under Regulation 2016/679

[82] Article 12(1) GDPR

[83] Guidelines on Transparency under Regulation 2016/679, p12.

[84] Ibid p12.

[85] Ibid.

[86] GDPR, Articles 13(3) and 14(4)

[87] GDPR Recital 58

[88] Article 8 (2).

[89] GDPR Recital 63.

[90] Ibid.

[91] Guidelines 01/2022 on data subject rights - Right of access, 28 March 2023, p. 22

[92] GDPR Recital 63.

[93] Ibid, p28.

[94] Ibid, p43.

[95] Ibid, p43.

[96] GDPR Article 12(5).

[97] GDPR Article 15(4)

Funded by Horizon Europe Framework Programme of the European Union

[98] GDPR Article 23.

[99] GDPR, Article 17(1).

[100] GDPR, Article 18(2).

[101] WP29 “Guidelines on the right to data portability”, p18.

[102] GDPR Recital 68.

[103] GDPR Article 21(1).

[104] GDPR Article 21(3).

[105] GDPR Article 21(5).

[106] GDPR Article 21(6).

[107] GDPR, Article 21(2)

[108] WP29, ‘Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, p7

[109] GDPR, Article 22(4)

[110] WP29, ‘Guidelines on Data Protection Officers (‘DPOs’)’, 16/EN WP 243 rev.01, 5 April 2017, p. 6

[111] WP29, ‘Guidelines on Data Protection Officers (‘DPOs’)’, 16/EN WP 243 rev.01, 5 April 2017, p. 7

[112] Ibid.

[113] See for more Recital 91 GDPR.

[114] GDPR Recital 91, WP29, ‘Guidelines on Data Protection Officers (‘DPOs’)’, 16/EN WP 243 rev.01, 5 April 2017, p. 8

[115] WP29, “Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679’, 17/EN WP248 rev.01, 4 October 2017, p. 9”

[116] Ibid, p7-9.

[117] GDPR Recital 75

[118] Article 29 Working Party (2017), Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in high risk” for the purposes of Regulation 2016/679, WP 248 rev.01, Brussels, 4 October 2017 p. 9

[119] GDPR Article 36(1).

[120] GDPR Recital 85.

[121] WP29, ‘Guidelines on Personal data breach notification under Regulation 2016/679’, 18/EN WP250 rev.01, 6 February 2018, p. 10-11.

[122] GDPR Article 34.

[123] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the European Health Data Space COM/2022/197 final. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52022PC0197

Funded by Horizon Europe Framework Programme of the European Union

[124] Terzis, P., & Santamaria Echeverria, (Enrique) OE. (2023). Interoperability and governance in the European Health Data Space regulation. *Medical Law International*, *0*(0). https://doi.org/10.1177/09685332231165692

[125] Explanatory memorandum p1.

[126] EDHS Article 1.

[127] Ibid, Article 2(2)(c).

[128] Ibid, Article 2(2)(a).

[129] Ibid, Article 2(2)(d).

[130] For more see European Commission's, Assessment of the EU Member States' rules on health data in the light of the GDPR , 2021.

[131] Ibid, Article 2(2)(e).

[132] EDHS Article 36.

[133] EDHS Articles 56, 57 and 58.

[134] Terzis, P., & Santamaria Echeverria, (Enrique) OE. (2023). Interoperability and governance in the European Health Data Space regulation. *Medical Law International*, *0*(0). https://doi.org/10.1177/09685332231165692, p3.

[135] ENISA Threat Landscape (ETL) report 2022. Available at https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

[136] Biasin, Elisabetta and Kamenjasevic, Erik, Cybersecurity of Medical Devices: Regulatory Challenges in the EU (September 30, 2020). The Future of Medical Device Regulation: Innovation and Protection, Cambridge University Press, 2020, Available at SSRN: https://ssrn.com/abstract=3855491 or http://dx.doi.org/10.2139/ssrn.3855491

[137] Chowdhury, N. (2014). Conceptualizing Multilevel Regulation. In: European Regulation of Medical Devices and Pharmaceuticals. Springer, Cham. https://doi.org/10.1007/978-3-319-04594-8_2

[138] Biasin, Elisabetta and Kamenjasevic, Erik, Cybersecurity of Medical Devices: Regulatory Challenges in the EU (September 30, 2020). The Future of Medical Device Regulation: Innovation and Protection, Cambridge University Press, 2020, Available at SSRN: https://ssrn.com/abstract=3855491 or http://dx.doi.org/10.2139/ssrn.3855491

[139] 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)

[140] CSA Article 5.

