Cyber-security toolbox
for connected medical devices

D2.2 Examination of Ethical, Legal and Data Protection Requirements

Revision: v.1.0

Work package	WP 2
Task	Task 2.2
Due date	31/5/2024
Submission date	31/05/2024
Deliverable lead	KUL
Version	1.0
Author	Dusko Milojevic (KUL)
Coauthor	Maja Nisevic (KUL)
Project PI	Jan De Bruyne (KUL)
Reviewer	Juan Carlos Pérez Baún (Eviden-Atos)
Abstract	T2.2 further elaborates on the legal and ethical frameworks and requirements identified in T2.1. It provides a detailed ethical and legal analysis of the relevant EU legislation, jurisprudence, and doctrine regarding the technology to be developed. In addition, it will further examine in detail how the MCDG 2019-19 should be implemented in conjunction with all the applicable legal frameworks.

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

DOCUMENT REVISION HISTORY

Version	Date	Description of change	List of contributor(s)
V0.1	4/05/2024	First draft	Dusko Milojevic (KUL)
V0.2	8/05/2024	Comments on the First Draft	Maja Nisevic (KUL)
V0.3	12/05/2024	Implementation of Comments	Dusko Milojevic (KUL)
V0.4	20/05/2024	Internal Review	Juan Carlos Pérez Baún (Eviden-Atos)
V0.5	28/05/2024	Implementation of Comments	Dusko Milojevic (KUL)
V0.6	28/05/2024	Internal Review	Juan Carlos Pérez Baún (Eviden-Atos)
V1.0	28/05/2024	Implementation of Comments	Dusko Milojevic (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*	**x**
SEN	*Sensitive, limited under the conditions of the Grant Agreement*	
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

This deliverable is an in-depth legal and ethical study of CYLCOMED, and it should be read in conjunction with Deliverable D2.1, “Analysis of Ethical, Legal and Data Protection Frameworks.” It delves further into the legal and ethical frameworks that govern the CYLCOMED project design and its use cases.

This deliverable will focus on the frameworks governing the cybersecurity of medical devices and outline the main definitions and obligations applicable to the CYLCOMED stakeholders to facilitate legal and ethical compliance. Medical device cybersecurity will be observed through different legal frameworks relevant to CYLCOMED, such as frameworks that govern privacy and data protection, medical devices and artificial intelligence. The principal theme of this deliverable centres on the importance of ensuring that the privacy and data protection standards set by the GDPR are upheld in the design and deployment of the CYLCOMED project architecture. Furthermore, this deliverable examines the legal and ethical challenges relevant to the involvement of children in clinical studies.

This deliverable presents and specifies the overarching framework and its possible application to CYLCOMED. These requirements should be considered and integrated where feasible throughout the CYLCOMED project. Hence, the document is addressed to all CYLCOMED Consortium partners and its solutions as guidance material to promote compliance with the applicable legal and ethical principles.

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
IRB	Institutional Review Board
MDD	Medical Device Directive
MDCG	Medical Device Coordination Group
MDR	Medical Devices Regulation
NIS2	Network and Information Security Directive
RED	Radio Equipment Directive
REC	Research Ethical Committee

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

Funded by Horizon Europe Framework Programme of the European Union

1 Introduction

This deliverable builds on **D2.1 "**Analysis of Ethical, Legal and Data Protection Frameworks**"** [1], Deliverable **D5.1** "CYLCOMED toolbox prototype" [2], and Deliverable **D6.1** "Pilot planning and evaluation strategy" [3]. While it extends to the legal and ethical frameworks identified in the first KUL deliverable (D2.1), the legal and ethical analysis is applied to the development of the CYLCOMED cybersecurity toolbox and CYLCOMED pilots implementation.

As such, it aims to provide a detailed analysis of the applicable legal and ethical framework for the CYLCOMED. It will further analyse and discuss the identified legal and ethical frameworks, tailoring them to the CYLCOMED project architecture. More specifically, this document aims to inform and guide CYLCOMED Consortium partners of their legal obligations concerning the EU norms on privacy and data protection, cybersecurity and artificial intelligence. Furthermore, this deliverable examines the legal and ethical challenges relevant to the involvement of children in clinical studies and conducting health-related research in a broader context. This legal and ethical analysis should guide the architects and developers of the CYLCOMED toolbox who are creating the technical and functional specifications of the use cases. Hence, they consider the ethical principles and legal requirements laid down by legal and ethical frameworks relevant to the CYLCOMED project. Therefore, the purpose of this deliverable is threefold: (i) to analyse in more detail the EU legislation, case law and doctrine; (ii) to assess the legal and ethical implications of the CYLCOMED ecosystem; (iii) to provide recommendations for the legal and ethical design of the CYLCOMED architecture.

Hence, the in-depth legal and ethical analysis provided by this deliverable should serve as input for the **WP4** "Risk Management for CMDs", **WP5** "Cybersecurity Toolbox Design and Implementation" and **WP6** "Integration and Validation with Real-world Applications", as well as guidance for legal and ethical compliance. Additionally, to avoid repetition, specific legal requirements that stem from analysed legal frameworks will be provided as a contribution to the **WP3** deliverable **D3.2** "Requirements and specifications consolidation".

Besides the existing legal framework for medical device cybersecurity, this deliverable will provide an overview and analysis of the most relevant legislative initiatives undergoing legislative procedure due to their relevance and possible influence on the CYLCOMED design. It is important to note that while this deliverable will build on the Deliverable D2.1 "Analysis of Ethical, Legal and Data Protection Frameworks," it will provide the basis for the subsequent D2.3 deliverable within Work Package 2 (WP2) of CYLCOMED.

Funded by Horizon Europe Framework Programme of the European Union

1.1 Purpose and Scope

The CYLCOMED addresses the overall ambitious goal of strengthening the cybersecurity of connected medical devices (CMDs). 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 twin’s simulation without the involvement of any human participants, Pilot 2 “, Cybersecurity for Telemedicine Platforms”, will be conducted as an observational study. The CYLCOMED’s ultimate goal is twofold: on the one hand, to improve the effectiveness and quality of personalised healthcare services, and on the other hand, to reduce risks and non-compliance costs. The project aims to identify gaps and introduce new requirements from innovative analysis schemes, establishing an adequate balance between patient benefits and cybersecurity risks. A complete overview of the CYLCOMED pilots has been elaborated in the Deliverable D5.1 [4], whereas the prototype of the first iteration of the CYLCOMED Cybersecurity toolbox has been described in the Deliverable D6.1 [5].

The cybersecurity regulatory landscape in the EU is evolving rapidly. Medical device stakeholders already operate within a complex legal environment, and new legislative initiatives introduce additional layers of complexity and uncertainty.

1.2 Structure

This document's legal and ethical analysis is performed within the four main chapters: Privacy and Data Protection, Cybersecurity of CMD, Artificial Intelligence, and Ethical requirements for participation in health-related research. Each chapter lays down the legal framework comprising the principal normative acts relevant to its theme, briefly explaining the subject matter and its relevance to CYLCOMED.

Chapter 2 covers the principal theme of privacy and data protection regulatory frameworks. It provides an analysis of both existing and upcoming legislative acts relevant to cybersecurity data governance. Chapter 3 analyses the cybersecurity framework related to connected medical devices.

Chapter 4 analyses documents related to the legal frameworks governing Medical Devices, whereas Chapter 5 examines documents related to the AI legal and ethical frameworks. The 6th Chapter provides an analysis of requirements laid down by ethical guidance and legal acts. Chapter 7 presents the concluding remarks.

An overview of the legal and ethical frameworks is presented in the diagram below (Figure 1).

Funded by Horizon Europe Framework Programme of the European Union

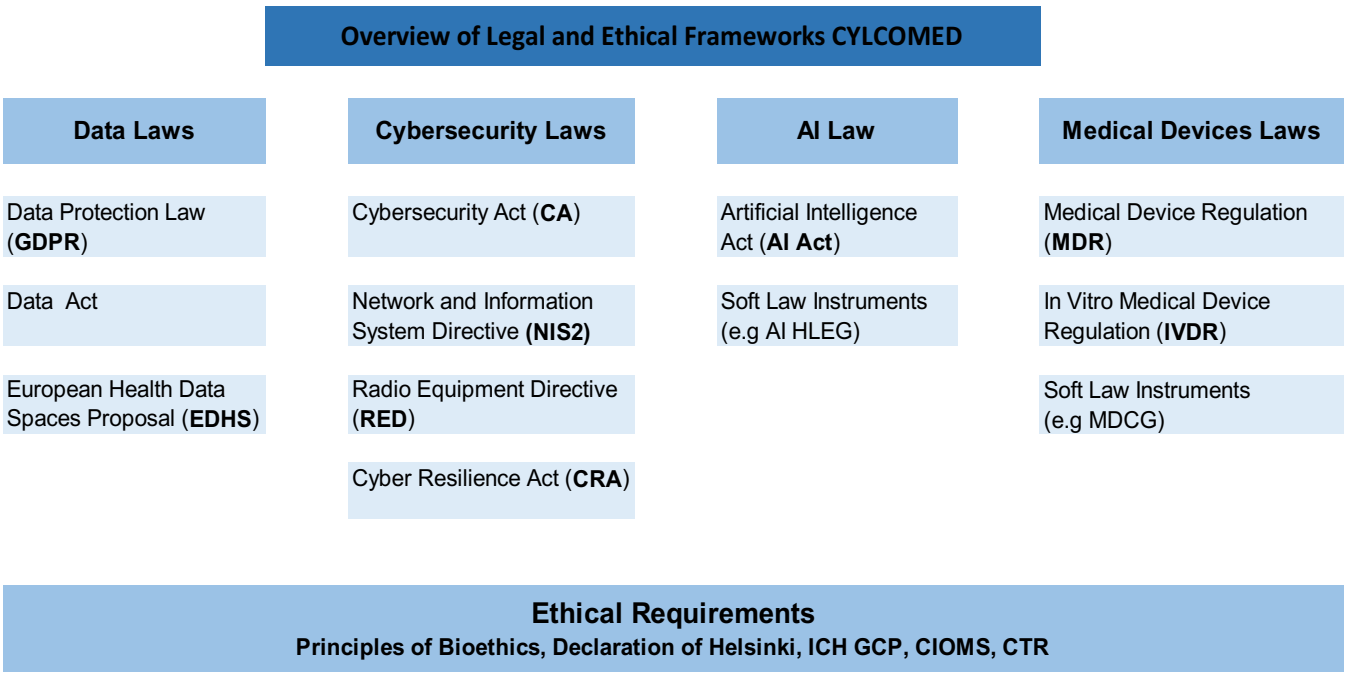

Figure 1Overview of Legal and Ethical Frameworks relevant to CYLCOMED

Funded by Horizon Europe Framework Programme of the European Union

2 Privacy and Data Protection Legal Framework

This chapter will overview the main regulatory instruments applicable to the CYLCOMED technology under Europe's privacy and data protection regime. While the first deliverable provided an analysis of the relevant international treaties and primary and secondary sources of EU legislation, this section will focus on the legal and ethical requirements that are essential for the CYLCOMED project architecture and compliance. The analysis will primarily encompass a detailed analysis of the GDPR, Data Act, and EDHS.

However, it is essential to first distinguish the notion of privacy from that of data protection. Even though privacy and personal data protection are two interrelated terms that are often used interchangeably, it is essential to note that they actually constitute two discrete and different notions [6]. 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, builds upon UDHR and provides that everyone has the right to respect his or her private and family life, home and correspondence [7]. 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" [8]. 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 [9]. 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 [10]. 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 [11]. 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 [12].

2.1 General Data Protection Regulation and CYLCOMED Design

Deliverable D2.1(T2.1) provided an overview of the applicable legal and ethical framework in the context of CYLCOMED design, placing a specific emphasis on GDPR

Funded by Horizon Europe Framework Programme of the European Union

compliance. This section will extend the analysis presented in the KUL's first deliverable, and provide a more detailed overview, elaborating more on specific normative requirements of relevance for CYLCOMED compliance, while providing concrete recommendations to Consortium partners that should be taken into account in the execution of CYLCOMED pilots.

It is imperative that all EU-funded projects demonstrate compliance with the General Data Protection Regulation (GDPR). Data protection stands as a central concern in research ethics throughout Europe, serving not only as a fundamental human right but also as a cornerstone of autonomy and human dignity. It embodies the principle that every individual deserves to be valued and respected, reinforcing the ethical imperative to safeguard personal data with utmost care and integrity [13]. By providing cybersecurity solutions to enhance the cybersecurity of connected medical devices, the CYLCOMED project will necessarily engage in processing personal data. More specifically, throughout the project lifespan, it is envisaged that the children's health-related data will be processed under the activities conducted in Pilot 2. Therefore, GDPR compliance presents one of the key pillars of the CYLCOMED project.

Although CYLCOMED Pilot 1 will be performed at laboratory level and will not encompass personal data processing, all recommendations given in this section would apply to Pilot 1 if it was performed in the real-life scenario.

The compliance analysis in this report is structured to provide a comprehensive understanding of GDPR compliance in the CYLCOMED project. It begins with a discussion on the concept of personal data, followed by the legal grounds for processing such data. The key actors responsible for compliance are then identified, and their respective obligations are elaborated upon. The rights of data subjects regarding their data are also outlined. The chapter concludes by highlighting the importance of the data protection officer, data protection impact assessment, personal data breaches, and record-keeping obligations for the CYLCOMED project.

2.1.1 Material Scope of Application

The GDPR entered into force on 25 May 2018, replacing Directive 95/46/EC (the GDPR) [14]. 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. This technology-neutral approach, as foreseen by the EU legislator, seeks to make the data protection legislation fit for the digital age. Given the extensive scope of the GDPR, it is crucial to outline the key concepts that determine its application. This involves identifying two distinct components within Article 2. First, for

Funded by Horizon Europe Framework Programme of the European Union

the GDPR to apply, the **data must qualify as personal data**. Second, this personal data **must undergo processing**, either wholly or partly, through automated means. Alternatively, if the data are processed in a non-automated manner, they must be part of a filing system or intended to be part of one.

Given the complexity, it is important to further clarify the building blocks that constitute the material scope, namely, when data are to be considered '*personal data*', and what falls under the scope of "processing". More specifically, as stated above, GDPR Article 2(1) states that the Regulation applies to the **processing** of ***personal data.*** Therefore, "**personal data**" and "**processing**" are threshold concepts for the general application of data protection law. Thus, it is important to introduce these definitions more closely.

2.1.2 Personal Data

Article 4(1) of the GDPR defines the concept of "personal data" as follows:

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

The GDPR contains a broad notion of personal data. It may consist of any information, not only information concerning what is traditionally considered within the private sphere. The Article 29 Working Party (hereafter, 'WP29'), precursor to the European Data Protection Board (EDPB), underscored that the concept of personal data was intentionally formulated broadly to ensure adequate protection for data subjects regarding the processing of their data. However, to avoid excessively broad interpretation, the WP29 issued guidelines on the definition of personal data, identifying four essential elements inherent in the legal definition provided in Article 4(1) of the GDPR [15]. These building blocks are: "Any information", "Relating to", "Identified or identifiable", and "Natural person", as it is shown in Figure 2:

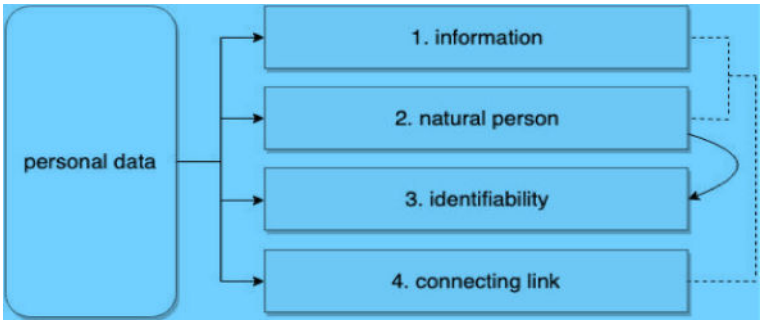

Figure 2 Personal Data Building Blocks

Funded by Horizon Europe Framework Programme of the European Union

2.1.2.1 The meaning of “Any information”

The expression “any information” underlines the legislator's intention 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 [16]. Some of the examples of personal data that were subject of case law by the Court of Justice of the European Union are, inter alia, name, date of birth, nationality, gender, ethnicity, religion and language [17], telephone numbers, employment and hobbies [18], dynamic IP address [19], fingerprints [20] and salaries of employees of a public body [21].

The concept of personal data encompasses information in any format or medium, whether it is alphabetical, numerical, graphical, photographic, or acoustic. This includes information stored on paper, in computer memory using binary code, or on a videotape, among other forms of storage. The key consideration is whether the information relates to an identified or identifiable individual, regardless of the specific format or medium in which it is stored [22]. However, it is important to note that determining whether data qualifies as personal data depends on the context and requires a case-by-case analysis.

2.1.2.2 The Meaning of “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. In many instances, such a connection can be easily recognised. For example, details of a patient's diagnostic examination within their medical history are directly related to that specific patient. Similarly, the patient's drug prescriptions, whether recorded in a single prescription or derived from multiple prescriptions, are also inherently linked to the individual patient [23].

2.1.2.3 The Meaning of “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 or physiological identity of a particular individual [24]. Additionally, a person is considered “identifiable” when someone may not have been identified yet, but it is possible to do so. This may be the case directly, e.g., through one’s name, or indirectly through ID or telephone numbers. Another example is geolocation data. While location data can be challenging to define and regulate, it is considered “personal information” when the data relates to an identifiable person. More specifically, personal location data is any location data directly or indirectly linked to an individual, or that can be directly or indirectly used to identify an individual [25]. By combining the GPS coordinates of the location of a smartphone and telephone subscription account information linked to the smartphone, a natural person might be identified, thus subject protection provided by the GDPR. Besides, possible attributes include computerised files, cookies and web traffic surveillance tools. It is not necessary to have the name or other explicit information, such as the address of the

Funded by Horizon Europe Framework Programme of the European Union

individual, disclosed. However, whether a person is identifiable will always depend on the case-specific circumstances.

To determine whether a person is identifiable, all the means likely reasonably to be used by the controller or any other person to identify the individual at issue should be taken into account. To ascertain whether means are reasonably likely to be used to identify the individual, all objective factors should be taken into account (e.g., the costs and the amount of time required for identification, the available technology at the time of processing, technological developments) [26]. However, this criterion would not be met if identifying a data subject requires an unreasonable amount of time, cost, or effort, making the probability of identification negligible in practice. The UK GDPR provides a non-exhaustive list of common identifiers that, when used, may allow the identification of the individual to whom the information in question relates [27]. These identifiers include:

Examples of common identifiers:

- Name;
- Photo;
- Passport or ID number;
- Telephone number and email address;
- Biometric data;
- Location data;
- An online identifier;

Examples of online identifiers:

- Internet protocol (IP) addresses;
- Cookie identifiers;
- Radio frequency identification (RFID) tags;
- MAC addresses;
- Advertising IDs;
- Pixel tags;
- Account handles and device fingerprints.

Significantly, for the CYLCOMED project, it must be underlined that the European independent bodies and courts apply a very low threshold for determining whether a piece of information allows singling out a person, bringing a wide variety of information within the scope of personal data. Technological tools and devices that collect information on the behaviour of a machine can make it possible to identify or influence the behaviour of their user or assign decisions for him or her without the necessity of identifying the identity of the individual in a strict sense.

Funded by Horizon Europe Framework Programme of the European Union

2.1.2.4 The Meaning of "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 are not protected by the GDPR [28]. However, even in these cases there are possible exceptions. In the former case, if the official title of a legal entity identifies one or more natural persons, the legal entity may have grounds to claim data protection for the individuals associated with it [29]. Regarding the latter, the data of the deceased persons may still indirectly receive protection in certain cases. For instance, the information on dead individuals may also refer to living persons. Thus, where the information which is data on the dead can be considered to relate at the same time also to the living and be personal data subject to the Directive, the personal data of the deceased may indirectly enjoy the protection of data protection rules. Moreover, Member States have the discretion to establish alternative rules for the protection of deceased persons, often accomplished through additional data protection measures, constitutional provisions, or recognition of personality rights [30].

Taking into account all the above mentioned, it stems that any combination of an identifier with a piece of information would be considered personal data if it allows for an individual to be singled out through reasonable practical means. Particularly in a digital ecosystem, online identifiers, either alone or in combination with other information, can be used to distinguish one user from another – in which case they are likely to qualify as personal data. Furthermore, it is crucial to highlight again that European doctrine and case-law tend to favour a broad interpretation of the concept of personal data. Consequently, the threshold for data to qualify as personal data is set quite low. Electronic devices no longer require the disclosure of someone's identity in the narrow sense, it is perfectly possible to categorise a person and link certain decisions to him or her, without specifically needing to know that person's name. It is important that the CYLCOMED toolbox developers and end-users are aware of this. Any type of data has the potential to become personal data. For instance, even simple traffic data within an information system, when linked to an employee's personal computer, may qualify as personal data. Actual identification of the data subject is not necessary for the GDPR to apply. The benchmark for determining this, is whether it is likely that reasonable means for identification will be available and administered by the foreseeable users of the information, including information held by third-party recipients.