[141] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

[142] CSA Article 6.

[143] CSA Article 7.

[144] CSA Article 12.

[145] CSA Article 8.

Funded by Horizon Europe Framework Programme of the European Union

[146] CSA Article 9.

[147] CSA Recital 69.

[148] CSA Article 46.

[149] CSA Article 47(1)(2).

[150] CSA Recital 84.

[151] CSA Article 49(1)(7).

[152] CSA Article 52(1).

[153] CSA Article 54.

[154] For more about Cybersecurity Certification visit https://certification.enisa.europa.eu/#about

[155] CSA Article 56(2).

[156] 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 (NISD).

[157] Markopoulou, D., Papakonstantinou, V. and De Hert, P. "The New EU Cybersecurity Framework: The NIS Directive, ENISA's Role and the General Data Protection Regulation" (November 1, 2019). Computer Law & Security Review, Volume 35, Issue 6, November 2019, 105336, Available at SSRN: https://ssrn.com/abstract=3493561 or http://dx.doi.org/10.2139/ssrn.3493561

[158] Impact assessment Proposal for directive on measures for high common level of cybersecurity across the Union | Shaping Europe's digital future (europa.eu)

[159] COMBINED EVALUATION ROADMAP/INCEPTION IMPACT ASSESSMENT, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=PI_COM:Ares(2020)3320999

[160] Biasin E, Siapka (2020) A SAFECARE D3.10. Implementation of ethics, privacy and confidentiality. https://www.safecare-project.eu.

[161] Biasin, E., Kamenjašević, E. Cybersecurity of medical devices: new challenges arising from the AI Act and NIS 2 Directive proposals. *Int. Cybersecur. Law Rev.* **3**, 163–180 (2022). https://doi.org/10.1365/s43439-022-00054-x

[162] Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (Text with EEA relevance) (notified under document number C(2003) 1422)**; EUR-Lex - 32003H0361 - EN - EUR-Lex (europa.eu)**

[163] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (Text with EEA relevance); EUR-Lex - 32022L2557 - EN - EUR-Lex (europa.eu)

[164] NIS 2 Directive Article 3(3).

[165] See for more Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare (OJ L 88, 4.4.2011, p. 45).

[166] Regulation (EU) 2022/2371 of the European Parliament and of the Council of 23 November 2022on serious cross-border threats to health and repealing Decision No 1082/2013/EU (OJ L 314, 6.12.2022, p. 26). "In the area of public health or for specific areas of public health relevant for the implementation of this Regulation or of the national prevention, preparedness and response plans, the Commission may, by means of implementing acts,

Funded by Horizon Europe

designate **EU reference laboratories** to provide support to national reference laboratories to promote good practice and alignment by Member States on a voluntary basis on diagnostics, testing methods, use of certain tests for the uniform surveillance, notification and reporting of diseases by Member States."

[167] See for more Directive 2001/83/EC of the European Parliament and of the Council of 6 November 2001 on the Community code relating to medicinal products for human use (OJ L 311, 28.11.2001, p. 67).

[168] Regulation (EU) 2022/123 of the European Parliament and of the Council of 25 January 2022on a reinforced role for the European Medicines Agency in crisis preparedness and management for medicinal products and medical devices (OJ L 20, 31.1.2022, p. 1).

[169] NIS 2 Directive Article 7.

[170] Ibid, Article 8.

[171] Ibid, Article 9.

[172] Ibid, Article 10.

[173] Ibid, Article 13.

[174] Ibid, Article 23(1).

[175] Ibid, Article 34(4)(5).

[176] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020.

[177] Impact assessment report on the Cyber Resilience Act (CRA). Available at Cyber Resilience Act - Impact assessment | Shaping Europe's digital future (europa.eu)

[178] CRA Explanatory memorandum.

[179] CRA Article 1.

[180] Ibid, Article 3(1).

[181] Ibid, Article 8.

[182] Ibid, Article 2(2).

[183] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC.

[184] Proposal for a Directive of the European Parliament and of the Council on the Resilience of critical entities, Explenatory Memorandum p1.

[185] CER Recital 4.

[186] Ibid, Recital 9.

[187] Ibid, Recital 13.

[188] Ibid Recital 24.

[189] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC.

[190] CER Article 2(4).

Funded by Horizon Europe Framework Programme of the European Union

[191] Ibid, Article 2(5).

[192] CER Directive Article 4.

[193] Ibid, Article 5.

[194] Ibid, Article 6.

[195] Ibid, Article 13.

[196] Ibid, Article 9.

[197] Ibid, Article 21.

[198] Ibid, Article 11.

[199] Ibid, Article 12.

[200] Ibid, Article 13.

[201] Ibid, Article 13(1)(b)(e).

[202] Ibid, Article 15.

[203] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017, on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC, 2017 O.J. (L 117/1)

[204] MDR Article 1.

[205] Malvehy, J., Ginsberg, R., Sampietro-Colom, L., Ficapal, J., Combalia, M. and Svedenhag, P. (2022), New regulation of medical devices in the EU: impact in dermatology. J Eur Acad Dermatol Venereol, 36: 360-364. https://doi.org/10.1111/jdv.17830

[206] See more on Medical Devices Coordination Group, ""Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR". DocsRoom - European Commission (europa.eu)

[207] Biasin, E., & Kamenjasevic, E. (2022). Cybersecurity of Medical Devices: Regulatory Challenges in the European Union. In I. Cohen, T. Minssen, W. Price II, C. Robertson, & C. Shachar (Eds.), The Future of Medical Device Regulation: Innovation and Protection (pp. 51-62). Cambridge: Cambridge University Press. doi:10.1017/9781108975452.005

[208] Ibid, Article 2(30).

[209] The intended purpose is defined in Article 2(12) as "the use for which a device is intended according to the data supplied by the manufacturer on the label, in the instructions for use or in promotional or sales materials or statements and as specified by the manufacturer in the clinical evaluation."

[210] Macomber, L.S., Alexandra, A. (2017). General safety and performance requirements (Annex I) in the new medical device regulation. In BSI White Paper. BSI Online 2017.

[211] MDCG 2021-24 Guidance on classification of medical devices. mdcg_2021-24_en_0.pdf (europa.eu)

[212] MDR Recital 44.

[213] MDR Article 2(65).

Funded by Horizon Europe Framework Programme of the European Union

[214] Ibid, 2(66) "'serious public health threat' means an event which could result in imminent risk of death, serious deterioration in a person's state of health, or serious illness, that may require prompt remedial action, and that may cause significant morbidity or mortality in humans, or that is unusual or unexpected for the given place and time;"

[215] Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU (Text with EEA relevance).

[216] IVDR Article 1(1).

[217] MDCG (2019a) Guidance on cybersecurity of medical devices. https://ec.europa.eu/docsroom/documents/41863.

[218] Ibid, p1.

[219] Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC Text with EEA relevance

[220] RED Article 1.

[221] Ibid, Article 2(1)(1)

[222] Biasin, Elisabetta and Kamenjasevic, Erik, Cybersecurity of Medical Devices: Regulatory Challenges in the EU (September 30, 2020). The Future of Medical Device Regulation: Innovation and Protection, Cambridge University Press, 2020, Available at SSRN: https://ssrn.com/abstract=3855491

[223] Council Directive 96/98/EC of 20 December 1996 on marine equipment (OJ L 46, 17.2.1997, p. 25).

[224] Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91 (OJ L 212, 22.8.2018, p. 1).

[225] RED Article 1(3).

[226] Ibid, Article 3(1)(2).

[227] IMPACT ASSESSMENT REPORT Accompanying the document Commission Delegated Regulation supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3), points (d), (e) and (f), of that Directive. Available at SWD(2021) 302_EN_impact_assessment_part1_v3.pdf (europa.eu)

[228] Ibid, p. 72.

[229] Commission Delegated Regulation (EU) 2022/30 of 29 October 2021 supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3), points (d), (e) and (f), of that Directive (Text with EEA relevance). Available at EUR-Lex - 32022R0030 - EN - EUR-Lex (europa.eu)

Funded by Horizon Europe Framework Programme of the European Union

[230] Ibid, Article 1. defines **internet-connected radio equipment as** any radio equipment that can communicate itself over the internet, whether it communicates directly or via any other equipment.

[231] The provisions of the Regulation shall apply from 1 August 2024, whereas delegated regulation will not affect radio equipment placed on the Union market before that date of applicability

[232] Guide to the Radio Equipment Directive 2014/53/EU. Available at DocsRoom - European Commission (europa.eu)

[233] Ibid, p.46.

[234] Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206

[235] Ibid, p9.

[236] Ibid, p3.

[237] Ibid, Article 1.

[238] Ibid, Article 3(2).