Regarding the case law, in *Breyer v Bundesrepublik Deutschland,* the CJEU considered that a dynamic IP address, which an online media services provider registers when a person accesses a website that the provider has made accessible to the public, constitutes personal data where only a third party – the internet service provider in this case – has the additional data necessary to identify the person [31]. It held that "it is not required that all information enabling the identification of the data subject must be held in the hands of one person" for information to constitute personal data. Users of a dynamic IP address registered by an internet service provider may be identified in certain situations, for instance within the framework of criminal

Funded by Horizon Europe Framework Programme of the European Union

proceedings in the event of cyber-attacks, with the assistance of other persons. According to the CJEU, when the provider "has the legal means which enable it to identify the data subject with additional data which the internet provider has about that person", this constitutes "a means likely reasonable to be used to identify the data subject". Therefore, such data are considered personal data.

2.1.3 Special Categories of Personal Data

Some personal data are more sensitive in nature and, thus, enjoy higher protection under the GDPR, since they reveal information that could significantly jeopardise the fundamental rights and freedoms of the individuals concerned. The GDPR refers to these "sensitive" personal data as special categories of personal data. Therefore, these data enjoy special status and higher protection under the GDPR, which prohibits their processing unless specific conditions are met. This highlights the risk-based approach of the Regulation, which aims to protect individuals' rights and mitigate potential harms associated with sensitive personal data. Article 9(1) GDPR enlists the following data as special categories of personal data:

- Personal data revealing racial or ethnic origin;
- Personal data revealing political opinions, religious or other beliefs, including philosophical beliefs;
- Personal data revealing trade union membership;
- Genetic data;
- Biometric data processed for the purpose of uniquely identifying a person;
- Data concerning health;
- Data concerning a person's sex life or sexual orientation.

Since CYLCOMED pilot 2 will encompass the processing of health data, particular attention will be given to the analysis of this special category of data. It is helpful first to understand what constitutes "health data" under the GDPR. The common misconception is that this term refers simply to medical records, but the definition is much broader. Article 4(15) GDPR adopts a broad interpretation of the notion of data concerning health, encompassing all "***personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status***". GDPR Recital 35 further clarifies that personal data concerning health should include all data pertaining to the health status of a data subject, which reveals information relating to the past, current or future physical or mental health status of the data subject. Data concerning health include a wide range of personal data, for instance:

Funded by Horizon Europe Framework Programme of the European Union

- Any information on injury, disease, disability or disease risk, including medical history, clinical treatment, medical opinions, and diagnosis;
- Information collected when a person registers for healthcare or seeks medication;
- Information on medical appointments scheduling, reminders, and invoices for healthcare provisions that reveal information about a person's health;
- A number, symbol or other identifier assigned to an individual to uniquely identify them for health purposes when combined with information revealing something about the state of the individual's health;
- Data from medical examinations, test results, medical devices, or fitness trackers;

It is important to point out that, in certain circumstances**, data that initially may not appear to be related to health can nonetheless be categorised as health data**. There are certain types of data processing where it may not be immediately apparent whether it qualifies as processing health data. This is particularly true when data is processed for additional purposes, combined with other data, or transferred to third parties. Such processing can pose risks, including the risk of unfair treatment based on assumptions or actual health status inferred from the data. Due to possible "grey area", WP29 provides examples of potential indicators that health data are processed. More specifically, as clarified by WP29, raw, relatively low privacy impact personal data can quickly change into health data when the dataset can be used to determine a person's health status.

To assess this, it is not enough to only consider the nature of the data itself. The intended use of the data, either alone or in combination with other information, must also be taken into account. **This involves understanding how the data is intended to be used and the potential implications when combined with other sources of information.** The context and purpose of data processing play a crucial role in determining whether certain data should be considered as health data. For example, a single registration of a person's weight, blood pressure or pulse/heart rate (if not excessive in absolute terms), at least without any further information about age or sex, does not allow for the inference of information about the actual or likely future health status of that person. However, that aspect measured over time, especially in combination with age and sex, may be used to determine a significant aspect of an individual's health, such as the health risks related to obesity or an illness causing a significant loss of weight, high/low blood pressure, arrhythmia etc.

There must be a clear relationship between **the raw data set and the ability to determine a health aspect of a person, either based on the raw data itself or in combination with data from other sources**. This relationship should demonstrate how the data, whether on its own or when combined with other information, can be used to infer or ascertain a health-related aspect of an individual. For example, if a diet

Funded by Horizon Europe Framework Programme of the European Union

app only counts the calories as calculated from input provided by the data subject, and the information about the specific foods eaten is not stored, it would be unlikely that any meaningful conclusions can be drawn with regard to the health of that person (unless the daily intake of calories is excessive in absolute terms). But if data from a diet app, heart rate monitor or sleep diary app are combined with information provided by the data subject (directly or indirectly, for example, based on information collected from that person's social networking profile), conclusions (whether accurate or inaccurate) may be drawn about that person's health condition, such as medical risk or diabetics. In these cases, health data can likely be inferred from the combined data. It is important to emphasise that **data generated by devices** (such as those analysing a person's blood or measuring heart rate through apps) **may be classified as health data.** This classification applies irrespective of whether the testing is conducted by medical professionals or by devices/apps available on the market and regardless of whether these devices are marketed as medical devices. The critical factor is whether the data can be used to infer or determine an individual's health status or health-related information [32]. In other words, the source of the data is irrelevant in this context – they can come from a physician or other health professional, a hospital, a medical device, an in vitro diagnostic test, or a health/lifestyle/well-being app, so long conclusions can be reasonably drawn about the health status of a data subject.

On the other hand, it should be noted that data processing and sharing concerning health and genetic data is subject to different governance models and national laws. Article 9(4) GDPR states that Member States may introduce special conditions and limitations regarding the processing of genetic data and data concerning health. Different legal bases may apply depending on the aim for which the data is processed, such as patient care, cross-border access to and sharing of data, or the re-/use of data for scientific research.

2.1.4 Processing

Processing refers to any operation carried out on personal data and is defined by Article 4(2) of the GDPR as follows:

> **"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.

This provision clarifies that the term "**processing**" encompasses both automated and non-automated activities involving personal data. This broad definition ensures that the protection afforded to data subjects is not dependent on the specific processing techniques employed. In practice, this means that all imaginable handling of personal

Funded by Horizon Europe Framework Programme of the European Union

data constitutes processing. This approach helps prevent the circumvention of data protection measures and maintains consistent safeguards for data subjects regardless of the processing methods used. **If personal data is processed using wholly or partly automated means, the GDPR automatically applies**. In other words, the GDPR covers any processing of personal data that involves the use of technologies such as computers, mobile devices, or routers, even if only partially. In this regard, the CJEU stated that operations trigger the applicability of the GDPR if they result in "*exploring the internet automatically, constantly and systematically in search of the information which is published there, the operator of a search engine 'collects' such data which it subsequently 'retrieves', 'records' and 'organises' within the framework of its indexing programmes, 'stores' on its servers and, as the case may be, 'discloses' and 'makes available' to its users in the form of lists of search results*" [33].

On the other hand**, if personal data is not processed using wholly or partly automated means, the GDPR applies only if the data is part of a manual filing system or is intended to be included in such a system.** For instance, the CJEU indicated that a filing system is *"any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis"* [34]. The applicability of the GDPR to a manual filing system is less relevant to the CYLCOMED solution, as all processing within CYLCOMED is intended to be conducted, at least partly, by automated means.

It may be noted that the definition of processing is comprehensive. Concerning CYLCOMED, an example of data processing is the collection and storage of information concerning individuals. Therefore, such operations have to be considered 'personal data processing' within the meaning of the GDPR.

While the hospitals will undoubtedly process personal data during the execution of the CYLCOMED Pilot 2, **toolbox developers are advised to assess the nature of data used by the tools carefully** and whether the toolbox operations qualify as personal data processing, taking into account the personal data building blocks and the notion of processing.

2.1.5 Key Roles under the GDPR

Understanding the key roles in processing personal data is crucial in ensuring compliance with the GDPR requirements. Since multiple GDPR obligations are 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 to comply with the obligations under GDPR. In other words, the first step is to determine your role in data processing activities. Different roles are distributed over the various parties involved.

Funded by Horizon Europe Framework Programme of the European Union

2.1.5.1 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, that entity constitutes that entity as controller. In order to assess whether someone exercises decision-making power, EDPB Guidelines propose 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 [35].

The data controller is responsible for deciding the purpose and means of data processing. This means that the controller cannot solely determine the purpose of the processing; they must also make decisions about how the processing will be carried out. However, 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 [36]. In some cases, especially in complex situations where many subjects are involved in the processing, the identification of the controller might bear significant challenges. Information Commissioner's Office Guidelines on the controllers and processors provide an exemplary questionnaire list which might help determine whether the organisation is a controller or processor [37].

Consortium partners need to ask which of the partners decide:

- To collect personal data in the first place;
- The lawful basis for doing so;
- What types of personal data to collect;
- The purpose or purposes the data are to be used for;
- Which individuals to collect data about;
- Whether to disclose the data, and if so, to whom what to tell individuals about the processing;

Funded by Horizon Europe Framework Programme of the European Union

- How to respond to requests made in line with individuals' rights and
- How long to retain the data or whether to make non-routine amendments to the data.

These decisions refer to determining the purposes and means of processing personal data. If you are involved in making these decisions, it is likely that you are considered a data controller under data protection laws. Controllers are responsible for deciding why and how personal data will be processed, which involves defining the objectives of processing (purposes) and the methods used to carry out the processing (means).

2.1.5.2 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**. Therefore, when assessing the existence of joint controllers, it is necessary to examine whether the determination of purposes and means is made by more than one party. **The term "jointly" should be interpreted to mean "together with" or "not alone", considering various forms and combinations of decision-making involvement**.

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) to a more loose relationship (e.g., partially sharing purposes).[38] Moreover, the mutual relationship between joint controllers can occur at different stages and with varying 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. Hence, the evaluation of joint controllership should be conducted based on a factual analysis, considering the actual influence on the purposes and means of the processing. All existing or planned arrangements should be evaluated based on the factual circumstances surrounding the relationship between the parties involved. This includes examining the level of influence each party has over the processing activities and decision-making related to purposes and means. Joint participation in the determination of purposes and means implies that multiple entities have a decisive influence over whether and how the processing of data occurs. This means that each party involved has a substantial role in shaping the objectives and methods of the processing activities, indicating shared responsibility as joint controllers.

EDPB Guidelines 07/2020 on the concepts of controller and processor points out that the fact that one of the parties does not have access to personal data processed is insufficient to exclude joint controllership. This standpoint is also confirmed in the CJEU judgement in the case of Jehovah's Witnesses [39]. In the case of Jehovah's

Funded by Horizon Europe Framework Programme of the European Union

Witnesses, the Court of Justice of the European Union (CJEU) considered that a religious community must be regarded as a joint controller along with its members engaged in door-to-door preaching. Despite the religious community not having direct access to the personal data, its involvement and influence in organising and coordinating the preaching activities established joint controllership over the processing of personal data during these activities.

However, it is important to note that the involvement of multiple actors in the same processing does not automatically imply that they are acting as joint controllers of the processing. Not all forms of partnerships, cooperation, or collaboration result in joint controllership. Therefore, the qualification of joint controllership requires a case-by-case analysis of each processing scenario, considering the specific role of each entity involved in relation to that processing. Each situation must be evaluated individually to determine whether joint controllership applies based on each party's influence and decision-making authority over the processing activities. For instance, when two entities exchange the same data or set of data without jointly determining the purposes or means of processing, this should be considered as a transmission of data between separate controllers. In such cases, each entity independently determines its own purposes and methods of processing the shared data, indicating separate controller status rather than joint controllership.

Furthermore, GDPR Article 26(1) specifies that joint controllers must determine their respective responsibilities (tasks) for complying with obligations under the GDPR, particularly concerning the exercise of data subject rights and the duties to provide information as described in Articles 13 and 14. This determination of responsibilities should be made unless the responsibilities of the controllers are specifically determined by Union or Member State law applicable to them. This provision emphasises the need for joint controllers to establish clear arrangements for fulfilling their obligations under the GDPR, ensuring clarity and accountability in managing data subject rights and information duties. While Article 26(1) of the GDPR introduces an obligation for joint controllers to determine their respective responsibilities "*by means of an arrangement between them*", GDPR does not specify the legal form of this arrangement, giving joint controllers the flexibility to agree on the specific format and details of the arrangement that suits their needs and circumstances. Although GDPR does not stipulate a specific legal form of these arrangements, for the sake of legal certainty, the EDPB recommends that such arrangements be made in the form of a binding document such as a contract or other legally binding act under EU or Member State law to which the controllers are subject. This would provide certainty and could be used to evidence transparency and accountability. 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.

Funded by Horizon Europe Framework Programme of the European Union

2.1.5.3 Processor

Under GDPR Article 4(8), a processor is defined as “a natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller”. Similar to the definition of a controller, the definition of a processor encompasses a broad range of entities. A processor can be a natural person, legal entity, public authority, agency, or any other organisation or body. This broad definition means that there is no specific limitation on the type of entity that can act as a processor. It could be an organisation, a business entity, a government agency, or even an individual person, depending on the context and nature of the data processing activities involved. The key criterion is that the processor processes personal data on behalf of the controller and according to the controller's instructions.

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 concerning the controller and
- The processing of personal data must be made on the controller’s behalf [40].

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) [41]. Besides, the controller may decide to authorise the processor to engage one or more processors (“subprocessor(s)”) [42]. 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., the 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 [43]. Despite the fact that, in accordance with Article 5(2), the controller is responsible for ensuring compliance with GDPR principles and is obliged to demonstrate such compliance, it is essential to note that GDPR, through several norms, holds processors accountable for compliance, which is presented in Table 1 below.

Funded by Horizon Europe Framework Programme of the European Union

PROCESSOR's RESPONSIBILITIES AND OBLIGATIONS	***GDPR***
Conclude a data processing agreement (DPA) with a controller that meets all the GDPR requirements	*Art.* **28(3)**
Must ensure that persons authorised to process the personal data have committed themselves to confidentiality	*Art.* ***28(3)b***
Maintain a record of processing activities.	*Art.* ***30(2)***
Implement appropriate technical and organisational measures while processing personal data	*Art.* ***32***
Report a personal data breach	*Art.* ***33(2)***
Appoint a data protection officer (DPO)	*Art.* ***37***
Delete or return data to sponsor at the end of the contract.	*Rec.* **81**

Table 1 Processor's Responsibilities and Obligations

2.1.5.4 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 [44].

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 [45]. 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

Funded by Horizon Europe Framework Programme of the European Union

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 [46].**

Recommendation

Considering this subsection, it is essential to determine roles against the personal data processing within the CYLCOMED Consortium, as it serves as the foundation for the distribution of compliance obligations. To properly assess the role of each entity involved, one must first identify the specific personal data processing at stake and its exact purpose.

2.1.6 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 (Figure 3):**

Figure 3 Data Protection Principles

Funded by Horizon Europe Framework Programme of the European Union

2.1.6.1 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[47]. 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 [48]. 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 [49]. Therefore, according to the principle of fair processing, **the CYLCOMED must make sure that data subjects are aware of the processing conducted on their data and understand what exactly is happening to it. It should not be performed in secret and data subjects should be aware of the risks that accompany such processing.**

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 [50]. 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 [51]. Besides, detailed elaboration on how to understand the concept of transparency can be found in Article 29 Working Party Guidelines on transparency [52].

Recommendation

CYLCOMED must be developed and exploited in a manner that allows for complete transparency so that data subjects are informed of the processing activities. Data subjects should be given all necessary information before the processing of their data starts. Information should be readily available to them, but the transparency principle also requires that additional information be offered to the data subjects whenever they formulate a request for access to their own data.

Funded by Horizon Europe Framework Programme of the European Union

2.1.6.2 Purpose limitation

Purpose limitation is a fundamental principle in data protection that safeguards data subjects by ensuring personal data is collected for specified, legitimate purposes and not used for incompatible purposes. 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 [53]. This means that the purpose should be defined before processing personal data and should be 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. This principle aims to prevent the use of personal data in ways that could be unexpected, inappropriate, or objectionable to the data subject.

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))*. Compatibility should be evaluated on a case-by-case basis, considering factors such as the context, nature of the data, impact on data subjects, and safeguards implemented by the controller. This assessment ensures that any additional processing aligns with the initial purpose and respects the rights and expectations of data subjects. Evaluating compatibility requires careful consideration of the specific circumstances surrounding the processing activities to maintain transparency, fairness, and compliance with data protection regulations.

Recommendation

To ensure the purpose limitation principle is satisfied throughout the CYLCOMED solutions, it is of high importance to communicate clearly to all users the purposes for processing their personal data. This information can form part of the Privacy Notice, reducing the risk that the users' expectations will differ from the expectations of the controllers. Note that Article 30 GDPR obliges controllers to also maintain records of processing activities under their responsibility where they need to clearly state the purpose(s) of the processing activities.

2.1.6.3 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" [54]. It can be seen that the data minimisation principle is closely linked to the principle of purpose

Funded by Horizon Europe Framework Programme of the European Union

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. This principle requires collecting and retaining only the personal data necessary for a specific purpose. From the technical side, the data minimisation principle is implemented through privacy-enhancing technologies or other measures such as pseudonymisation.

Recommendation

To align with the data minimisation principle, CYLCOMED should ensure they only process personal data that is limited and relevant to fulfil the identified purpose. Therefore, partners should identify the minimum amount of personal data needed to fulfil the processing purpose.

2.1.6.4 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. **CYLCOMED must allow for continuous checks and the rectification of inaccurate data.**

2.1.6.5 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, the GDPR requires the implementation of the appropriate technical and organisational measures in order to protect the rights and freedoms of the data subject. To align with the principle of storage limitation, CYLCOMED Consortium partners may consider identifying a data retention policy once they have identified the purpose(s) of data processing. The data retention policy should regulate the period of retention of personal data and the consequent action to be taken once the purposes of the processing have been fulfilled (**anonymisation or erasure** of personal data).

Funded by Horizon Europe Framework Programme of the European Union

Recommendation

CYLCOMED developers must ensure that adequate technical and organizational measures are adopted to make sure that personal data can be deleted or anonymised whenever they lose their necessity to achieve cyber security.

2.1.6.6 Integrity and Confidentiality

Integrity and confidentiality are commonly also referred to as the "**data security principle**". 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 [55]. The security and confidentiality of personal data are key to preventing any adverse effects for the individual concerned, and they include technical and organisational measures. 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. According to GDPR Article 25(1), data controllers and/or processors are mandated to establish appropriate technical and organisational measures proportional to the data processing risk.

GDPR Article 32(1) states that state of the art, the costs of implementation, and the nature, scope, context, and purpose of processing should be taken into account when assessing which technical or organisational measures should be put in place. However, the term state-of-the-art is not precisely defined in the GDPR. In its Recital 78, the GDPR provides some examples of technical and organisational measures. However, the specific meaning of state-of-the-art remains open and subject to ongoing technological advancements, as the European Data Protection Board (EDPB) acknowledges in its Guidelines on Article 25 Data Protection by Design and by Default. While the GDPR obliges the data controllers and/or processors to ground the implementation of these measures on the risk-based approach, taking into account the current technological progress, the practical implementation leaves room for different interpretations of what constitutes the state-of-the-art. State-of-the-art measures may include anonymisation**,** pseudonymisation or 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 [56].

- Anonymous and Pseudonymised Data

Pseudonymisation and anonymisation, often referred to as 'privacy-enhancing techniques,' aim to prevent or at least impede the re-identification of individuals to varying degrees. However, there is often some confusion between the notion of pseudonymisation and that of anonymisation and their application in practice. Pseudonymised data retains its status as personal data because it can still be traced

Funded by Horizon Europe Framework Programme of the European Union

back to an individual using supplementary information. On the other hand, anonymised data undergoes alterations that eliminate any possibility of identifying the individual. Due to their importance, they will be elaborated more closely.

Anonymisation of data refers to the processing of data with the goal of irreversibly preventing the identification of the individual to whom it pertains [57]. This process ensures that the data can no longer be linked back to any specific individual. The process of anonymising data involves removing all identifying elements from a dataset to permanently prevent the identification of the individual to whom the data refers. GDPR Recital 26 defines **anonymous data** as information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. Furthermore, according to the GDPR Recital 26, GDPR does not apply to data rendered anonymous in such a way that the data is no longer identifiable. The same recital further clarifies that to determine whether a natural person is identifiable, in account should be taken all the means reasonably likely to be used, such as singling out, either by the controller or by another person, to identify the natural person directly or indirectly.

To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. This means that for data to be anonymised, no element can allow, by exercising reasonable effort, to re-identify the person(s) concerned. The risk of re-identification can be assessed by taking into account the time, effort or resources needed in light of the nature of the data, the context of their use, the available re-identification technologies and related costs [58].

On the other hand, it must be clarified that anonymisation is a kind of processing of personal data. Therefore, GDPR applies to the anonymisation itself. More specifically, WP29 points out that the anonymisation process, meaning the processing of such personal data to achieve their anonymisation, is an instance of “further processing”. As such, this processing must comply with the test of compatibility in accordance with the guidelines provided by the Working Party in its Opinion 03/2013 on purpose limitation. The Working Party considers that anonymisation as an instance of further processing of personal data can be considered to be compatible with the original purposes of the processing, but only on condition that the anonymisation process is such as to reliably produce anonymised information [59]. This standpoint has been reaffirmed by the EDPB Document in response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research, where it restates that the process of anonymising personal data constitutes the processing of personal data under the GDPR, such processing must be conducted in a manner that complies with the GDPR and adheres to the principles of data protection [60].

Funded by Horizon Europe Framework Programme of the European Union

Information Commissioner's Office holds the stance that data can be considered effectively anonymised when it:

- Does not relate to an identified or identifiable individual or
- Is rendered anonymous in such a way that individuals are not (or are no longer) identifiable.[61]

Examples of anonymisation techniques provided by the WP29 are randomization and generalisation [62]. Article 29 Working Party points out that whether the anonymisation techniques are robust must be assessed case by case. Besides, It is worth noting that determining when data can be considered fully anonymised is a topic of debate in legal doctrine [63]. Moreover, in practice, making personal data anonymous has become increasingly challenging due to technological advancements.

In contrast to anonymised data, pseudonymised data still fall within the scope of the GDPR. **Pseudonymisation** plays a crucial role in GDPR as a security measure (Article 32 GDPR) in the context of data protection by design (Article 25 GDPR) and implementation of the data minimisation principle. The primary benefit of pseudonymisation is to conceal the identity of data subjects from any third party not involved in the pseudonymisation process within a specific data processing operation [64]. According to GDPR Article 4(5) GDPR, pseudonymisation is defined as "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisation measures to ensure that the personal data are not attributed to an identified or identifiable natural person". It refers to a way of processing ''personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information'' [65].

In a general sense, pseudonymisation aims to protect personal data by concealing the identity of individuals within a dataset. This is achieved by replacing one or more personal data identifiers with pseudonyms and appropriately safeguarding the link between the pseudonyms and the original identifiers [66]. Identifying elements such as name, date of birth or address are replaced by a pseudonym or an identifier and kept separately from the rest of the information relating to the individual. Such identifiers are further protected on a technical and organisational level, for instance, by allowing only a limited number of authorised persons to access the pseudonymised data [67]. Importantly, this process maintains an association between the original personal identifiers and the pseudonyms, allowing for re-identification when necessary. This method ensures that the actual identities of individuals are obscured while retaining the ability to reconnect the pseudonymised data with the original identifiers if required. There are different pseudonymisation techniques, such as data random number generator (RNG), encryption, replacement of names through ID's, codes or aliases and hashing of personal data [68]. The choice of specific technique should be based on a

Funded by Horizon Europe Framework Programme of the European Union

case-by-case analysis, considering all the desired pseudonymisation goals for the specific case (by whom the identities need to be hidden, which is the desired utility for the derived pseudonyms, etc.), as well as the ease of the implementation.

Data controllers and processors should carefully consider the implementation of pseudonymisation following a risk-based approach, taking into account the purpose and overall context of the personal data processing, as well as the utility and scalability levels they wish to achieve. A risk-based approach needs to be adopted concerning the choice of the proper pseudonymisation technique so as to properly assess and mitigate the relevant privacy threats. Indeed, simply protecting the additional data that are required for re-identification, although it is a prerequisite, does not necessarily ensure the elimination of all risks.

Recommendation

Where appropriate and applicable, controllers should look to use measures such as pseudonymisation and encryption. Given the sensitive nature of the processed data, this is of particular importance for the purposes of the CYLCOMED project. Based on an assessment of risks, the CYLCOMED design must ensure the integrity and confidentiality of the data, as well as a regular review of the security measures so that they may be updated as necessary.

2.1.6.7 Accountability principle

Art. 5(2) GDPR enshrines accountability as an overarching principle of data protection law. 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 [69]. 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, conducting data protection impact assessments, recording processing activities, implementing appropriate technical and organisational measures and ensuring data protection by design and by default, to mention just a few compliance mechanisms. These may depend on the risk of processing and the nature of the data.

2.1.7 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. According to the lawfulness principle, every controller needs to actively identify the lawful basis for processing personal data, document it, communicate and explain it in the privacy notice presented to the data subject.

Funded by Horizon Europe Framework Programme of the European Union

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. Before initiating the processing of any individual's personal data, it is essential to carefully consider the basis for processing to ensure its lawfulness. Article 6(1) GDPR provides an exhaustive list of six potential legal bases for processing personal data, as listed in Table 2:

Legal Basis	***GDPR***
Consent The data subject has given consent to the processing of his or her personal data for one or more specific purposes;	*Art. 6(1)(a)*
Contract Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;	*Art. 6(1)((b)*
Legal obligation Processing is necessary for compliance with a legal obligation to which the controller is subject;	*Art. 6(1)(c)*
Vital interests Processing is necessary in order to protect the vital interests of the data subject or of another natural person;	*Art. 6(1)(d)*
Public task Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;	*Art. 6(1)(e)*
Legitimate interests 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.	*Art. 6(1)(f)*

Table 2 Legal Bases for Processing Personal Data

Funded by Horizon Europe Framework Programme of the European Union

2.1.7.1 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.

Taking into account the scope of the CYLCOMED project design, this legal basis is not likely to be used. However, EDPB Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR provide further guidance on the matter [70].

2.1.7.2 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.

2.1.7.3 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 [71].

2.1.7.4 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

Funded by Horizon Europe Framework Programme of the European Union

individual processing, but either the EU or Member State law should determine the purpose of processing [72].

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).

2.1.7.5 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 [73] 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 specific context of the CYLCOMED project, it is worth noting that legitimate interest can serve as a valid legal ground for processing personal data. The GDPR Recital 49 offers a concrete example of this: preventing unauthorised access to electronic communications networks and malicious code distribution, halting ‘denial of service’ attacks, and repairing damaged computer and electronic communication systems. This example illustrates how legitimate interest can be applied in real-world scenarios, providing a practical understanding of its use.

Before any processing activity, if this legal basis is to be used, **it is essential to determine that processing does not override the interests or fundamental rights and freedoms of the data subject**. However, the method of conducting such a balancing test has not been further clarified. Some guidance can be found in the Opinion mentioned above 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,

Funded by Horizon Europe Framework Programme of the European Union

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 [74] 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 public authorities cannot invoke legitimate interest as a legal basis for processing carried out in the performance of their tasks.

2.1.7.6 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 (Table 3):

Consent requirements under data protection law	
Freely given	Consent must be freely given, meaning 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 [75] 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) [76]. Therefore, controllers should provide a separate opt-in for each purpose, to allow users to give specific consent for specific purposes [77].

Funded by Horizon Europe Framework Programme of the European Union

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 [78]. 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 a means of giving consent bears some difficulties for the controller in proving that all conditions for valid explicit consent were met [79]. On the other hand, silence, pre-ticked boxes or inactivity are not deemed acceptable.
Explicit	In certain situations where serious data protection risk emerge, for the processing of special categories of data (including data concerning health) consent must be provided explicitly. The term explicit refers to the way consent is expressed by the data subject. It means that the data subject must give an express statement of consent. An obvious way to make sure consent is explicit would be to expressly confirm consent in a written statement.

Table 3 Consent Requirements

Furthermore, 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.

2.1.8 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

Funded by Horizon Europe Framework Programme of the European Union

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. This variability in application across Member States may mean that the GDPR will not be uniformly applied in the area of 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 to 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) (see Table 4):

Legal Basis for Processing Health Data	***GDPR***
The data subject has given **explicit consent** to processing those personal data for one or more specified purposes, except when Union or Member State law provides that the data subject cannot give consent.	*Art. 9(2)(a)*
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.	*Art. 9(2)(b)*
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	*Art. 9(2)(c)*

Funded by Horizon Europe Framework Programme of the European Union

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	*Art. 9(2)(g)*
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 contract with a health professional and subject to the conditions and safeguards.	*Art. 9(2)(h)*
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.	*Art. 9(2)(i)*
Processing is necessary 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.	*Art. 9(2)(j)*

Table 4 Legal Basis for Processing Health Data

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.

2.1.9 Determining Legal Basis

The literature indicates that determining the appropriate legal bases for use in the context of research can be challenging in practice. A significant source of uncertainty for the industry relates to identifying the suitable legal basis for processing data when explicit consent is not obtained and understanding which activities reasonably qualify for the exemptions provided by the GDPR [80]. EDPB Document, in response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research, provides a more comprehensive interpretation of the various provisions in the GDPR that are relevant for the processing of health-related data for scientific research purposes [81]. However, it is essential to firstly clarify the term “processing of personal data for scientific research purposes”.

Funded by Horizon Europe Framework Programme of the European Union

Although Article 4 GDPR does not entail an explicit definition of "**processing for the purpose of scientific research**", GDPR Recital 159 sheds more light on the term, and defines it as:

> "The term processing of personal data for **scientific research purposes** should be interpreted in a broad manner including for example **technological development and demonstration, fundamental research, applied research and privately funded research**. In addition, it should take into account the Union's objective under Article 179 (1) TFEU of achieving a European Research Area. Scientific research purposes should also include **studies conducted in the public interest in the area of public health [82].**"

As potential legal bases for processing personal data for scientific research purposes EDBP points out several legal grounds, which are shown in Table 5 below.

Lawful processing grounds for regular data		**Lawful processing grounds for special data**
Consent **Art. 6(1)a**	**In conjunction with**	**Explicit consent** **Art. 9(2)(a)**
Legal obligation **Art. 6(1)c**		**Necessity for reasons of substantial public interest based on Union or Member State law Art. 9(2)(g)**
Task carried out in the public interest **Art. 6(1)e**		**Necessity for reasons of public interest in the field of public health based on Union or Member State law** **Art. 9(2)(i)**
Legitimate interests **Art. 6(1)f**		**Necessity for scientific research purposes based on Union or Member State law** **Art. 9(2)(j)**

Table 5 Potential legal bases for processing personal data for scientific research purposes

Likewise, due to concerns raised regarding the processing personal data in the context of the clinical trials, EDBP has clarified the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR), focusing, inter alia, on the possible legal grounds for processing personal data. The EDBP distinguishes two main categories of processing activities. In particular, processing **operations purely related to research activities** must be distinguished from processing **operations related to the purposes of protection of health**, while setting standards of quality and safety for medicinal products by generating reliable and robust data (reliability and safety related purposes). EDBP clarifies that these two main categories of processing activities fall under different legal bases.

Funded by Horizon Europe Framework Programme of the European Union

2.1.9.1 Processing Operations Related to Reliability and Safety Purposes

The European Data Protection Board (EDPB) holds the opinion that processing operations explicitly defined by the CTR and relevant national provisions, particularly those related to reliability and safety purposes, can be considered as falling within the scope of "legal obligations to which the controller is subject" under Article 6(1)(c) of the GDPR. The EDPB provides examples of this interpretation through obligations related to safety reporting as defined in Articles 41 to 43 of the CTR, and obligations regarding the archiving of the clinical trial master file and the medical files of subjects. Similarly, the EDPB's interpretation extends to any disclosure of clinical trial data to national competent authorities during inspections, conducted in accordance with relevant national rules as specified in Article 78 of the CTR.

The corresponding appropriate condition for lawful processing of special categories of data in the context of these obligations shall be Article 9(2)(i). Hence, the processing of personal data in the context of safety reporting, inspections by national competent authorities, or the retention of clinical trial data in compliance with archiving obligations established by the CTR or relevant national laws have to be considered as necessary for complying with legal obligations applicable to the sponsor and/or investigator, and as such, appropriate legal basis for the processing personal data, as shown in Table 6.

Lawful processing grounds regular data		**Lawful processing grounds special data**
Art. 6(1)c Legal obligation	**In conjunction with**	**Art. 9(2)(i)** Necessity for reasons of public interest in the field of public health based on Union or Member State law

Table 6 Lawful legal basis for the processing operations related to reliability and safety purposes CTR

2.1.9.2 Processing Operations Purely Related to Research Activities

In the case of research activities, several legal bases might come into play. However, EDBP acknowledges that processing operations purely related to research activities in the context of a clinical trial cannot be derived from a legal obligation. According to the European Data Protection Board (EDPB), the processing of personal data is lawful and falls under one of the three legal bases, depending on the whole circumstances attached to a specific clinical trial, as shown in Table 7 below.

Funded by Horizon Europe Framework Programme of the European Union

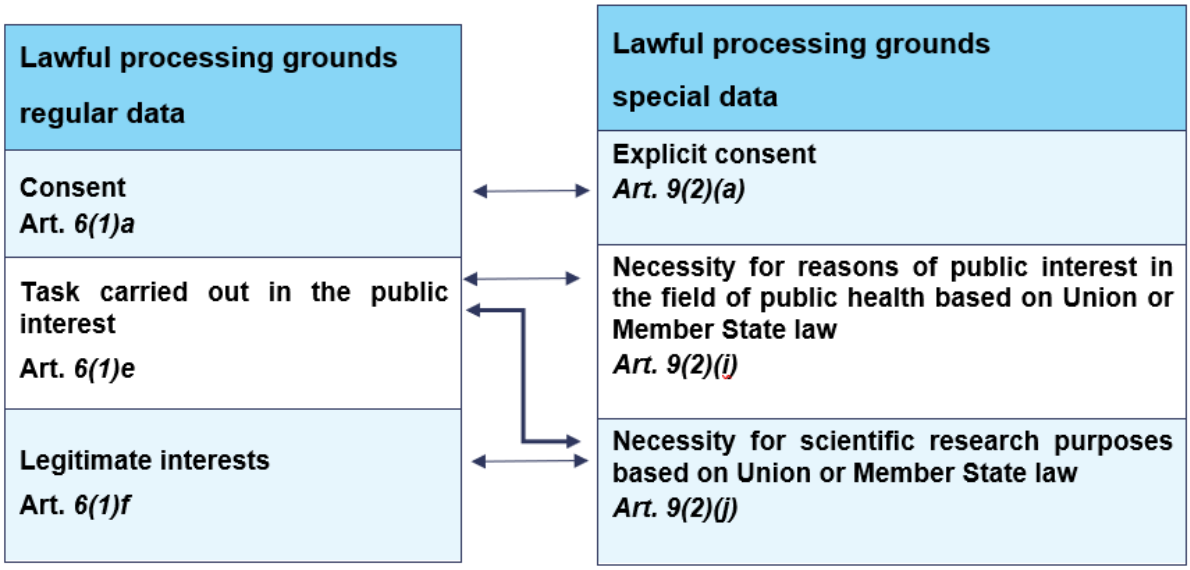

Table 7 Lawful legal basis for the processing operations related to the purposes of protection of health

It can be observed that the potential legal bases applicable to clinical trial studies also correspond to possible legal bases for research conducted in a clinical setting that is not governed by laws specifically addressing clinical trials, such as observational research. In regard to clinical trials, "Data Protection Law in Clinical Trials –Local Country Report" provides insight into Member States practices in determining legal basis in the context of the clinical trials (see Table 8) [83].

Country	What are the common data protection roles (controller or processor) typically assigned to sponsors and sites in practice with respect to the processing of personal data in the context of clinical trials?	What are the common legal bases relied upon in practice for the processing of personal health data in the context of clinical trials (e.g., informed consent or research privilege)?
Germany	Sponsors and sites are usually considered as joint controllers.	The legal basis for the processing of personal health data within clinical trials, subject to regulatory requirements, is usually Art. 9 para. 2 lit. a) GDPR (**explicit consent**).
Italy	Sponsors and sites are usually considered as joint controllers.	The legal basis for the processing of personal health data within clinical trials is usually Art. 9 para. 2 lit. a) GDPR (**explicit consent**).

Funded by Horizon Europe Framework Programme of the European Union

Spain	Sponsors and sites are usually considered independent data controllers.	The legal basis for the processing of personal health data within clinical trials is usually Art. 9 para. 2 lit. a) GDPR (**explicit consent**).

Table 8 Adapted from the "Data Protection Law in Clinical Trials –Local Country Report". Source: "Data Protection Law in Clinical Trials –Local Country Report" [84].

Since consent is the most often used legal basis, it is crucial to provide some additional consideration regarding the consent requirement in the context of the health-related research in the context of the CYLCOMED project. As stated in section 2.1.7.6, one of the essential legal requirements for consent to serve as an appropriate legal basis is that it is "freely given." Specifically, Article 4(11) of the GDPR outlines that valid consent must be freely given, emphasising the importance of individuals' voluntary and uncoerced agreement to the processing of their personal data. The concept of "free" consent under the GDPR implies that data subjects have genuine choice and control over their data. As a general rule, the GDPR specifies that if a data subject feels compelled to consent or will face negative consequences if they do not consent, then the consent obtained will not be considered valid.

When assessing whether consent is freely given EDBP points out taking into account **imbalance of power**, which occurs in, for instance, in the employment context and in the context of processing personal data by the public authorities [85]. Recital 43 of the GDPR clearly indicates that it is unlikely for public authorities to rely on consent as a lawful basis for processing. This is because when a public authority acts as the controller, there is typically a significant imbalance of power in the relationship between the controller (the public authority) and the data subject. This imbalance can undermine the voluntary nature of consent, making it less likely that consent will be freely given.

Depending on the circumstances of the clinical research study, an imbalance of power between the sponsor/investigator and participants may occur. As a result, the European Data Protection Board (EDPB) recommends that data controllers conduct a comprehensive assessment of the circumstances of the clinical trial before relying on individuals' consent as a legal basis for processing personal data for the purposes of the research activities associated with that trial [86].

2.1.10 Informed Consent for Participation in Research and GDPR Consent

The existence of these two coexisting forms of consent and their intertwined relationship is often not completely clear or straightforward. As also acknowledged by the recent EDPS Preliminary Opinion on data protection and scientific research, "there is some (understandable) confusion regarding consent, which is a principle of both data protection and research involving human participants" [87]. Consequently, there

Funded by Horizon Europe Framework Programme of the European Union

is often confusion between informed consent, as required in clinical research, and GDPR-consent related to data protection. However, the requirement of informed consent for participation in scientific research must be distinguished from explicit consent as a possibility to legitimise the processing of personal data for scientific research purposes [88]. To clarify the distinction between the two, it is important to elaborate on the differences between informed consent for participation in any research study that involves humans and consent based on the GDPR.

Firstly, informed consent and GDPR consent have **different purposes**. **The informed consent** required by the Clinical Trials Regulation (CTR), as well as other types of studies involving humans, serves as both an ethical standard and a procedural obligation in the context of clinical trials. It is a fundamental condition that must be met for a person to participate in a clinical trial. The purpose of informed consent under the CTR is to ensure that individuals understand the nature of the trial, including potential risks and benefits, and voluntarily agree to participate based on this understanding [89]. Informed consent, in the context of CTR, is a safeguard, not a legal basis for data processing. The provisions of Chapter V of the Clinical Trials Regulation (CTR), particularly Article 28, primarily address core ethical requirements for research projects involving humans, drawing from principles outlined in the Helsinki Declaration. The obligation to obtain informed consent from participants in a clinical trial is fundamentally aimed at protecting the rights to human dignity and integrity of individuals, as articulated in Articles 1 and 3 of the Charter of Fundamental Rights of the EU. Hence, the requirement for informed consent in clinical trials and other studies involving humans is rooted in ethical principles and human rights protections rather than serving as a mechanism for data protection compliance.

On the other hand, **the purpose of GDPR-consent** is to provide a lawful basis for processing personal data under the General Data Protection Regulation (GDPR). It is not intended to inform a patient about the proposed treatment or serve as a substitute for informed consent required in clinical trials. GDPR-consent focuses on data protection principles and requires that individuals provide explicit, informed, and freely given consent for the processing of their personal data for specific purposes. This consent is necessary to ensure compliance with data protection laws and to establish a lawful ground for processing personal data. Moreover, it is one of the legal bases, and instead of consent other legal grounds specified under the Article 6(1) may constitute lawful processing.

Next, it is important to distinguish the implications of **withdrawal** informed consent and GDPR consent. Article 28(3) of the CTR states that withdrawal of the informed consent to participate in a clinical trial **shall not affect** any activities already carried out and the use of data obtained on the basis of the informed consent before that withdrawal. The EDPB clarifies that personal data may continue to be processed where there is an appropriate legal basis for such processing under GDPR. In such cases, the personal data of that person gathered before the withdrawal shall be kept for the purposes and in the conditions defined by the protocol and the legislation. For instance, in situations where a serious adverse reaction occurs to a patient during a clinical trial, the sponsor

Funded by Horizon Europe Framework Programme of the European Union

may have the right to process relevant personal data by reporting the data to national competent authorities. This processing is typically justified under the legal obligation of the controller, as outlined in Article 6(1)(c) of the GDPR, in conjunction with Article 9(2)(i) [90].

In regard to GDPR consent, EDBP states that, as a general rule, if consent is withdrawn, all data processing operations that were based on consent remain lawful in accordance with the GDPR (Article 7(3)). However, the controller shall stop the processing actions concerned and if there is no other lawful basis justifying the retention for further processing, the data should be deleted by the controller [91].