[239] Ibid, Article 3(4).

[240] Ibid, Article 2.

[241] Ibid, Article 2(3).

[242] Ibid, Article 2(4).

[243] Ibid, Article 8-15.

[244] Ibid, Article 9(1)(2).

[245] Konttila, Jenni and Väyrynen, Karin, "CHALLENGES OF CURRENT REGULATION OF AI-BASED HEALTHCARE TECHNOLOGY (AIHT) AND POTENTIAL CONSEQUENCES OF THE EUROPEAN AI ACT PROPOSAL" (2022). 13th Scandinavian Conference on Information Systems. https://aisel.aisnet.org/scis2022/7

[246] Ibid, Title IV.

[247] Ibid, Article 69.

[248] Ibid, Article 71.

[249] 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 Coordinated Plan on Artificial Intelligence. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:795:FIN.

[250] European Commission, The High-Level Expert Group on AI, Ethics Guidelines for Trustworthy AI, 2019Ethics guidelines for trustworthy AI. https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

[251] Ibid, p4.

[252] Ibid.

[253] Ibid, p10-11.

[254] Ibid, p11-13.

[255] Ibid, p14.

Funded by Horizon Europe Framework Programme of the European Union

[256] THE ASSESSMENT LIST FOR TRUSTWORTHY ARTIFICIAL INTELLIGENCE (ALTAI). Available at altai_final_14072020_cs_accessible2_jsd5pdf_correct-title_3AC24743-DE11-0B7C-7C891D1484944E0A_68342(1).pdf

[257] Available at https://futurium.ec.europa.eu/en/european-ai-alliance/pages/welcome-altai-portal

[258] World Medical Association Declaration of Helsinki – Ethical Principles for Medical Research Involving Human Subjects.

[259] Wu Y, Howarth M, Zhou C, Hu M, Cong W. Reporting of ethical approval and informed consent in clinical research published in leading nursing journals: a retrospective observational study. BMC Med Ethics. 2019 Dec 5;20(1):94. doi: 10.1186/s12910-019-0431-5. PMID: 31805918; PMCID: PMC6896583.

[260] Frédérique Claudot and others, Ethics and observational studies in medical research: various rules in a common framework, International Journal of Epidemiology, Volume 38, Issue 4, August 2009, Pages 1104–1108, https://doi.org/10.1093/ije/dyp164

[261] World Medical Association Declaration of Taipei on ethical considerations regarding health databases and biobanks.

[262] Ibid, Article 19.

[263] Directive 2001/20/EC of the European Parliament and of the Council of 4 April 2001 on the approximation of the laws, regulations and administrative provisions of the Member States relating to the implementation of good clinical practice in the conduct of clinical trials on medicinal products for human use. Available at https://health.ec.europa.eu/system/files/2016-11/dir_2001_20_en_0.pdf

[264] Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC Text with EEA relevance. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014R0536

[265] For more see https://health.ec.europa.eu/medicinal-products/clinical-trials/clinical-trials-directive-200120ec_en

[266] Ibid, CTR Recital 82

[267]https://health.ec.europa.eu/medicinal-products/clinical-trials/clinical-trials-regulation-eu-no-5362014_en

[268] Available at https://www.ema.europa.eu/en/documents/scientific-guideline/ich-guideline-good-clinical-practice-e6r2-step-5_en.pdf

[269] Ibid, p6.

[270] Ibid.

[271] Available at https://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/ethics_en.htm

[272] 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.

[273] Regulation (EU) No 1290/2013 of the European Parliament and of the Council of 11 December 2013 laying down the rules for participation and dissemination in "Horizon 2020 - the Framework Programme for Research and Innovation (2014-2020)" and repealing Regulation (EC) No 1906/2006.

Funded by Horizon Europe Framework Programme of the European Union

[274] Article 19. 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.

[275] Horizon 2020 Programme Guidance: How to complete your ethics self-assessment, European Commission, February 2019.

[276] Ethics and data protection, European Commission, November 2018.

[277] Ibid, p3.

[278] Ibid, p10.

[279] Ibid.

[280] EC Guidance note on informed consent. Available at: https://ec.europa.eu/research/participants/data/ref/fp7/89807/informed-consent_en.pdf

[281] Ibid, p1.

[282] Ethics in Social Science and Humanities, European Commission, October 2018.

[283] Ibid, p.5.

[284] The European Code of Conduct for Research Integrity, ALLEA - All European Academies.

Funded by Horizon Europe Framework Programme of the European Union