In cases where personal data are processed based on consent under the General Data Protection Regulation (GDPR) in the context of a clinical trial governed by the Clinical Trials Regulation (CTR), it is important for investigators to clarify with trial subjects the scope of their withdrawal of consent. Specifically, the investigator should determine whether the trial subject's withdrawal of consent under the CTR pertains solely to their participation in trial activities (e.g., discontinuing their involvement in the trial) or if it also includes the withdrawal of consent for the processing of their personal data [92].

Recommendation

Although it is not regulated by CTR nor by GDPR, it is advised to develop separate consent forms for participation in clinical study and for processing personal data.

The informed consent as an ethical standard will be further analysed in Chapter 4.

2.1.11 Consent of Children

The GDPR establishes additional protection mechanisms for vulnerable individuals, including specific provisions regarding the consent obtained for children's data. This is exemplified by the Recital 38, which states that:

> "Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child."

The phrase "in particular" indicates that the specific protection extends beyond marketing or profiling to encompass the broader collection of personal data concerning children [93]. Furthermore, Article 8 of GDPR states that where consent is given in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. However, the processing of data from children below 16 years should only be lawful "**if and to the extent that consent is given or authorised by the holder of parental**

Funded by Horizon Europe Framework Programme of the European Union

responsibility over the child" [94]. Regarding the age limit for valid consent, the GDPR allows flexibility. Member States can establish a lower age limit by law, but this age cannot be below 13 years old. The Article 29 Working Party further clarifies that Article 8 applies where the following two requirements are fulfilled:

- The processing is based on consent as per Article 6(1) GDPR, and
- The processing is related to the offer of information society services directly to a child.

When assessing the applicability of GDPR Article 8 in the CYLCOMED context, it is crucial to determine whether the processing is directly related to the offer of information society services to a child. This is the key factor that will guide our analysis.

2.1.11.1 Information Society Service

Article 4(25) GDPR defines 'information society service' by referring to the definition of 'service' in Article 1(1)(b) of Directive (EU) 2015/1535 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services [95]. As defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council, "**Information society service**" means **any service** normally provided for remuneration, at a distance, by electronic means and **at the individual request of a recipient of services**"**.** For the purposes of this definition:

- '**At a distance**' means that the service is provided without the parties being simultaneously present;
- '**By electronic means**' means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means;
- '**At the individual request of a recipient of services**' means that the service is provided through the transmission of data on individual request.

The definition of information society service is drafted in broad and vague terms, meaning that most online services are likely to be covered by the definition of 'information society service', including here online professional services, such as online health services [96]. According to Annex I of the Directive (EU) 2015/1535, "medical examinations or treatments at a doctor's surgery using electronic equipment where the patient is physically present" should not be considered as an "information society service" [97]. However, other medical services that meets the aforementioned conditions might fall under this definition.

Hence, understanding this definition is essential for clarifying the scope of application of the specific safeguards outlined in the GDPR for processing children's personal

Funded by Horizon Europe Framework Programme of the European Union

data, especially concerning the conditions governing a child's consent for information society services. However, it is not an easy task. Due to complexity, for instance in UK, if controllers intend to use children's personal data to offer an online service to a child, they are obliged to undertake a DPIA to establish whether processing at place will result in a high risk to the rights and freedoms of your data subjects. The Information Commissioner's Office (ICO) considers offering online services to children as one of the circumstances likely to result in such a risk [98]. While assessing the scope of this definition, the EDPB also refers to case law of the European Court of Justice. The European Court of Justice held that information society services cover contracts and other services that are concluded or transmitted on-line [99].

The use of the phrase **'offered directly to a child'** in Article 8 signifies that this provision is intended to apply selectively to certain information society services, rather than all of them. Accordingly, if a provider of an information society service clearly communicates to prospective users that the service is exclusively intended for individuals aged 18 or older, and this intent is not contradicted by other indicators (such as the site's content or marketing strategies), then the service will not be deemed as 'offered directly to a child,' and Article 8 will not be applicable in this context [100].

In circumstances where controllers are offering an Information Society Service directly to children and wish to rely upon consent as the lawful basis for processing their personal data, Article 8(2) of the GDPR obliges the controller to make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.

In practice, this would mean that:

- Only children aged 13 years and over, depending on the Member States established age limit, may lawfully provide their own consent for the processing of their personal data;
- An adult with parental responsibility must provide consent for processing if the child is under 13, and in such cases, the controller must make reasonable efforts, taking into consideration available technology, to verify that the person providing parental consent does, in fact, hold parental responsibility for the child.

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 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

Funded by Horizon Europe Framework Programme of the European Union

data in the health sector. The legal basis for using the CYLCOMED system should be established in advance. CYLCOMED developers should take into account that each processing activity might rely on a different legal basis and might be thus subject to different limitations.

2.1.12 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 delineated in Table 9.

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

Table 9 Data subject's rights

2.1.12.1 Right to be Informed

To ensure transparency of data processing, data subjects should be made aware of the fact that data relating to them is or will be collected and used. 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

Funded by Horizon Europe Framework Programme of the European Union

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) [101].

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**. In such case, controller must provide meaningful information about the logic involved. However, instead of providing a complex mathematical explanation about how algorithms or machine-learning work, the controller should consider using clear and comprehensive ways to deliver the information to the data subject;

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;

Funded by Horizon Europe Framework Programme of the European Union

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 [102]. 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) [103] including, where appropriate, **by electronic means** (e.g. “just-in-time” contextual pop-up notices, 3D touch or hover-over notices, and privacy dashboards [104]). 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 [105]. 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 [106].

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 [107]. Data controllers have an obligation to ensure that when they target children or are aware that their goods or services are predominantly used by children of a certain age group, they must communicate information in a clear and simple manner that children can easily understand. This means using language that is appropriate for the age and literacy level of the children. However, Article 29 of the Data Protection Working Party (WP29) recognises that very young children or those who are pre-literate may not understand written or non-written messages about transparency. In such cases, transparency measures may need to be directed towards parents or legal guardians who have responsibility for the child's data [108].

Recommendation

In the CYLCOMED project, individuals may directly provide their personal information to a partner in the consortium; for example, this might be the case for those who will participate in the pilots. In this situation, the required information

Funded by Horizon Europe Framework Programme of the European Union

should be provided to the data subject providing the data at the time when personal data are obtained from the data subject. On the other hand, the use of AI, robotics and connected devices may result in capturing data relating to individuals without their knowledge or intention. To ensure the effective use of the right to be informed during the project and any future use, the technology should be developed and used in a way that will enable controllers to properly inform data subjects about the processing of data relating to them.

2.1.12.2 Right of Access

GDPR Article 15 embodies the Right to access, which is specifically recognised under the EU Charter of Fundamental Rights [109]. 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 [110]. 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 [111]. 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 [112].

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 [113]. 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 [114]. 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 [115]. 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) [116].

GDPR Article12(3) sets 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

Funded by Horizon Europe Framework Programme of the European Union

allowed to reject the request for access if the request is manifestly unfounded or excessive [117] if it adversely affects the rights and freedoms of others [118] or when such restriction is stipulated by the Member States' national law [119].

Recommendation

The design of CYLCOMED technologies should allow data controllers to respond to any potential information request by data subjects who wish to exercise their right to access protected by GDPR. Data controllers should be able to keep records about the data collected and processed relating data subjects and trace back any processing activity relating to a given individual.

2.1.12.3 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 right to erasure aligns closely with the principle of accuracy in data processing. The principle of accuracy requires data controllers to take reasonable steps to ensure that personal data are accurate, complete, and kept up to date as necessary.

2.1.12.4 Right to Erasure ("Right to be Forgotten")

Following the landmark decision of the Court of Justice of the European Union (CJEU) in the case of Google Spain v Mario Costeja González [120], the right to erasure, also known as the right to be forgotten, emerged as a significant topic of discussion within the academic and policymaking communities. The right to erasure is based on the notion that individuals should have the ability to request the deletion or removal of their personal data when there is no compelling reason for its continued processing or retention. GDPR Article 17 entitles data subjects to request from data controllers the erasure of their personal data, in certain circumstances. While It imposes an obligation upon the controller to erase personal data without undue delay under the conditions set out by Article 17(1) of the GDPR, this right is not absolute and it must be balanced against the considerations listed in Article 17(2) GDPR, as presented in Table 10.

Article 17(1) GDPR	Article 17(2) GDPR
Controller must erase the personal data when:	**Unless the processing is necessary for:**
The personal data are no longer necessary for the purposes they were collected.	Exercising the right of freedom of expression and information.

Funded by Horizon Europe Framework Programme of the European Union

The data subject withdraws consent and no other legal ground for processing applies	Compliance with a legal obligation or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
The data subject objects and there are no overriding legitimate grounds	Reasons of public interest in the area of public health.
The personal data have been unlawfully processed	Archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.
The personal data have been collected in relation to the offer of information society services to a minor	The establishment, exercise or defence of legal claims.

Table 10 Right to Erasure

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. In the context of artificial intelligence, the question arises whether the request to erase the personal data used to train an algorithmic model imposes an obligation on data controller to also delete the personal data or group data (i.e. trained algorithmic model) that are inferred from such personal data. It has been noted that inferred personal data would fall under the obligation of erasure because it still qualifies personal data relating to a natural person. On the other hand, inferred group data do not trigger such obligation as ''data that are embedded in an algorithmic model are no longer personal'' [121].

2.1.12.5 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.

Funded by Horizon Europe Framework Programme of the European Union

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) [122]. 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. Additionally, If personal data has been disclosed to third parties by a data controller before the processing of that data is restricted, the data controller has an obligation to communicate the restriction to these third parties.

2.1.12.6 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.

If personal data processing is based on another legal basis, such as public interest (Article 6(1)(e)) or legitimate interests (Article 6(1)(f)) of the controller, the right to data portability do not apply. 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 [123]. 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" [124]. It is important to highlight that in the context of processing through AI-based applications, there is uncertainty about whether the right to data portability also extends to the data collected by AI when tracking the activity of the data subject or data inferred from the data provided by the data subject [125]. This means that questions arise regarding whether individuals have the right to obtain and transfer this type of AI-generated data under data portability provisions. The nature of AI-generated data, which includes information inferred from user interactions and

Funded by Horizon Europe Framework Programme of the European Union

behaviours, presents challenges in interpreting its status as personal data eligible for portability rights.

Recommendation

To accommodate the right to data portability in any case, where consent or a contract forms the basis of processing, 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.

2.1.12.7 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 [126];
- Where personal data are processed for direct marketing purposes [127];
- Where personal data are processed by automated means in the context of information society services [128];
- Where personal data are processed for scientific, historical, or statistical purposes [129];

However, the exercises of the right to object is not absolute and does not grant the data subject a general right to terminate the processing in all circumstances. 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 [130]. 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.

In case of existence of automated decision-making, including profiling, the right to object in Article 21(1) and (2) has to be explicitly brought to the attention of the data subject and presented clearly and separately from other information (Article 21(4).

Funded by Horizon Europe Framework Programme of the European Union

Controllers need to ensure that this right is prominently displayed on their website or in any relevant documentation and not hidden away within any other terms and conditions.

2.1.12.8 Right not to be Subject to Automated Decision-making

The General Data Protection Regulation (GDPR) explicitly addresses the topics of profiling and automated individual decision-making, including profiling, to safeguard individuals' rights and freedoms in the context of data processing.

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 [131]. Profiling is composed of three following elements, namely:

1. It has to be an automated form of processing;
2. It has to be carried out on personal data; and
3. The objective of the profiling must be to evaluate personal aspects about a natural person [132].

Profiling is utilised in certain medical treatments, leveraging machine learning techniques to predict patients' health outcomes or the likelihood of treatment success based on specific group characteristics or individual data. This application of profiling in healthcare is known as predictive modelling or precision medicine, and it holds significant potential for improving patient care and treatment outcomes [133].

On the other hand, the WP29 Working Party clarifies that automated decision-making, in contrast to profiling, has a different scope and may partially overlap with or result from profiling. WP29 defines solely automated decision-making as the process of making decisions exclusively through technological means, without any human involvement or intervention in the decision-making process. Additionally, WP29 points out that there are potentially three ways in which profiling may be used:

- **General profiling**;
- **Decision-making based on profiling**; and

Funded by Horizon Europe Framework Programme of the European Union

- **Solely automated decision-making, including profiling**, which produces legal effects or similarly significantly affects the data subject (Article 22[1]).

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 a **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 [134]. 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. The required safeguarding measures, include, for instance, the exercise of the right to be and safeguards, such as the right to obtain human intervention and the right to challenge the decision (addressed in Article 22(3)). Moreover, WP29 sheds more light on appropriate safeguards in light of GDPR requirements. More specifically, WP2 provides a non-exhaustive list of good practice suggestions for controllers to consider when making solely automated decisions, including profiling, as shown below.

Good practice recommendations

- Regular quality assurance checks of their systems to make sure that individuals are being treated fairly and not discriminated against, whether on the basis of special categories of personal data or otherwise;
- Algorithmic auditing – testing the algorithms used and developed by machine learning systems to prove that they are actually performing as intended, and not producing discriminatory, erroneous or unjustified results;
- For independent 'third party' auditing (where decision-making based on profiling has a high impact on individuals), provide the auditor with all necessary information about how the algorithm or machine learning system works;
- Obtaining contractual assurances for third party algorithms that auditing and testing have been carried out and the algorithm is compliant with agreed standards;

Funded by Horizon Europe Framework Programme of the European Union

- Specific measures for data minimisation to incorporate clear retention periods for profiles and for any personal data used when creating or applying the profiles;
- Using anonymisation or pseudonymisation techniques in the context of profiling;
- Ways to allow the data subject to express his or her point of view and contest the decision; and,
- A mechanism for human intervention in defined cases, for example providing a link to an appeals process at the point the automated decision is delivered to the data subject, with agreed timescales for the review and a named contact point for any queries.

Controllers are also advised to explore options such as:

- Certification mechanisms for processing operations;
- Codes of conduct for auditing processes involving machine learning;
- Ethical review boards to assess the potential harms and benefits to society of particular applications for profiling.

Recommendation

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.

2.1.13 Data Protection Officer

The General Data Protection Regulation (GDPR) indeed recognises the Data Protection Officer (DPO) as a central figure in the new data governance framework and sets out specific conditions for their appointment, position, and tasks. The role of the DPO is critical in ensuring compliance with data protection laws and promoting a culture of data privacy within organisations [135]. In some situations, the data controller must designate a data protection officer (DPO) in order to comply with the GDPR. This scenario is likely applicable to the CYLCOMED project design.

Funded by Horizon Europe Framework Programme of the European Union

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 [136]. 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" [137]. 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 activities. 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 [138].

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 [139].

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 [140].

Funded by Horizon Europe Framework Programme of the European Union

Recommendation

Since the processing activities performed through CYLCOMED fall under the specific cases defined by the GDPR Article 37(1), designation and oversight of a DPO are required. While all Hospitals have appointed DPOs, when it comes to project activities performed under the CYLCOMED, the Hospitals must allow proper and easily understandable access to the DPO.

2.1.14 Data Protection Impact Assessment

A DPIA is a process designed to describe the processing, assess the necessity and proportionality of a processing and help manage the risks to the rights and freedoms of data subjects resulting from the processing of personal data. DPIA is an important tool for accountability, as it helps controllers not only to comply with the requirements of the GDPR but also to demonstrate that appropriate measures have been taken to ensure compliance with the Regulation. More specifically, as EDPB describes it, DPIA is a process for building and demonstrating compliance [141]. The DPIA encompasses an assessment of the impact of the envisaged processing operation on the protection of personal data, taking into account the nature, scope, context, and purposes of the data processing. Such assessment must be conducted by the data controller prior to the processing and the controller shall seek the advice of the data protection officer, if appointed, when carrying out the DPIA [142].

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".

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 [143]. Moreover, in order to further

Funded by Horizon Europe Framework Programme of the European Union

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 [144].

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";
- Processing 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 [145];
- 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 [146]. It is important to note that sometimes a single criterion suffices to trigger a DPIA. If the controller believes that despite the fact that the processing meets at least two criteria, it is considered not to be "likely high risk", he has to **thoroughly document the reasons for not carrying out a DPIA.**

Additionally, besides the non-exhaustive list provided by the WP29, it is important to note that National Data Protection Authorities have elaborated on this list and have created their own list of high-risk processing activities that may include more examples. For instance, the France Data protection authority (CNIL) recommends carrying out a DPIA before filing the application for the authorisation of health research and including it in the application. If the organization does not provide the DPIA, the CNIL can request the DPIA during its examination of the application. Likewise, Spain's Code of Conduct Regulating the Processing of Personal Data (the Code), which was approved by the Data protection authority of Spain, requires the completion of a DPIA *before* the start of a clinical trial, with the option to perform a single DPIA for all of the clinical trials conducted by the clinical trial sponsor [147].

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.

Funded by Horizon Europe Framework Programme of the European Union

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 [148].

There are various data protection impact assessment methodologies and approaches developed and proposed by different actors, in particular Data Protection Supervisory Authorities, academics, and civil society organisations [149]. Some of those DPIA approaches propose a separate or integrated impact assessment analysing the fundamental rights implications of the intended data processing operations and use of technology beyond the scope of the right to data protection [150]. Also, a growing trend is having more tailored DPIA's, considering the nature of the technology and the specific context where it will be deployed [151].

Recommendation

Since CYLCOMED will engage in processing sensitive categories of data (health data) concerning vulnerable data subjects (children), as well as innovative use of technological solutions, it will thus meet more than two criteria, in which case data protection impact assessment is required. If CYLCOMED controllers consider that processing is not likely "likely to result in a high risk", despite the meeting more than two criteria, controller should justify and document the reasons for not carrying out a DPIA, and include/record the views of the data protection officer.

2.1.15 Record of Data Processing Activities

Another requirement set by the GDPR for the promotion of compliance concerns **the documentation and recording of processing activities**. Art. 30 GDPR requires that controllers and processors must maintain a record of the processing activities carried out under their responsibility and provide it to the DPA when required. Article 30(1)(2) of the GDPR provides obligatory content of the record, as presented in Table 11:

Article 30(1)	**Article 30(2)**
Controller	**Processor**
Name and contact details of the controller (and, where applicable, other controllers and DPO);	Name and contact details of the processor (controller on behalf of which the processor is acting and DPO);

Funded by Horizon Europe Framework Programme of the European Union

The purposes of the processing;	The categories of processing carried out on behalf of each controller;
A description of the categories of data subjects and of the categories of personal data;	Details of transfers to third countries, including documenting the transfer mechanism safeguards in place
The categories of recipients of personal data;	A general description of the technical and organisational security measures;
Details of transfers to third countries including documenting the transfer mechanism safeguards in place	
Retention periods for the storage of personal data	
A general description of the technical and organisational security measures.	

Table 11 Record of Data Processing Activities

Additionally, it is provided an exception not to keep records for organisations employing less than 250 persons. However, this does not apply if data controllers or processors engage in processing that is likely to result in risks to the rights of data subjects or the processing is not occasional, or it includes special categories of personal data. The WP29 emphasises that maintaining a record of processing activities is highly beneficial as it supports the analysis of implications related to existing or planned processing activities. This record facilitates a factual assessment of the risks associated with processing activities conducted by a controller or processor on individuals' rights. Furthermore, it aids in the identification and implementation of appropriate security measures to safeguard personal data, which are key components of the principle of accountability outlined in the GDPR [152].

Recommendation

- Consortium partners are mandated to maintain written records of all processing activities involving personal data conducted during the execution of the research project.
- Consortium partners are encouraged to consider utilising templates provided by national Data Protection Authorities (DPAs) to assist in meeting documentation requirements under the GDPR.

Funded by Horizon Europe Framework Programme of the European Union

2.1.16 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 [153]. In situations involving a personal data breach, data controllers and processors are obligated to fulfil certain responsibilities towards the supervisory authority and the affected data subjects.

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” [154].

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 [155].

Recommendation

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. In order to comply with such

Funded by Horizon Europe Framework Programme of the European Union

requirement, Consortium partners may wish to ensure to have robust breach detection, investigation and internal reporting policies and procedures in place, also in order to facilitate decision-making about notification and communication to the relevant supervisory authority and the affected individuals. Also, in case a data breach will occur, controllers have to keep a record of it, regardless of whether the requirement of notification exists.

2.2 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 [156]. The EHDS builds upon and complements 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 [157].

The EHDS proposal is a comprehensive legal document that addresses the issue of electronic health data in detail. As of now, the proposal is structured into eight chapters. It includes an explanatory memorandum that introduces the act and provides substantiation through numerous recitals. Additionally, the proposal contains annexes that specify technical requirements and items for patient summaries. The EHDS's general objective is to ensure that natural persons in the EU have increased access to and control of their (electronic) health data across the EU while at the same time providing a legal framework allowing researchers, innovators, policymakers and regulators to access relevant electronic health data [158]. In other words, the overarching goal of the European Health Data Space proposal is to enable and promote both the primary and secondary use of electronic health record data. To attain objectives, the proposal establishes a set of rules and infrastructures to support the primary and secondary use of health data, as well as a European governance framework.

2.2.1 Scope and Application

The EHDS proposal builds on the notion of electronic health data. It applies, amongst other things, to manufacturers and suppliers of electronic health record systems and wellness applications placed on the market and put into service [159]. Electronic health data is in the current proposal defined as "personal and non-personal electronic health data" [160]. 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" [161].

Funded by Horizon Europe Framework Programme of the European Union

Generally speaking, this framework establishes provisions for placing electronic health records systems on the market, making them available on the market, or putting them into service. The framework establishes a clear distinction between primary and secondary use of electronic health data, forming the proposed framework's core pillars.

Article 2(2)(d) of the EHDS Proposal 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"

The primary use provisions emphasise electronic health data processing directly for patient care and healthcare delivery purposes. This includes activities such as prescribing, dispensing, and providing medicinal products and medical devices, as well as facilitating relevant social security, administrative, or reimbursement services. Regarding primary use, the proposal introduces additional rights and mechanisms designed to complement the rights established in the General Data Protection Regulation (GDPR).

On the other hand, the secondary use framework enables the responsible and regulated utilisation of health data beyond direct patient care for broader societal benefits and advancements in healthcare. Secondary use involves processing electronic health data by businesses, researchers, and governments for specific purposes of public interest.

According to Article 2(2)(e) EHDS Proposal, the secondary use of electronic health data means:

"The processing of electronic health data for purposes set out in Chapter IV of this Regulation. 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."

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. Article 34 of the EHDS proposal outlines specific purposes for which electronic health data can be processed for secondary use. These purposes include public interest in areas such as public and occupational health, education or teaching activities in the health or care sector, and scientific research related to health or care sectors. The secondary use of electronic health data for general interest purposes encompasses personal and non-personal health data. However, concerning personal data, the proposal allows for using electronic health data only in pseudonymised form [162].

Funded by Horizon Europe Framework Programme of the European Union

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, existing public sector bodies, or internal services of public sector bodies [163]. 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 [164].

2.2.2 Initial Challenges

The European Health Data Space (EHDS) presents the first domain-specific "data space" within the European Union and represents a significant and transformative development in health data governance [165]. This initiative holds substantial importance and has the potential to reshape how health data is managed and utilised across the EU region [166]. Based on the current draft of the Regulation, many concerns have been raised by industry and academia. For instance, there are concerns that the European Health Data Space (EHDS) may pose risks such as undermining patient control over data, hindering the work of health professionals and researchers, and potentially eroding the public value generated through health data sharing rather than enhancing it [167].

Next, EHDS imposes significant responsibilities and administrative burdens on health professionals. While the current EHDS proposal includes obligations to share patient data (Article 33), some scholars raise concerns about potential violations of professional secrecy and confidentiality duties. This could lead to legal uncertainty and conflicts with existing EU and national legal frameworks, as well as established principles of medical ethics. The EHDS Proposal does not offer clear guidance or support on how health professionals should address these complex issues, leaving them to navigate these challenges without adequate clarity or assistance [168].

Another example is the patient's right to restrict health professionals' access to their health data – either in whole or in part [169]. This implies that patients will have control over whether and to what extent healthcare professionals can access their electronic health data. Moreover, the Proposal does not mandate that healthcare professionals be informed when they do not have access to complete information. Only in situations where processing is essential to protect the vital interests of the data subject or other individual healthcare providers or health professionals may be granted access to restricted electronic health data [170]. This EDHS norm is also translated in security requirement 3.5 of EDHS Annex II, "Essential requirements for EHR systems and products claiming interoperability with EHR systems", which mandates developers of an EHR system to include tools and mechanisms to allow natural persons to restrict health professionals' access to their personal electronic health data. Besides, it shall also include mechanisms that will enable access to personal electronic health data in

Funded by Horizon Europe Framework Programme of the European Union

emergency situations and ensure that access is strictly logged. Unsurprisingly, some authors pointed out that this situation creates tension between a patient's right to self-determination and the quality of patient care and raises challenging liability questions. More specifically, complex liability issues may arise for healthcare workers when they make decisions based on restricted information, potentially leading to unintended consequences for a patient's treatment [171].

Next, the EHDS can be expected to have complex interactions with the GDPR, MDR, IVDR, AI Act and other current or anticipated EU laws. The EHDS legislative proposal already addresses some overlaps, but the risk of unintended overlaps and incoherence is nonetheless substantial. Some studies have already acknowledged that while the EHDS legislative proposal aims to address certain overlaps, there remains a significant risk of unintended overlaps and potential incoherence among these regulatory frameworks [172]. For instance, many stakeholders presenting their views have called for clarification of the relationship between GDPR and EHDS [173]. Medical device cybersecurity is not an exception.

2.2.3 EDHS Cybersecurity Requirements and Interplay with MDR

Although EDHS is still undergoing legislative process and its content is subject to change, primarily due to the debate surrounding it, some authors argue that it might be relevant to the medical device cybersecurity legal framework because it may introduce novel cybersecurity requirements for medical devices considered EHR systems [174]. Therefore, in order to determine EDHS applicability, the main question is whether and how a medical device may qualify as an EHR system.

Firstly, it is important to distinguish between the electronic health record (EHR) and the electronic health record system (EHRS). Pursuant to the EDHS Article 2(2)(m) and Article 2(2)(n), these notions are defined as follows:

Electronic health record (EHR)
"A collection of electronic health data related to a natural person and collected in the health system, processed for healthcare purposes" [175].
Electronic health record system (EHRS)
"Any appliance or software intended by the manufacturer to be used for storing, intermediating, importing, exporting, converting, editing or viewing electronic health records" [176].

Since a medical device is defined as "any instrument, apparatus, software", it is argued that a medical device that qualifies as software meets the first part of the EHRS ", **Any** appliance or **software**". The second part of the EHRS definition requires that the software in question shall process EHR. In that regard, medical device software used in eHealth settings may access data, such as personal details, medical history or plan

Funded by Horizon Europe Framework Programme of the European Union

of care, to provide health-related recommendations, such as setting reminders or managing prescriptions for patients. Therefore, it is argued that the current version of the European Health Data Space (EHDS) proposal permits the consideration that specific medical devices may qualify as electronic health record (EHR) systems [177]. Arguments that medical devices may qualify as electronic health record (EHR) systems or vice versa may also be found elsewhere [178][179]. For instance, the European Trade Association representing the medical imaging, radiotherapy, health ICT and electromedical industries points out in its feedback to the EDHS Proposal that "the definition of EHR system should be adapted, as the proposed, very broad, definition will potentially encompass all medical devices which store, intermediate, import, export, convert, edit or view electronic health records and thus make the delineation between EHR systems, medical devices and high-risk AI systems very challenging" [180]. Similar concerns are also expressed by MedTech Europe [181].

Under the presumption that medical devices fall under the category of EHR systems, manufacturers of such medical devices must meet cybersecurity requirements laid down by the EHDS Proposal. **More specifically, manufacturers will be mandated to demonstrate compliance with essential requirements laid down in the EHDS Annex II "3. Security requirements",** as presented in Table 12**:**

3.1 An EHR system shall be designed and developed in such a way that it ensures safe and secure processing of electronic health data and that it prevents unauthorised access to such data.
3.2. An EHR system designed to be used by health professionals shall provide reliable mechanisms for the identification and authentication of health professionals, including checks on professional rights and qualifications.
3.3. An EHR system designed to be used by health professionals shall support the use of information on professional rights and qualifications as part of access control mechanisms, such as role-based access control.
3.4. An EHR system designed to enable access by health professionals or other individuals to personal electronic health data shall provide sufficient logging mechanisms that record at least the following information on every access event or group of events: (a) Identification of the health professional or other individual having accessed electronic health data; (b) Identification of the individual; (c) Categories of data accessed; (d) Time and date of access; (e) Origin(s) of data.
3.5. An EHR system shall include tools and mechanisms to allow natural persons to restrict health professionals' access to their personal electronic health data. It shall

Funded by Horizon Europe Framework Programme of the European Union

also include mechanisms that allow access to personal electronic health data in emergency situations and ensure that access is strictly logged.
3.6. An EHR system shall include tools or mechanisms to review and analyse the log data, or it shall support the connection and use of external software for the same purposes.
3.7. An EHR system designed to be used by health professionals shall support digital signatures or similar non-repudiation mechanisms.
3.8. An EHR system designed for the storage of electronic health data shall support different retention periods and access rights that take into account the origins and categories of electronic health data. 3.9. An EHR system designed to be used by natural persons shall enable their identification using any recognised electronic identification means as defined in Regulation (EU) No 910/2014, regardless of the Member State that has issued it. If the service supports other electronic identification means, they shall be of assurance levels ‘substantial’ or ‘high’.

Table 12 Essential Requirements Enlisted in the EHDS Annex II “3. Security requirements”

Article 14. of EDHS, with its heading “Interplay with legislation governing medical devices and AI systems”, explicitly addresses the above-mentioned relationship. Under the Article14(3) of the EHDS, manufacturers of medical devices that claim interoperability of those medical devices with EHR systems shall prove compliance with the essential requirements on interoperability laid down in Section 2 of Annex II of this Regulation. EHDS Recital 29 clarifies this norm, pointing out that the essential requirements on interoperability of this Regulation should only apply to the extent that the manufacturer of a medical device (or high-risk AI system) which is providing electronic health data to be processed as part of the EHR system, claims interoperability with such EHR system. In such cases, the provisions on common specifications for EHR systems should be applicable to those medical devices (and high-risk AI systems). Once manufacturers demonstrate compliance with the essential requirements, they can affix the Conformité Européenne (CE)-marking and place the systems on the market.

Regarding the relationship between the European Health Data Space (EHDS) and the Medical Device Regulation (MDR), it is notable that Article 1(3)(a) of the EHDS proposal does not explicitly mention medical device manufacturers and suppliers as subjects falling under the scope of the EHDS application. However, medical devices and the data they collect are covered by other EHDS chapters, such as chapter III that lay down rules for developing and using EHR systems and wellness applications. Due to this inconsistency, the EDPB and the EDPS, in their joint opinion, recommend adding manufacturers and suppliers of medical devices in Article 1(3)(a) of the Proposal [182].

These challenges are just some of the ongoing debates over the EDHS, and they are displayed just as examples of the practical complexities that will arise with the adoption of the EDHS. Costs of implementation, complex infrastructure, achieving

Funded by Horizon Europe Framework Programme of the European Union

interoperability, transparency concerns in terms of patient data sharing, and intellectual property rights are also topical issues being discussed in the public domain [183][184]. However, an in-depth analysis of these challenges is out of the scope of this deliverable. The proposal for the European Health Data Space (EHDS) is currently undergoing the legislative process, and it is challenging to predict the final form of the EHDS as it evolves. The proposal currently delegates several central aspects to the European Commission for further specification through delegated and implementing acts. Additionally, significant changes can be anticipated during the legislative procedure, particularly in areas involving important policy and constitutional considerations for the EU and its Member States. Therefore, the provisions of the EHDS may undergo substantial changes and will be subject to detailed analysis accordingly.

2.3 Data Act

The Data Act was published in the Official Journal of the EU on 22 December 2023, and it will become applicable on 12 September 2025 [185]. The Data Act is based on the premise that innovation is increasingly dependent on the use of industrial data, which includes data generated through machine-to-machine interaction (such as connected factory machines) and human-to-machine interaction (such as data from connected devices). This data type is essential for driving innovation in business contexts (such as algorithm training for improving operations) and public sector applications (such as using data to shape and optimise smart city initiatives). By harnessing and leveraging industrial data effectively, organisations and public authorities can unlock new opportunities for innovation and development [186].

The proposed act establishes common rules governing the sharing of data generated by the use of connected products or related services (such as the Internet of Things and industrial machines). Additionally, the Data Act introduces new rules to facilitate the transition between providers of cloud services and other data processing services. It also implements safeguards to prevent unlawful international data transfers by cloud service providers. These measures aim to enhance data portability, security, and compliance with data protection regulations, ensuring greater transparency and control for users over their data. The measures laid down in the proposed regulation will complement the Data Governance Act. While the Data Governance Act increases trust in voluntary data-sharing mechanisms, the Data Act provides legal clarity regarding the access to and use of data [187].

A key objective of the Data Act is to promote fairness in the data economy and empower users to derive value from the data they generate through connected products that they own, rent, or lease [188]. In addition to the overarching goal of empowering users to gain and exert control over their data, the Data Act (DA) pursues various other objectives, including safeguarding and promoting competition, innovation, and fairness in the digital economy. To achieve these diverse goals, the

Funded by Horizon Europe Framework Programme of the European Union

Data Act introduces provisions that target different stakeholders and address specific challenges within the digital ecosystem [189]. In essence, the Data Act achieves its objectives primarily by introducing new rights for users to access and share the data they generate through their IoT devices, which will be analysed in this section.

2.3.1 Scope of Application

The Data Act is a comprehensive and intricate piece of legislation that will have significant implications across various industries and enterprises of all sizes. It sets horizontal principles that apply to all sectors, potentially covering a broad scope of applications, including all Internet of Things (IoT) devices, business-to-consumer (B2C) and business-to-business (B2B) relationships, and both personal and non-personal data [190].

In accordance with Article 1.1. Data Act lays down harmonised rules, among other things, on:

- Making available product data and related service data to the user of the connected product or related service,
- Facilitating switching between data processing service,
- Making data available by data holders to data recipients and
- Making data available by data holders to public sector bodies or Union institutions, agencies or bodies, where there is an exceptional need, for the performance of a task carried out in the public interest.

The subjects that fall under the regulation's scope are set quite broad. Pursuant Article 1(2) Data Act applies to:

- **Manufacturers of connected products** placed on the market in the Union and providers of related services, irrespective of the place of establishment of those manufacturers and providers,
- Users in the Union of connected products or related services,
- Data holders, irrespective of their place of establishment, that make data available to data recipients in the Union,
- Data recipients in the Union to whom data are made available,
- Public sector bodies, the Commission, the European Central Bank and Union bodies that request data holders to make data available where there is an exceptional need for those data for the performance of a specific task carried out in the public interest and to the data holders that provide those data in response to such request,
- Providers of data processing services, irrespective of their place of establishment, providing such services to customers in the Union,

Funded by Horizon Europe Framework Programme of the European Union

- Participants in data spaces and vendors of applications using smart contracts and persons whose trade, business or profession involves the deployment of smart contracts for others in the context of executing an agreement.

Regarding data in scope, the Data Act differentiates between the sharing of data obtained from or generated by the use of **connected products or related services**. Furthermore, the types of products and services covered by the Data Act are broadly defined. **A connected product** is defined as "*an item that obtains, generates or collects data concerning its use or environment and that is able to communicate product data via an electronic communications service, physical connection or on-device access, and whose primary function is not the storing, processing or transmission of data on behalf of any party other than the user*" [191]. In other words, Data Act applies to all products that obtain, generate or collect, using their components, data concerning their performance, use or environment and that are able to communicate that data via a publicly available electronic communications service (often referred to as the Internet of Things). Recital 14 provides some examples of products that fall under the scope of the definition, such as vehicles, home equipment and consumer goods, **medical and health devices** or agricultural and industrial machinery.

Besides products, the Data Act applies to **related services**, which is defined by the Data Act Article 2(6) and means a "*digital service, other than an electronic communications service, including software, which is connected with the product at the time of the purchase, rent or lease in such a way that its absence would prevent the connected product from performing one or more of its functions, or which is subsequently connected to the product by the manufacturer or a third party to add to, update or adapt the functions of the connected product*". Therefore, to fall within the scope of the Data Act, 'related service data' must be directly associated with the use of the device in question. This means that the data should be generated or processed by services that are specifically linked to the functionality or operation of the connected device. Such related services involve the exchange of data between the connected product and the service provider. They should be understood to be explicitly linked to the operation of the connected product's functions, such as services that, where applicable, transmit commands to the connected product that are able to have an impact on its action or behaviour. Services that do not impact the operation of the connected product and do not involve transmitting data or commands to the connected product by the service provider should not be considered related services. Such services could include, for example, auxiliary consulting, analytics or financial services, or regular repair and maintenance [192].

The Data Act defines the key parties involved in data transactions under the Data Act. In the IoT environment, data generation is the result of the actions of at least two actors: the designer or manufacturer of a product and the user of that product [193]. The Data Act defines the key parties involved in data transactions under the Data Act. The **user**

Funded by Horizon Europe Framework Programme of the European Union

is defined as a natural or legal person who owns a connected product or to whom temporary rights to use that connected product have been contractually transferred or who receives related services (Article 2(12)). On the other hand, the Data Act Article 2(13) defines the **data holder** as "a natural or legal person that has the right or obligation, in accordance with this Regulation, applicable Union law or national legislation adopted in accordance with Union law, to use and make available data, including, where contractually agreed, product data or related service data which it has retrieved or generated during the provision of a related service".

2.3.2 Data Act Applicability to the CYLCOMED

The first question to answer is whether the CYLCOMED toolbox and medical devices used in the pilots fall within the scope of the Data Act. As mentioned above, the Data Act applies to any connected products that acquire, generate, or collect data as part of their functionality. Recital 14 refers explicitly to **medical devices** as an example of products that might fall under the Data Act scope and, thus, subject to requirements defined by Regulation. Putting the definition of the product and related service in the healthcare context, the Data Act applies to medical devices such as peacemakers, insulin pumps and wearables, to mention just a few.

If the connected products fall under the scope of the Data Act, the next step is to determine who is the subject of the compliance obligations. The rights and responsibilities under the Data Act primarily apply to users of medical devices and other health-related devices and to the holders of data generated by connected medical and health devices. However, as with determining factual roles under the GDPR, the Data Act might pose the same challenges in the healthcare ecosystem. More specifically, due to the complexity of healthcare value chains, there is a risk that the roles and responsibilities of different actors may not always be clearly defined or understood. Some scholars have already noted this challenge. For instance, medical device manufacturers may be data holders concerning a device used by a patient. Nevertheless, other situations may change the qualification of actors, depending on the case under analysis. In certain circumstances, patients are not the primary entities for renting or leasing medical devices directly for manufacturers, such as CAD systems. Healthcare organisations may also fall under the definition of users for patients' data and non-personal data processed by the medical product or service. In turn, healthcare organisations themselves may be data holders towards patients [194]. Therefore, a hospital or healthcare provider may act as a user in relation to the manufacturer of the medical device but as a data holder with regard to the patient using the medical device. Hence, roles within healthcare value chains may vary depending on specific circumstances and contexts.

An additional layer of complexity in such relations is the applicability of GDPR Rules. For instance, Recital 34 clarifies that, insofar as personal data are processed, the data holder should be a controller under the GDPR. Where users are data subjects, data

Funded by Horizon Europe Framework Programme of the European Union

holders should be obliged to provide them access to their data and make the data available to third parties of the user's choice per this Regulation. However, this Regulation does not create a legal basis under GDPR for the data holder to provide access to personal data or make it available to a third party when requested by a user who is not a data subject and should not be understood as conferring any new right on the data holder to use data generated by the use of a product or related service. This applies particularly where the manufacturer is the data holder. In other words, the Data Act distinguishes between two situations: one where the data subject is also the data user and another where the data user is not the data subject. For example, when a hospital purchases and implants a medical device in a patient, the hospital acts as a user in relation to the manufacturer. At the same time, the patient is the data subject. In these scenarios, it's crucial to note that the user (hospital) cannot access the patient's personal data without a valid legal basis under the GDPR, as they are not the data subject themselves [195].

Article 4 of the Data Act defines the right of users to access and use data generated by the use of products or related services, whereas Article 5 establishes the **right to share** data with third parties. In regards to the former, Article 4(1) sets out that **where data cannot be directly accessed** by the user from the connected product or related service, data holders **shall make readily available data**, as well as the relevant metadata necessary to interpret and use those data, **accessible to the user without undue delay**, of the same quality as is available to the data holder, easily, securely, free of charge, in a comprehensive, structured, commonly used and machine-readable format and, where relevant and technically feasible, continuously and in real-time. This shall be done based on a simple request through electronic means where technically feasible. Being applicable to non-personal data in contrast to GDPR, it is important to note that the Data Act expands the scope to the right of access.

Regarding the latter, Article 5(1) prescribes that **upon request by a user** or by a party acting on behalf of a user, the data holder shall make available readily available data, as well as the relevant metadata necessary to interpret and use those data, **to a third party without undue delay**, of the same quality as is available to the data holder, easily, securely, free of charge to the user, in a comprehensive, structured, commonly used and machine-readable format and, where relevant and technically feasible, continuously and in real-time. This right complements Article 20 GDPR, establishing a right to data portability for data subjects. However, the right to share data is much broader in scope than the GDPR portability, as it includes both personal and non-personal data. Besides, Article 5(7) of the Data Act prescribes that where the user is not a data subject, any personal data generated by the use of a product or related service shall only be made available where there is a valid legal basis under Article 6(1) of GDPR, and of Article 9 respectively if sensitive personal data are processed.

When it comes to data generated by a product or related service, it is essential to note that the right to access and share data with third parties applies to personal and non-personal data. Moreover, Recital 15 clarifies that this obligation includes data

Funded by Horizon Europe Framework Programme of the European Union

generated by the use of a product or related service, including data recorded intentionally by the user. Such data include data generated as a by-product of the user's action, such as diagnostics data, without any action by the user, such as when the product is in 'standby mode', and data recorded during periods when the product is switched off. This is justified because the data represent the digitalisation of user actions and events and should accordingly be accessible to the user [196]. However, as stated by the Recital 15, By contrast, information inferred or derived from such data, which is the outcome of additional investments into assigning values or insights from the data, in particular using proprietary, complex algorithms, including those that are a part of proprietary software, should not be considered to fall within the scope of this Regulation and consequently should not be subject to the obligation of a data holder to make it available to a user or a data recipient, unless otherwise agreed between the user and the data holder. In other words, the data sharing provisions relate only to data that has not been substantially modified, more specifically, raw data. Conversely, any derived information that is the outcome of additional investments into assigning values or insights from the data (e.g. diagnoses, tests, medical treatments, correlations between certain lifestyle factors and diseases, etc.) is excluded from the scope of the Data Act [197]. However, it is already acknowledged that the differentiation above might be challenging to implement in the medical device's context [198].

2.3.3 Obligation Stemming From the Data Act

Article 3. of the Data Act introduces an obligation to make data generated by using products or related services accessible.

More specifically, Article 3(1) prescribes the following:

"Connected products shall be designed and manufactured, and related services shall be designed and provided, in such a manner that product data and related service data, including the relevant metadata necessary to interpret and use those data, are, by default, easily, securely, free of charge, in a comprehensive, structured, commonly used and machine-readable format, and, where relevant and technically feasible, directly accessible to the user."

Hence, manufacturers and designers have to design the products to make the data easily accessible by default, and they will have to be transparent about what data will be accessible and how to access it. This requirement for technical design poses a significant burden on all IoT devices, with far-reaching implications [199].

The obligation resulting from Article 3(1) shall apply to connected products and the services related to them placed on the market after 12 September 2026. Besides, Article 3(2) and Article 3(3) lists transparency information that needs to be provided to user before concluding a contract for the purchase, rent or lease of a connected product or before concluding contract for the provision of a related service. For instance, manufacturer is obliged to provide to the user, in a clear and comprehensible

Funded by Horizon Europe Framework Programme of the European Union

manner, information regarding the type, format and estimated volume of product data which the connected product is capable of generating, whether the connected product is capable of generating data continuously and in real-time and how the user may access, retrieve or, where relevant, erase the data, including the technical means to do so, as well as their terms of use and quality of service, to mention just a few of transparency requirements.

Additionally, if processing involves significant risks to fundamental rights, implementation of the principles of data minimisation and data protection by design and by default is essential, including the implementation of technical and organisational measures to protect these rights. Although the Data Act does not specify or clarify when this will be the case, it provides some examples of measures that should be implemented. Such measures include not only pseudonymisation and encryption, but also the use of increasingly available technology that permits algorithms to be brought to the data and allows valuable insights to be derived without the transmission between parties or unnecessary copying of the raw or structured data [200].

Regarding the obligation defined by Article 3(1) of the Data Act, some stakeholders have expressed concerns that it might negatively impact medical device manufacturers and even undermine the cyber security of medical devices. For instance, the Data Act mandates medical device manufacturers falling under the scope of its application to ensure direct user access to user-generated data, which could introduce cybersecurity vulnerabilities, potentially conflicting with obligations under the MDR/IVDR. Additionally, complying with the Data Act's requirement to share data with users or authorised third parties could disrupt device functionality, necessitating design alterations not originally accounted for. Recertification may be necessary if these modifications are deemed "substantial changes" under MDR/IVDR, leading to significant costs [201].

Funded by Horizon Europe Framework Programme of the European Union

3 Cybersecurity Framework

The health sector is among the most targeted sectors when it comes to cyberattacks [202]. 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 [203]. 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 characterised by regulatory specialisation and fragmentation [204]. Consequently, regulating the cybersecurity of medical devices bears the complexities of both legal frameworks [205].

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 solutions, the EU laws establish 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), the Radio Equipment Directive (RED) and Cyber Resilience Act (CRA). This creates legal uncertainty for both manufacturers and users while adding an unnecessary burden on market operators to comply with overlapping requirements for similar types of products.

3.1 The Cybersecurity Act (CSA)

The first deliverable extensively analysed the Cybersecurity Act as part of the EU policy that governs the cybersecurity certification framework. Therefore, this section will briefly introduce the Regulation background and outline the Cybersecurity Act's key pillars and the most recent developments. In the beginning, it is important to note that, over the last decade, cybersecurity has become one of the top priorities of the European Union. In order to increase the cybersecurity of the EU, in light of the increased cybersecurity challenges, the European Parliament and the European Council approved the Cybersecurity Act, repealing Regulation (EU) 526/2013 [206]. Cybersecurity Act (CSA) entered into force in June 2019 and became directly applicable in all EU Member States. The regulation addresses two central issues: firstly, delineating the roles and responsibilities designated to ENISA, and secondly, introducing a cybersecurity certification scheme [207].

More specifically, 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 in achieving common

Funded by Horizon Europe Framework Programme of the European Union

and high-level cybersecurity. Cybersecurity Act gives ENISA a pivotal role in the EU cybersecurity domain. The tasks delegated to ENISA include, inter alia, development and implementation of Union policy and law [208], capacity-building [209], operational cooperation at the Union level [210], cybersecurity certification and standardisation [211], and awareness-raising and education [212].

For instance, 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.

3.1.1 Certification Framework

The certification scheme, as defined under Article 2(9) of the CSA, stipulates that the European cybersecurity certification scheme means a “comprehensive set of rules, technical requirements, standards and procedures that are established at Union level and that apply to the certification or conformity assessment of specific information and communication technology (ICT) products, ICT services or ICT processes”. Cybersecurity certification most often takes place at the national level. As a result, certificates issued by national certification authorities may not be universally recognised across Member States [213]. Consequently, companies operating across borders might need to secure certification from multiple Member States. To address that issue, 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 [214]. 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 [215].

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 [216]. 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.

Funded by Horizon Europe Framework Programme of the European Union

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') [217]. Each European cybersecurity certificate, as stated above, might refer to one of the assurance levels: '**basic'**, '**substantial**' or '**high**', while the EU statement of conformity might only refer to the assurance level 'basic' [218]. For achieving a Basic Assurance level, evaluation activities should include, at a minimum, a review of technical documentation or an alternative evaluation method with comparable effectiveness [219]. Additionally, in accordance with CSA Article 53, a cybersecurity certification scheme may allow for the conformity self-assessment under the sole responsibility of the manufacturer or provider of ICT products, ICT services or ICT processes. However, in such cases, conformity self-assessment shall be permitted only in relation to ICT products, ICT services and ICT processes that present a low risk corresponding to assurance level 'basic'.

For the '**substantial**' assurance level, evaluation criteria should encompass, beyond the prerequisites for the 'basic' level, the verification of the compliance of the security functionalities of the ICT product, ICT service, or ICT process with its technical documentation [220]. The highest level of assurance attainable for an IoT device is "**high**". Evaluation procedures for a product necessitating a high level of assurance should encompass all the activities outlined for the substantial level, along with penetration testing of the IoT device or software to assess its resilience against targeted and well-known attacks [221]. Certification validity is contingent upon the particular characteristics of the scheme, typically capped at a maximum duration of five years. This timeframe reflects the rapid pace of technological advancements in this sector, often necessitating revisions to the scheme within shorter intervals to prevent obsolescence [222].

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. It is important to note that **cybersecurity certification is voluntary** unless otherwise specified by EU or Member State regulations [223]. However, the European Commission is currently deliberating on whether certain types of products and services should be subject to compulsory certification [224].

It is important to note that the European Cybersecurity Scheme on Common Criteria (EUCC) drafted by the ENISA was adopted in January 2024 as the first scheme within the EU cybersecurity certification framework [225]. The new EUCC scheme, based on voluntary participation, enables ICT suppliers aiming to demonstrate assurance to undergo a standardised EU assessment process. This process certifies a range of ICT products, including technological components like chips and smart cards, as well as hardware and software. This Regulation specifies the roles, rules and obligations, as well as the structure of the European Common Criteria-based cybersecurity

Funded by Horizon Europe Framework Programme of the European Union

certification scheme (EUCC) in accordance with the European cybersecurity certification framework laid down by the CSA [226]. It proposes two levels of assurance determined by the risk level linked to the intended use of the product, service, or process, considering the likelihood and potential impact of an incident [227].

Besides, two cybersecurity certification schemes are under development: the European Certification Scheme for Cloud Services (EUCS) and The European Cybersecurity Certification Scheme for 5G networks (EU5G) [228]. Moreover, the Agency has initiated a feasibility study regarding EU cybersecurity certification requirements for AI.

One of the main ambitions of the CYLCOMED project is the development of a technical cybersecurity framework designed for healthcare services that use CMDs. Hence, if Consortium partners opt for cybersecurity certification of their technical solutions, the European Cybersecurity Scheme on Common Criteria (EUCC) might be one pathway for the cybersecurity certification of the toolbox.

3.2 The NIS 2 Directive

The NIS 2 Directive was identified by the first KUL deliverable, D2.1, as the legislation of relevance to the CYLCOMED project. This section will dive into more specific analysis and specific obligations that arise from the NIS 2 Directive and how it affects the CYLCOMED. Although NIS2 clarifies that compliance is not just a matter of implementing technical solutions and has a holistic approach, the analysis will be focused to the scope of the project and will not cover in depth the obligations that are imposed at the Member States, such as adoption of National Cybersecurity strategies, and appointment of enforcement bodies, as they were discussed in the first deliverable.

The Network and Information Security Directive (NISD) 2016/1148/EU [229] 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 [230]. 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 has demonstrated its limitations over time [231].

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 [232]. 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 [233]. Additionally, ineffective supervision, limited enforcement of the Directive and a lack of systematic information sharing among Member States are some of the identified

Funded by Horizon Europe Framework Programme of the European Union

shortcomings in the implementation of the Nis Directive [234]. Eventually, in order to address recognised weaknesses in December 2022, Directive (EU) 2016/1148 (NIS Directive) was repealed by Directive (EU) 2022/2555 on measures for a high common level of network and information security across the Union (NIS 2 Directive) [235]. The directive entered into force on January 2023. However, each EU member state has until October 2024 to integrate it into their own national laws.

3.2.1 Scope of Application

To strengthen the cybersecurity level across the Union, the NIS 2 Directive lays down the following [236]:

- 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 [237];
- 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. The NIS2 Directive extends its coverage by incorporating additional sectors deemed vital to the economy and society, alongside implementing distinct size thresholds that encompass medium and large businesses within certain sectors. Additionally, it provides more detailed guidelines for incident reporting, report content, and reporting deadlines. Furthermore, it introduces stricter penalties for non-compliance, broadens the scope of application to include new sectors, and imposes more rigorous cybersecurity requirements [238].

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 regard to their sector or the type of service they provide, their size, and 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 [239]. Article 2(1) of the aforementioned recommendation sets out

Funded by Horizon Europe Framework Programme of the European Union

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 [240], 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 [241].

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**). In essence, the NIS2 scope is covered by two annexes. The Directive applies to both public and private entities referred to in Annex I or II, as depicted in Tables 13 and 14.

Sectors of high criticality (Annex I)	
Sector	**Type of entity**
Energy	
Transport	

Funded by Horizon Europe Framework Programme of the European Union

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 [242]
	EU reference laboratories [243]
	Entities carrying out research and development activities of medicinal products [244]
	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) [245]

Table 13 Adapted for the purposes of Deliverable D2.2 from Annex I NIS 2 Directive [246]

As it can be seen, Annex I lists the sectors of high criticality, which can be either an essential or an important entity depending on the total annual revenue and size of the organisation, as presented above. On the other hand, Annex II provides the other critical sectors set out by the EU, which will only fall into the Important Entity category (Table 14).

Funded by Horizon Europe Framework Programme of the European Union

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

Table 14 Adapted for the purposes of Deliverable D2.1 from Annex II NIS 2 Directive [247]

3.2.2 Cybersecurity 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 2 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

Funded by Horizon Europe Framework Programme of the European Union

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 that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following:

- Policies on risk analysis and information system security;
- Incident handling;
- Business continuity, such as backup management disaster recovery, and crisis management;
- Supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;
- Security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;
- Policies and procedures to assess the effectiveness of cybersecurity risk-management measures;
- Basic cyber hygiene practices and cybersecurity training;
- Policies and procedures regarding the use of cryptography and, where appropriate, encryption;
- Human resources security, access control policies and asset management;
- The use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.

Hence, the scope of measures and actions defined by the NIS 2 should encompass organisational, operational, and technical facets, addressing both strategic (managerial responsibility) and operational (management responsibility) concerns. Therefore, all elements must be integrated into a unified strategic process and architecture. Figure 4 depicts the necessary steps entities must take for effective risk management across these three dimensions [248].

Funded by Horizon Europe Framework Programme of the European Union

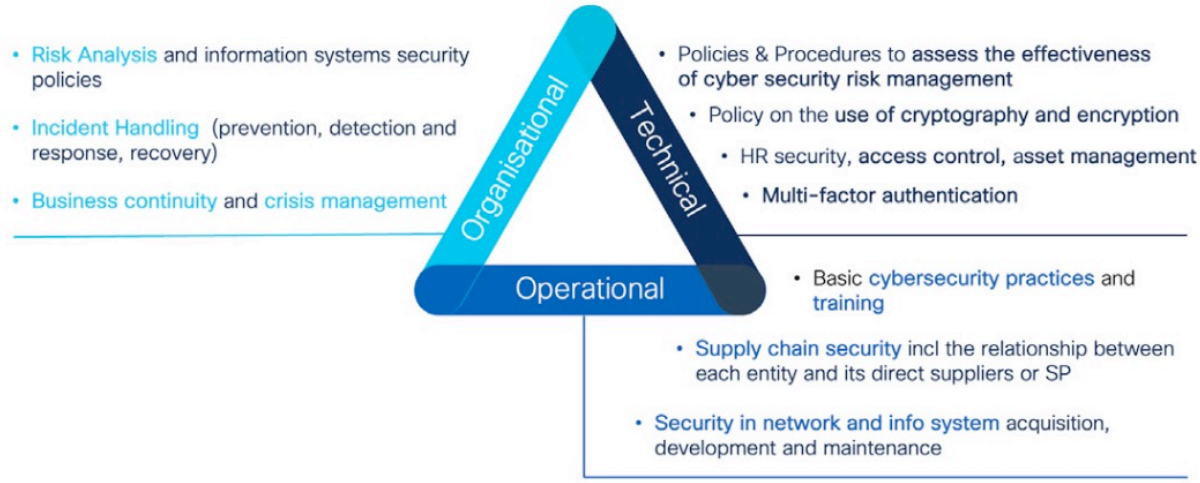

Figure 4 NIS 2 Risk Management. Source: CISCO White Paper, p17 [249].

In order to demonstrate compliance with particular requirements of Article 21, Member States may require essential and important entities to use particular ICT products, ICT services and ICT processes developed by the essential or important entity or procured from third parties, that are certified under European cybersecurity certification schemes adopted pursuant to Article 49 CSA. Moreover, The Commission is empowered to adopt delegated acts, in accordance with Article 38, to supplement this Directive by specifying which categories of essential and important entities are to be required to use certain certified ICT products, ICT services and ICT processes or obtain a certificate under a European cybersecurity certification scheme [250].

However, the specific requirements mandated by the NIS2 are still ambiguous, as the detailed requirements of the NIS2 Directive are to be released by October 2024. More specifically, Member States shall adopt and publish the measures necessary to comply with this Directive by 17 October 2024 [251].

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 [252]. 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, and 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**;

Funded by Horizon Europe Framework Programme of the European Union

- **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.

Recommendation

Given that healthcare providers and manufacturers of medical devices and in vitro medical devices are designated as "essential entities" and "important entities," the CYLCOMED consortium partners are advised to monitor the adoption of measures required to comply with cybersecurity regulations as issued by the respective Member States.

3.3 Radio Equipment Directive (RED)

The Radio Equipment Directive (RED) [253] has been mapped in the first deliverable as Regulation of relevance for the CYLCOMED toolbox technical solutions as it encompasses cybersecurity requirements that might be applicable to the CYLCOMED toolbox architecture. However, due to recent regulatory activities of EU legislator, especially in the light of the adopted Delegated Act to RED and CRA text, which will discussed below, the RED cybersecurity requirements exclude medical devices from its scope. However, although it is not applicable in regard to medical devices cybersecurity requirements it is still relevant to medical devices and toolbox development and will be briefly analysed in this section.

The RED entered into force in June 2014 and is applicable as of June 2016. The RED establishes a regulatory framework for placing radio equipment on the Single Market, 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" [254].

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. Consequently, the RED applies to medical devices if they include components such as Wi-Fi or Bluetooth modules, which means that, apart from meeting stringent MDR requirements, medical device manufacturers will need to comply with RED, conduct conformity assessment under its rules, and declare conformity with RED, in addition to the MDR. Hence, medical devices such as

Funded by Horizon Europe Framework Programme of the European Union

pacemakers or implantable cardioverter defibrillators are likely to fall under the scope of the Directive and thus be subject to its requirements [255].

On the other hand, pursuant to the RED Article 1(2), it excludes from its scope radio equipment used by radio amateurs, marine equipment airborne products, custom-built evaluation kits destined for professionals to be used solely at research and development facilities for such purposes. Additionally, it is not applicable to radio equipment exclusively used for activities concerning public security, defence, and 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 [256].

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 [257]. These requirements aim to ensure that radio equipment placed on the EU market is robust and resilient against potential cybersecurity threats. 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) [258], 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

Funded by Horizon Europe Framework Programme of the European Union

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** [259].

To address the above-mentioned issues, the Commission adopted a 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 [260]. The Delegated Regulation in its Recital 1 states that “protection of the network or its functioning from harm, protection of personal data and privacy of the user and of the subscriber and protection from fraud are elements that support protection against cybersecurity risks.” The delegated regulation complementing the RED Directive addresses the security of consumer IoT devices by imposing stringent requirements on manufacturers of internet-connected wireless and wearable radio equipment. These new requirements include incorporating safeguards to ensure the protection of personal data. Article 1(1) of the Delegated Act concerns the “network-preservation “requirement of Article 3(3)(d) RED. As clarified by recital 9 of the Delegated Act, the network security requirement shall be interpreted as broadly to cover main cybersecurity threats, such as DDOS attacks. This essential requirement "shall apply to any radio equipment that can communicate itself over the internet, whether it communicates directly or via any other equipment ('internet-connected radio equipment')" [261]. Next, a delegated act pursuant to Article 3(3)(e) of the RED requires that **internet-connected radio equipment** [262], 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) or traffic data and location data [263]. The Delegated Regulation has brought some clarity and relief to the medical device manufacturers as it excludes medical devices from its scope regarding cybersecurity requirements (Article 2(1a)).

The enforcement of the Radio Equipment Directive (RED), originally scheduled for August 2024, has been postponed and **will become applicable on 1 August 2025** due to ongoing preparations for harmonised standards [264]. It is important to note that the delegated act imposes essential requirements, formulated in general terms as objectives to be achieved, that are deemed necessary for ensuring an adequate level of cybersecurity, personal data protection and privacy. However, the delegated act does not provide concrete actions that should be taken by manufacturers to achieve compliance with defined essential requirements. However, the Commission issued on 5 August 2022 a standardisation request to the European Committee for Standardisation (CEN) and to the European Committee for Electrotechnical Standardisation CENELEC) to develop relevant harmonised standards by 30 June 2024. The manufacturers, when performing the conformity assessment procedures before placing their products on the EU market, will have the choice between two possibilities:

Funded by Horizon Europe Framework Programme of the European Union

- Perform a self-assessment, when their product has been designed in accordance with harmonised standards, after being available.
- Rely on a third-party assessment performed by an independent inspection body, regardless of whether or not a harmonised standard was used [265].

3.3.1 Interplay with the CRA

The CRA Recital 30 refers to the interplay between the RED Delegated Regulation and CRA. It clarifies that the essential requirements set out in the CRA include all the elements of the essential requirements referred to RED Delegated Regulation in Article 3(3), points (d), (e) and (f). Furthermore, the essential requirements set out in this Regulation are aligned with the objectives of the requirements for specific standards included in that standardisation request mentioned above. To ensure legal clarity and avoid overlapping issues, the RED Delegated Regulation will, therefore, be amended or repealed once the CRA enters into force. During the transition period of this Regulation, the Commission should provide guidance to manufacturers subject to this Regulation that are also subject to RED Delegated Regulation to facilitate the demonstration of compliance with the two Regulations.

3.4 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), which introduces mandatory cybersecurity requirements for products with digital elements [266]. A 2019 ENISA advisory group opinion ENISA acknowledged that connected devices for consumers often do not include the most basic security features and are therefore vulnerable to the most basic cyberattacks and misuse [267]. Impact assessment on the CRA supported ENISA's standpoint and pointed out 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 [268]. The main issues recognised by the Commission's Impact assessment are the low level of cybersecurity of products with digital elements and insufficient understanding among users as regards the cybersecurity of products. Hence, the main aim of the CRA Proposal was to ensure better protection for consumers by increasing the responsibility of manufacturers by obliging them to provide security support and software updates and providing them with information about the cybersecurity of products they buy and use.

T**he text was approved by Parliament as a whole on 12 March 2024,** and it still needs to be formally adopted by the Council before it can enter into force. Once the CRA is formally adopted and enters into force in 2024, economic operators and Member States will have 36 months to adapt to the new requirements. It is interesting

Funded by Horizon Europe Framework Programme of the European Union

to note that the adopted CRA has significantly changed in comparison to the last version of the proposal, both in terms of length and substance. This is best exemplified by the fact that the adopted text has 131 Recital in comparison to 71 Recital encompassed by the last version of the CRA. However, since the adopted CRA text will not be subject to significant changes, it will be subject to analysis in this deliverable as the CYLCOMED toolbox falls under the scope of this Regulation.

The CRA is often perceived as the last piece of the EU cybersecurity jigsaw. The EU Parliament describe the CRA as "the first-ever EU-wide legislation of its kind which seeks to bolster the cybersecurity of products with digital elements (digital products) in the European Union and to address existing regulatory cybersecurity gaps" [269]. In essence, the CRA has two primary goals for digital products, encompassing both hardware and software. Firstly, 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 manufacturers take security seriously throughout a product's life cycle. The second main objective aims to create conditions that allow users to take cybersecurity into account when selecting and using products with digital elements [270].

3.4.1 Scope of Application

The CRA is a piece of horizontal legislation that aims to harmonise cybersecurity rules for the placing on the market of products with digital elements, directly applicable to all Member States, without need to transpose the CRA into national legislative frameworks.

In accordance with Article 1, CRA lays down the following;

- Rules for the making available on the market of products with digital elements 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 those 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 time the product is expected to be in use, and obligations for economic operators in relation to those processes,
- Rules on market surveillance, including monitoring, and enforcement of the rules and requirements CRA requirements.

In Article 2(1), the CRA clarifies that Regulation applies to "products with digital elements **made available** on the market, **the intended purpose** or reasonably foreseeable use of **which** includes a direct or indirect logical or physical data connection to a device or network."

Funded by Horizon Europe Framework Programme of the European Union

The CRA Article 3(1) defines products with digital elements as

"A software or hardware product and its remote data processing solutions, including software or hardware components being placed on the market separately."

Therefore, the proposed CRA is a horizontal regulation that, with a few exceptions, covers a very wide range of digital products, such as connected devices (e.g. consumer and industrial IoT), operating systems and non-embedded software. 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.

However, it is important to note that the **CRA explicitly excludes products with digital elements governed by the MDR/IVDR from its scope of application** [271]. While this exclusion is undoubtedly welcomed by the MedTech industry, some advocate against it. For instance, the European Data Protection Supervisor (EDPS), in its opinion, recommended deleting MDR from the list of the legislations excluded from the application of the CRA Proposal, stating that "security-related provisions of some sectoral legislations excluded from the scope of the Proposal are not always as detailed and concrete as the ones in the Proposal itself" while pointing out the MDR as a particular example [272]. However, at this legislative stage, it is not likely that MDR/IVDR will be included in the scope of CRA. Manufacturers can consider it an additional guideline for the state of the art. Besides, from the scope of the CRA are excluded products with digital elements exclusively developed for national security, military purposes or specifically designed to process classified information [273].

Based on the level of the cybersecurity risk posed by the products with digital elements and cybersecurity-related functionalities, the CRA divides the digital products under its scope into two main categories. **The first category**, in accordance with Article 7 of CRA, encompasses "i**mportant products** with digital elements". More specifically, products with digital elements which have the core functionality of a product category set out in **Annex III** shall be considered to be **important products** with digital elements. The important products are further divided into two sub-categories. **Class I** lower risk (e.g. Identity management systems and privileged access management software and hardware, including authentication and access control readers, password managers and software that searches for, removes, or quarantines malicious software) and **class II higher risk** (e.g. hypervisors and container runtime systems that support virtualised execution of operating systems and firewalls, intrusion detection and prevention systems) reflecting criticality and intended use. To be considered as important products, the CRA requires meeting at least one of the following conditions [274]:

- The product with digital elements primarily performs functions critical to the cybersecurity of other products, networks or services, including securing authentication and access, intrusion prevention and detection, endpoint security or network protection;

Funded by Horizon Europe Framework Programme of the European Union

- The product with digital elements performs a function which carries a significant risk of adverse effects in terms of its intensity and ability to disrupt, control or cause damage to a large number of other products or to the health, security or safety of its users through direct manipulation, such as a central system function, including network management, configuration control, virtualisation or processing of personal data.

It is important to note that the Commission is empowered to adopt delegated acts to amend Annex III of the Regulation by including in the list a new category within each class of the categories of products with digital elements and specifying its definition, moving a category of products from one class to the other or withdrawing an existing category from that list.

The second category under the CRA is “critical products with digital elements”, listed in Annex IV of Regulation. These products are recognised by the legislator as product categories with digital elements that pose a significant risk due to their potential to disrupt, control, or cause damage to numerous other products, as well as to the health, security, or safety of users through direct manipulation. They encompass, inter alia, hardware devices with security boxes, smart meter gateways within smart metering systems and other devices for advanced security purposes, including for secure crypto processing [275]. The difference between important products and critical products with digital elements lies in the different conformity assessment procedures they must undergo.

3.4.2 CRA Impact on CYLCOMED and Corresponding Obligations

The proposed CRA assigns cybersecurity responsibilities to various economic operators based on their roles in the supply chain. Manufacturers would be tasked with ensuring that digital products meet essential cybersecurity requirements and undergo conformity assessment procedures before market placement. CRA imposes various obligations upon manufacturers, such as ensuring that digital products meet essential cybersecurity requirements, implementing vulnerability-handling procedures, and providing necessary information to users. Additionally, they would be required to maintain technical documentation and fulfil notification obligations for cybersecurity breaches. These requirements will be closely analysed below due to applicability to the CYLCOMED toolbox.

Namely, the CYLCOMED toolbox is likely to fall under the scope of the CRA and thus trigger compliance obligations by the toolbox developers. The CRA lays down conditions under which is allowed to place products with digital elements on the market. Pursuant to Article 6 products with digital elements shall be made available on the market only where:

- They meet the essential requirements set out in **Annex I**, Part I, provided that they are properly installed, maintained, used for their intended purpose or under

Funded by Horizon Europe Framework Programme of the European Union

conditions which can reasonably be foreseen, and, where applicable, the necessary security updates have been installed, and

- The processes put in place by the manufacturer comply with the essential requirements set out in Annex I, Part II.

To that end, the CRA Chapter II sets out various obligations that economic operators have to meet. When placing a product with digital elements on the market, according to Article 13, the manufacturer is obliged to ensure that the product **has been designed, developed and produced in accordance with the essential requirements set out in Annex I, Part I.** Furthermore, manufacturers shall undertake an assessment of the cybersecurity risks associated with a product with digital elements and take the outcome of that assessment into account during the planning, design, development, production, delivery and maintenance phases of the product with digital elements with a view to minimising cybersecurity risks, preventing incidents and minimising the impacts of such incidents, including in relation to the health and safety of users [276].

The CRA Annex I defines essential requirements that have to be met by the manufacturers. Essential requirements encompass **cybersecurity requirements relating to the properties** of products with digital elements (Part I) and **vulnerability handling requirements** (Part II). Significant cybersecurity requirements listed in Part I (Annex I) include, for instance, manufacturers' obligations to ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems, and report on possible unauthorised access, protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state of the art mechanisms, and by using other technical means. As regards Part II (Annex I) **vulnerability handling requirements**, after the product has been placed on the market, manufacturers would have to deploy, among other things, regular tests and reviews of their digital products' security, keep a record of vulnerabilities identified and remediate them by providing free security updates and patches. Since the functional and non-functional requirements regarding the CYLCOMED toolbox will be part of the deliverable D3.2, this deliverable will not go into detail regarding the specific cybersecurity requirements laid down by the CRA. Furthermore, manufacturers must ensure that products with digital elements are accompanied by the information and instructions outlined in Annex II, provided in either electronic or physical form, presented in a clear, understandable, intelligible, and legible language.

3.4.3 Reporting Obligations of Manufacturers

Article 14(1)(2) defines manufacturers reporting obligations, mandating manufacturers to **notify any actively exploited vulnerability** contained in the product with digital

Funded by Horizon Europe Framework Programme of the European Union

elements that it becomes aware of **simultaneously to the CSIRT designated as coordinator and to ENISA**. The manufacturer should submit:

- **An early warning notification** of an actively exploited vulnerability, without undue delay and in any event within 24 hours of the manufacturer becoming aware of it,
- **A vulnerability notification**, without undue delay and in any event within 72 hours of the manufacturer becoming aware of the actively exploited vulnerability.
- **A final report**, no later than 14 days after a corrective or mitigating measure is available, including at least the following:
- **A description of the vulnerability**, including its severity and impact;
  - Where available, information concerning any malicious actor that has exploited or that is exploiting the vulnerability;
  - Details about the security update or other corrective measures that have been made available to remedy the vulnerability.

Besides **notifying any actively exploited vulnerability** contained in the product with digital elements, pursuant to Article 14(3)(4), the manufacturer should notify **any severe incident** having an impact on the security of the product with digital elements within the same timeline as for the notifying any actively exploited vulnerability. Additionally, after becoming aware of an actively exploited vulnerability or a severe incident, the **manufacturer shall inform the impacted users** of the product with digital elements, and where appropriate, all users, about the actively exploited vulnerability or a severe incident having an impact on the security of the product with digital elements and, where necessary, about risk mitigation and any corrective measures that the users can deploy to mitigate the impact of that vulnerability or incident, where appropriate in a structured and easily automatically processible, machine-readable format [277]. Manufacturers, as well as other natural or legal persons, may notify any vulnerability contained in a product with digital elements as well as cyber threats that could affect the risk profile of a product with digital elements on a voluntary basis to a CSIRT designated as coordinator or ENISA [278]. In order to simplify the reporting obligations of manufacturers, ENISA will establish a single reporting platform.

3.4.4 Conformity Assessment and Certification

The CRA Article 32 lays down rules regarding the conformity assessment procedures for products with digital elements. Where compliance of the product with the applicable requirements has been demonstrated, manufacturers and developers would draw up an EU declaration of conformity and will be able to affix the CE marking. Manufacturers should undergo a process of conformity assessment to demonstrate whether the

Funded by Horizon Europe Framework Programme of the European Union

specified requirements relating to a product have been fulfilled. Depending on the level of risk, products with digital elements will undergo less or more rigorous conformity assessment procedures to verify compliance with the cybersecurity obligations outlined in the CRA. Such procedures range from a simple cybersecurity self-assessment to a third-party conformity assessment. The pathways to demonstrate conformity with the essential requirements in accordance with the CRA are as follows:

- The internal control procedure (based on module A) set out in Annex VIII;
- The EU-type examination procedure (based on module B) set out in Annex VIII, followed by conformity to EU-type based on internal production control (based on module C) set out in Annex VIII;
- Conformity assessment based on full quality assurance (based on module H) set out in Annex VIII; or
- Where available and applicable, a European cybersecurity certification scheme as specified in Article 27(9).

Products with digital elements considered as high-risk AI systems under the Artificial Intelligence Act must adhere to the essential requirements outlined in Annex I to the CRA. In fulfilling those requirements, they are presumed to also be compliant with the cybersecurity requirements established by the AI Act where those requirements are covered by an EU declaration of conformity issued under the CRA.

Eventually, it is important to note that non-compliance with the CRA bears high costs. Manufacturers could face significant penalties for non-compliance with security requirements outlined in Annex I, including fines of up to €15 million or 2.5% of their total annual global turnover, whichever is greater.

Funded by Horizon Europe Framework Programme of the European Union

4 Medical Device Legal Frameworks

In response to the risks and challenges posed by technological advancements in healthcare, the regulatory framework for medical devices was revised, leading to the enactment of the Medical Device Regulation (MDR) and the In Vitro Diagnostic Medical Devices Regulation (IVDR). MDR and IVDR are two key pieces of legislation that govern medical devices in the European Union (EU). These legislative acts have introduced, among other things, stringent requirements for making medical devices available on the market or putting them into service. To ensure the high level of safety and performance of medical devices that include electronic programmable systems and software considered as medical devices, the MDR and IVDR mandates demonstrating compliance with cybersecurity regulations outlined in the General Safety and Performance Requirements specified in Annex I (Article 5(2)).

At the beginning of this section, it is important to accentuate that the applicability of MDR/IVDR to the CYLCOMED toolbox will depend on the intended purpose of the tools, as it is going to be described below. On the other hand, the MDR/IVDR is fully applicable to the medical devices used in the CYLCOMED pilots (both certified and medical devices that are going to be tested at the laboratory level), which are closely elaborated in the deliverable D6.1.

4.1 Medical Devices Regulation (MDR)

The Medical Device Regulation (MDR) was adopted in April 2017, and after a staggering transitional period of four years, the MDR became fully binding in May 2021 [279]. 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 regarding medical devices, taking as a base a high level of health protection 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 [280].

In healthcare settings, numerous products used for healthcare purposes, whether medical or not, can fall into various regulatory categories based on their characteristics, mechanisms of action, intended uses, and claims. These products may be classified as medicinal products, medical devices, accessories of medical devices, food supplements, or cosmetics. Each category has specific regulatory requirements and considerations to ensure safety, efficacy, and appropriate use within the healthcare context. Understanding these distinctions is crucial for manufacturers, healthcare providers, and regulators to ensure proper classification and compliance with relevant regulations.

Funded by Horizon Europe Framework Programme of the European Union

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 [281]. Therefore, first and foremost, it is important to assess the applicability of the Medical Device Regulation on the technical solution developed under the CYLCOMED. Hence, it is important to clarify the material scope of MDR.

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 following specific medical purposes:

- 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 MDR rules apply to the accessory of a medical device. More specifically, pursuant to Article 2(2) of MDR, "Accessory for a medical device" means an article which, whilst not being itself a medical device, is intended by its manufacturer to be used together with one or several particular medical device(s) to specifically enable the medical device(s) to be used in accordance with its/their intended purpose(s) or to specifically and directly assist the medical functionality of the medical device(s) in terms of its/their intended purpose(s). Moreover, Art. 1(4) of MDR states that accessories are subjected to all provisions that apply to medical devices, including general safety and performance requirements, information supplied with the device, clinical investigations, technical documentation, and CE mark conformity assessment.

The threshold for a product to qualify as a medical device is **"Intended purpose".** According to Article 2(12) of MDR, **intended purpose** means "*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*." In other words**,** to qualify as a medical device in the first place, the technology should be a product intended by the manufacturer to be used for a medical purpose. The manufacturer's *intention remains a critical factor that determines the nature of the medical device*.

Funded by Horizon Europe Framework Programme of the European Union

In the context of the CYLCOMED Cybersecurity toolbox design and components it is important to assess the applicability of the MDR requirements. CYLCOMED technology involves various tools that mostly, but not entirely, interact with each other and perform specific functions in each of the project's pilots. CYLCOMED Cybersecurity toolbox prototype design and components first iteration has been described in the Deliverable D5.1. and will not be reiterated here. Generally speaking, tools that are going to be deployed in CYLCOMED use cases are developed as software solutions. Hence, applicability of MDR stringent requirements on the toolbox components will depend on the fact whether the software qualifies as a “medical device” or “an accessory to medical device” as defined in the MDR or IVDR. Besides, essential to the definition of a medical device is that the manufacturer must intend the device to have a medical purpose as set out in the legislation.

The use of software is very distinct when it comes to medical devices because of its lack of a physical presence. It may manifest its existence physically if it is part of a device (an accessory) or if it is necessary for it to function, and it may also be standalone and yet still be a medical device [282]. Hence, unlike other types of medical equipment, the use and design of software can be deceptive or misleading [283]. However, software must be treated and evaluated according to the same rules as for every other medical device if covered by the jurisdiction of the MDR. The Medical Device Regulation (MDR) explicitly refers to software in its Recital 19. It clarifies that software when specifically designed by the manufacturer to be used for medical purposes outlined in the definition of a medical device, qualifies as a medical device. Conversely, software intended for general purposes, even if used in a healthcare context, or software intended for lifestyle and well-being purposes, does not fall under the category of a medical device. The qualification of software, either as a device or an accessory, is independent of the software's location or the type of interconnection between the software and a device. It can be seen that the MDR establishes a clear distinction between software intended for use with or as a medical device (MD) and software designed for general purposes.

While MDR does not specifically define the medical device software, nor does it provide more clarity on this subject matter, apart from those enlisted in the General Safety and Performance Requirements set out in Annex I, Medical Device Coordination Group [284] (MDCG) Guidance sheds more light on this matter [285]. MDCG points out that:

“**Medical device software** is software that is intended to be used, alone or in combination, for a purpose as specified in the definition of a “medical device” in the medical devices regulation or in vitro diagnostic medical devices regulation, regardless of whether the software is independent or driving or influencing the use of a device”.

Therefore, in order to be qualified as medical device software, the product must first fulfil the definition of the software listed above and the definition of a medical device

Funded by Horizon Europe Framework Programme of the European Union

according to Article 2(1) of MDR. MDCG clarifies that for software to qualify as Medical Device Software (MDSW), it must have a medical purpose on its own. It is important to again emphasise that the manufacturer's intended purpose of the software is a critical factor in determining its qualification and classification as a medical device or Medical Device Software.

This is confirmed by the ruling by the Court of Justice of the European Union (CJEU), which clarified that **the manufacturer's intended purpose** remains the primary factor to consider when assessing whether a product qualifies as a medical device [286]. The Court emphasised that two specific conditions must be met for software to be considered a medical device. The first condition pertains to the objective pursued, meaning that the manufacturer must intend the software for use in humans for purposes such as diagnosis, prevention, monitoring, treatment, or alleviation of disease, as defined in the medical device definition. The Court clarified that software qualifies as a medical device when the manufacturer explicitly designates its purpose as medical. The second condition relates to the action resulting from the device's intended objective [287].

On the other hand, it is important to note that not all software used in healthcare settings is qualified as a medical device. MDCG provides some examples in which cases software does not meet the criteria to be classified as medical device software, namely:

- Software for hospital resource planning, reimbursement, management of doctors' visits,
- Software for the statistical analysis of clinical or epidemiological studies or registers,
- Electronic patient records or journal applications that simply replace paper-based health data, and
- Electronic reference works, general non-personalised medical information.

It's important to emphasise that the potential risk of harm to patients, software users, or others related to the use of software in healthcare, including the possibility of malfunction, does not determine whether the software qualifies as a medical device.

While it is not likely that CYLCOMED Cybersecurity toolbox components will fall under the MDR/IVDR scope, the toolbox developers are advised to assess such possibility against the criteria stated above. The MDCG guidance includes a "decision diagram to assist qualification of software as medical device", which might be useful in assessment.

If software qualifies as a medical device, manufacturers must ensure that all regulatory requirements for placing on the market and conformity assessment have been fulfilled. Pursuant to MDR Article 5(1), the manufacturer is obliged to ensure that the device is

Funded by Horizon Europe Framework Programme of the European Union

compliant with the MDR obligations when used in accordance with its intended purpose**.** 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.[288] 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;

Funded by Horizon Europe Framework Programme of the European Union

- Manufacturers shall set out minimum requirements concerning hardware, IT network characteristics, and IT security measures, including protection against unauthorised access;

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 [289]. Figure 5. provides an illustration of medical devices' classes, examples, requirements and risks.

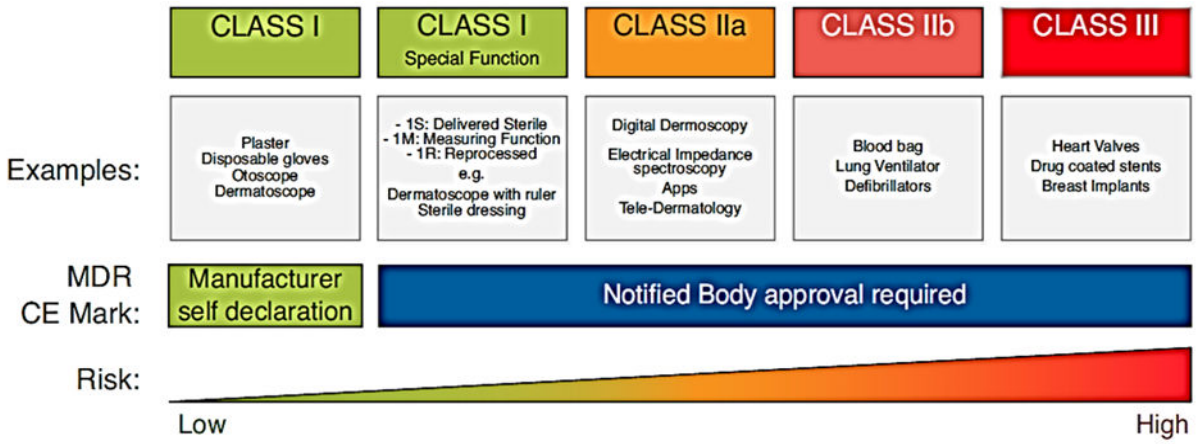

Figure 5 Medical Devices Classes. Source: New regulation of medical devices in the EU: impact in dermatology [290].

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

Funded by Horizon Europe Framework Programme of the European Union

in clinical use, and clinical evaluation that shows the product's safety and performance and that the benefits of using the device outweigh any risks.

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 [291].

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 [292] the report must be provided immediately, and not later than 2 days after the manufacturer becomes aware of that threat.

4.2 In Vitro Diagnostic Medical Devices (IVDR)

Regulation (EU) 2017/746 on in vitro diagnostic medical devices (IVDR) was adopted on April 5, 2017, and became applicable on May 26, 2022, after a transitional period of 5 years. It repealed the EU Directive 98/79/EC on in vitro diagnostic medical devices, which had been in force since 1998 [293]. As same as MDR, IVDR regulation is a legally binding legislative act that must be applied in its entirety by all EU Member States. Unlike the previously superseded EU Directive, the IVDR does not require transposition into national law before taking effect.

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 regarding 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 [294].

Funded by Horizon Europe Framework Programme of the European Union

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. Like MDR, IVDR outlines 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. 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. Although they have differences in terms of scope and focus, in the context of the cybersecurity of medical devices, they share the same requirements. Therefore, in order to avoid duplication in this deliverable, all content elaborated in the section relevant to the MDR section applies to this section.

4.3 Guidance on Cybersecurity for Medical Devices (MDCG)

It is interesting to note that neither MDR nor IVDR expressly refer to cybersecurity [295]. To assist device manufacturers in meeting the essential requirements of Annex I to the MDR/IVDR related to cybersecurity, the Medical Device Coordination Group of the European Commission in December 2019 endorsed the Guidance on Cybersecurity for Medical Devices (MDCG 2019-16 Rev.1) [296]. However, as same as the MDR/IVDR, the MDCG Guidance does not include explicit definitions nor reference to terms such as "cybersecurity," "security-by-design," and "security-by-default." Instead, the guidance outlines provisions related to cybersecurity for medical devices and emphasises conceptual connections between safety and security.

Funded by Horizon Europe Framework Programme of the European Union

However, leaving these terms theoretical and undefined may present challenges for stakeholders seeking to implement practical cybersecurity measures effectively. Clear and concrete definitions would enhance understanding and support the practical implementation of cybersecurity principles in the context of medical devices [297].

The MDCG Guidance, spanning 46 pages, addresses various topics. While its primary focus is to assist manufacturers in meeting the General and Safety Performance Requirements of the MDR/IVDR related to cybersecurity, it also offers insights and suggestions for addressing cybersecurity challenges to other stakeholders in the medical device supply chain, such as integrators and operators. 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.

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** [298]. Hence, in practice, manufacturers of medical devices are not legally bound by the Guidance and might differently approach/interpret its content. Consequently, this approach undermines the overall harmonisation approach of the MDR/IVDR. Figure 6 provides a visual summary of these requirements, which deal with both pre-market and post-market aspects.

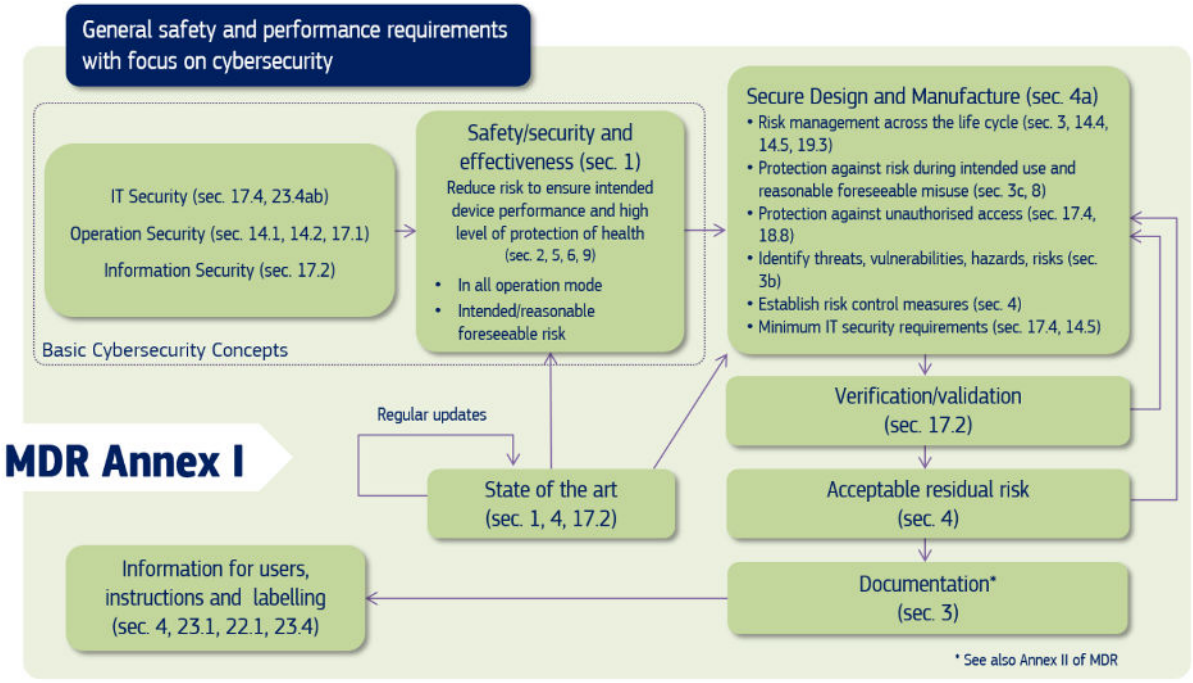

Figure 6 Cybersecurity Requirements Contained in MDR Annex I. Source: MDCG Guidance, p5 [299].

Cybersecurity requirements delineated by the MDR Annex I are encompassed by the preliminary set of technical, functional and non-functional requirements, which have been compiled as a first step contributing to the overall objective of developing the cybersecurity Toolbox and enlisted in the Deliverable D3.1. Hence, to avoid repetition,

Funded by Horizon Europe Framework Programme of the European Union

in terms of specific cybersecurity requirements, we refer the reader to Deliverable D3.1, “Baseline analysis, requirements and specifications”.

Although outdated to some extent in light of the recent EU legislative activities, Figure 7 depicts the requirements covering cybersecurity that the manufacturers should be particularly aware of, as well as its relationship with other legal frameworks. More specifically, MDCG’s Section 6 provides an overview of legislative intersection with different legal frameworks that might apply in parallel with MDR, particularly CSA, GDPR and NIS Directive. However, besides briefly touching upon the major purposes of these legal frameworks, the MDCG Guidance does not dive deeper into resolving overlapping and conflicting issues that might arise in practical implementation, nor does it establish any closer link with these acts. For instance, the MDCG Guidance briefly references the Cyber Security Act (CSA), which introduces an EU-wide cybersecurity certification framework. However, it does not establish a clear connection between the MDR and CSA, neither in terms of terminology nor substance. In regard to terminological inconsistency, the Guidance does not provide any reference to the definition of “cybersecurity”, thus missing the opportunity to establish a connection between the Guidance as the soft-law instrument and the CSA. Undoubtedly, by aligning soft-law guidance with hard-law definitions and requirements, stakeholders would benefit from clearer and more consistent guidelines for implementing cybersecurity measures in the context of medical devices and reduce ambiguity surrounding terms like "cybersecurity" [300].

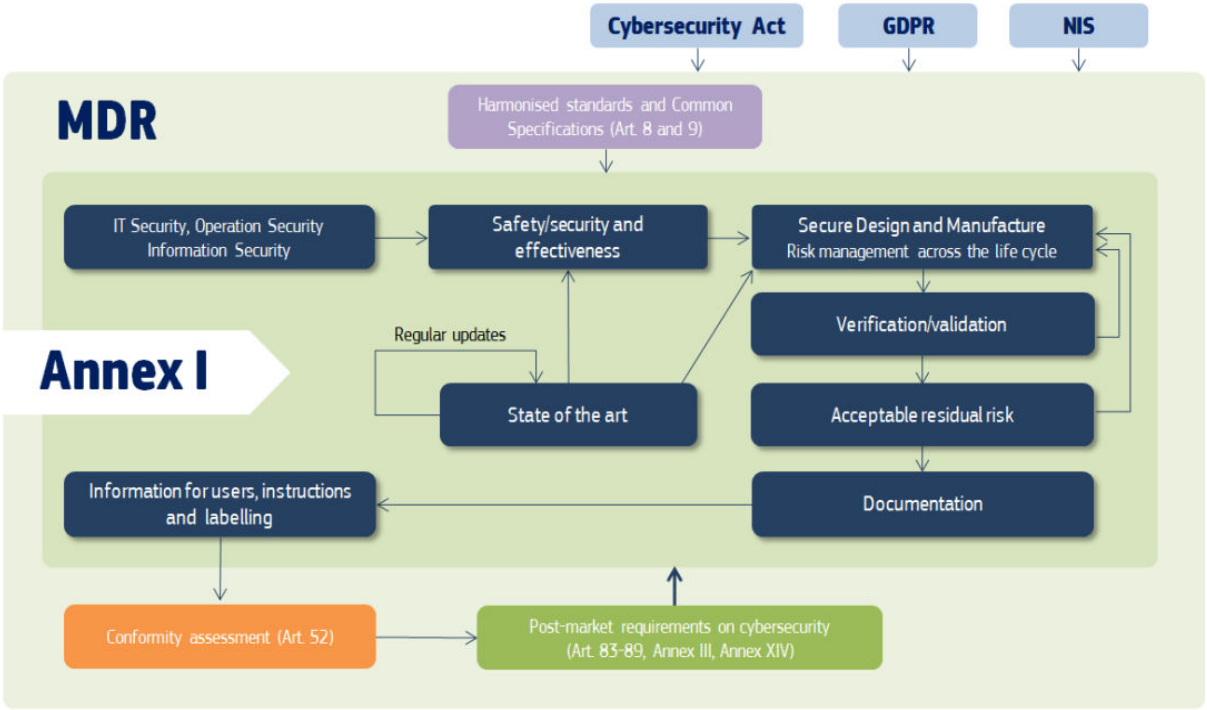

Figure 7 Cybersecurity Requirements in the MDR. Source: MDCG Guidance, p6. [301].

Furthermore, clarifying the interplay between the MDR and CSA, for instance, regarding cybersecurity certification, would be highly beneficial for stakeholders. In regard to certification, according to Article 56(2) of the CSA, cybersecurity certification is voluntary unless specifically mandated by EU or Member State regulations. If certain

Funded by Horizon Europe Framework Programme of the European Union

Member States were to require mandatory cybersecurity certification, manufacturers would need to obtain such certification for their devices to be marketed in those particular Member States. However, this requirement might not apply in other Member States, leading to inconsistencies across Member States and potential regulatory shopping. In such scenarios, manufacturers who have already obtained CE marking for their devices may be required to undergo an additional certification process, leading to duplicated requirements and increased costs [302]. This highlights potential challenges arising from differing regulatory approaches within the EU regarding cybersecurity certification for medical devices. Therefore, the MDCG Guidance could play a crucial role in providing clarity on the interplay between the Medical Device Regulation (MDR) and the Cyber Security Act (CSA). By addressing how these regulatory acts intersect and complement each other, the guidance could enhance stakeholders' understanding and facilitate compliance with both frameworks. This clarity would ultimately promote cybersecurity in the context of medical devices by helping manufacturers navigate potential requirements and certifications effectively across different Member States of the EU.

Next, MDCG Guidance does not address any connection between the MDR and Radio Equipment Directive (RED), which establishes a regulatory framework for placing radio equipment on the Single Market. All internet-connected radio equipment that is Wi-Fi, Bluetooth, LTE, 5G, or GPS enabled falls under the RED's scope. Consequently, the RED applies to medical devices if they include components such as Wi-Fi or Bluetooth modules, which means that, apart from meeting stringent MDR requirements, medical device manufacturers will need to comply with RED, conduct conformity assessment under its rules, and declare conformity with RED, in addition to the MDR. However, the MDCG Guidance does not address the applicability of the Radio Equipment Directive (RED), which is a notable omission considering its relevance. The RED should be acknowledged and included in the guidance to ensure comprehensive coverage of regulatory considerations related to medical devices incorporating radio technologies.

It is important to note that the Commission adopted a Delegated Act of the Radio Equipment Directive at the end of 2021, which aims to increase the level of cybersecurity, personal data protection and privacy for specific categories of radio equipment. The Delegated Regulation has brought some clarity and relief to the medical device manufacturers as it excludes medical devices from its scope regarding cybersecurity requirements (Article 2(1a)) [303].

While the MDCG primarily provides manufacturers with the necessary guidance on meeting the relevant General and Safety Performance Requirements of MDR with regards to cybersecurity, it also gives some hints on addressing cybersecurity challenges to other players in the medical device supply chains (e.g. Integrators and operators). For instance, Guidance states that healthcare and medical professionals are responsible for the use of medical devices for their purposes, such as diagnosing or monitoring patients. These users may access, review and exchange data with the devices and may be responsible for the patient’s education and establishing software and device parameters of usage. Furthermore, Guidance encourages patients and consumers to employ cyber smart behaviour, such as paying attention to privacy, being

Funded by Horizon Europe Framework Programme of the European Union

aware of suspicious messaging, and browsing responsibly. Eventually, 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.** However, from the space and content devoted to healthcare professionals and patients, one might say that MDCG Guidance fails to acknowledge that humans are the weakest link in the cybersecurity chain.

Additionally, MDCG Guidance does not delve into how the shared responsibilities of different stakeholders may be affected or potentially conflicted by various applicable laws to the medical device ecosystem [304]. Therefore, more guidance on this subject matter would facilitate the analysis of relevant aspects of other horizontal legislation and contribute to achieving a more coherent cybersecurity regulatory framework overall. By considering the interconnected responsibilities and legal implications across different regulatory domains, the guidance can provide more comprehensive guidance to stakeholders in navigating complex cybersecurity requirements for medical devices.

While some scholars [305] argue that "ethical issues are at the core of cybersecurity practices", it is interesting to note that MDCG Guidance does not contain any reference to ethics. 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 shapes legal solutions and plays a gap-filling function in the absence of legally binding norms. Therefore, casting more light on ethical principles and values would facilitate understanding the risks at stake and contribute to the implementation of ethical principles throughout the entire life cycle of medical devices [306].

Being the first and only guidance on medical device cybersecurity, MDCG endorsement was a significant step forward in facilitating the implementation of MDR cybersecurity requirements. However, it is important to accentuate the fact that the medical device cybersecurity landscape is a dynamic field that has undergone significant changes since the MDCG Guidance endorsement in 2019. Moreover, the regulatory landscape impacting medical device cybersecurity continues to evolve at a fast pace. For instance, It is worth noting that the NIS Directive, referred to in the Guidance, has been repealed by the NIS2 Directive. The new directive introduces various novelties and broadens the scope of its application to include medical device manufacturers. Even acknowledging this change in the Guidance would help readers understand that the Guidance is up to date [307].

Funded by Horizon Europe Framework Programme of the European Union

5 Legal and Ethical Frameworks Governing Artificial Intelligence

The CYLCOMED project will include the development and use of artificial intelligence (AI)-based systems. More specifically, the CYLCOMED toolbox encompasses two AI-based tools, namely, AI-behavioural analysis with Live Anomaly Detection System (LADS) and CMD Log monitoring with LOg Monitoring System (LOMOS) which will be deployed in CYLCOMED pilots. The detailed technical design and implementation of these tools is closely described in the deliverable D5.1. No personal data processing by these AI-based tools is envisaged. This section will provide an analysis of the relevant legal and ethical frameworks relevant to the CYLCOMED project, focusing on governance at the European Union level.

5.1 Artificial Intelligence Act (AI Act)

On March 13, 2024, the European Parliament approved the AI Act. The text provides specific rules for general-purpose AI models and high-risk AI systems, as well as some transparency obligations for certain AI systems. Even though it is not presently enforceable, it is crucial to start considering and integrating the obligations to guarantee the sustainability of the project's results.

The legislation is currently undergoing final linguistic checks before formal endorsement by the Council. The regulation will come into effect twenty days after its publication and will be applicable 24 months thereafter, potentially around mid-2026. However, it is important to emphasise that pursuant to Article 113 of the AI Act, certain provisions will come into effect earlier. AI-prohibited practices will be enforceable six months after entry into force, general-purpose AI models and governance systems will be implemented one year after entry into force, and obligations regarding high-risk AI systems will be enforced three years after entry into force.

5.1.1 Scope of Application

The proposed AI Act has a broad scope of application, both from a material and territorial perspective (Art. 2 AI Act). As for the first, the AI Act will apply to the following categories of subjects:

- Providers placing on the market or putting into service AI systems or general-purpose AI models in the Union,
- Deployers of AI systems that have their place of establishment or are located within the Union,
- Providers and deployers of AI systems that have their place of establishment or are located in a third country, where the output produced by the AI Act is used in the Union,

Funded by Horizon Europe Framework Programme of the European Union

- Importers and distributors of AI systems,
- Product manufacturers placing on the market or putting into service an AI system together with their product and under their own name or trademark,
- Authorised representatives of providers, which are not established in the Union, and
- Affected persons that are located in the Union.

Furthermore, the AI Act is not applicable to areas outside the scope of the Union law, such as military, defence, and national security (Art. 2(3) AI Act). Besides, it is important to note that the AI Act does not apply to AI systems developed and used **for the sole purpose of scientific research**. This means that research, testing and development activities regarding AI systems prior to their placement on the market or putting into service are not subject to the AI Act, provided that these activities are conducted respecting fundamental rights and other applicable EU laws (Article 2(6). However, the testing of AI systems in real-world conditions is not covered by the scientific research exemption of the AI Act. Nonetheless, it is most likely that the AI Act's obligations will still have a strong impact on CYLCOMED technologies, considering the need to anticipate placement on the market or to test in real-world conditions. Given the broad territorial scope, in combination with the fact that the providers are established in the Union and that the users are located in the Union, and that no exception applies, the project activities fall under the territorial scope of the AI Act.

Next, since the adopted AI Act underwent some changes in comparison to the previous versions in terms of definitions, it is important to introduce those for achieving terminological coherence and clarity. Firstly, Article 3(1)(1) AI Act clarifies the definition of an AI system, referring to "*a machine-based system designed to operate with varying levels of autonomy, that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments*."

Given the scope of the CYLCOMED project, it's vital to highlight certain definitions, as the AI Act allocates distinct obligations based on the roles they assume within the framework of the AI Act.

- **"Provider"** means a natural or legal person, public authority, agency or other body that develops an AI system or a general-purpose AI model or that has an AI system or a general-purpose AI model developed and places it on the market or puts the AI system into service under its own name or trademark, whether for payment or free of charge (Article 3(3) AI Act);

Funded by Horizon Europe Framework Programme of the European Union

- **"Deployer"** [308] means a natural or legal person, public authority, agency or other body using an AI system under its authority except where the AI system is used in the course of a personal non-professional activity (Article 3(4) AI Act);

5.1.2 Risk-based Approach

The AI Act adopts a risk-based approach. This means that different obligations apply depending on the risk posed by the AI system. The AI Act identifies four types of AI systems: AI systems that pose an unacceptable risk, a high risk, a limited risk, or a minimal risk [309], as illustrated by Figure 8.

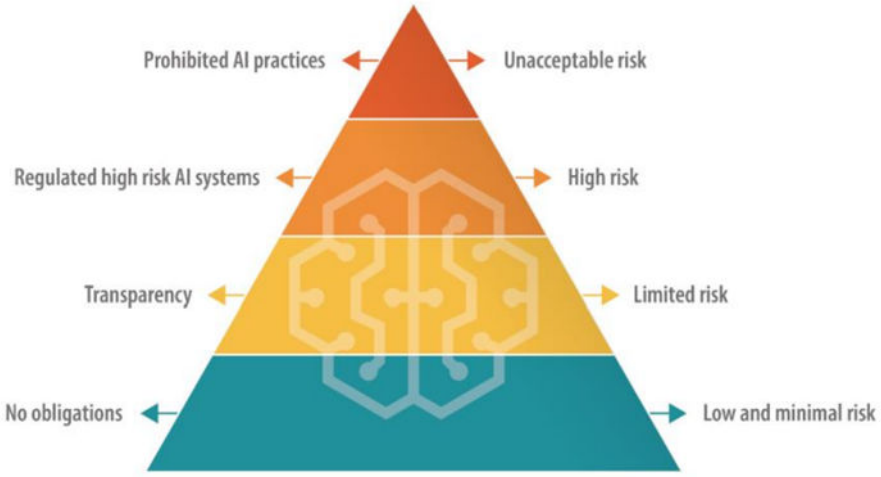

Figure 8 Risk Levels Specified Under the AI Act Proposal. Source: European Commission, 'Regulatory Framework Proposal on Artificial Intelligence' (Shaping Europe's Digital Future) [310].

5.1.2.1 CYLCOMED Tools as Prohibited Practice?

AI systems with an "**unacceptable risk**" are prohibited as they are deemed incompatible with the protection of fundamental rights (Art. 5 AI Act). Prohibited practices under Art. 5 AI Act are:

- AI systems using subliminal techniques,
- AI systems exploiting vulnerabilities of persons,
- social scoring systems,
- AI systems for risk assessments,
- AI systems for compiling facial recognition databases,
- Emotion recognition systems in workplace or education,
- Biometric categorization systems,
- Real-time remote biometric identification systems in publicly accessible spaces for law enforcement.

Funded by Horizon Europe Framework Programme of the European Union

Taking into account the architecture and intended purpose of the CYLCOMED AI tools LOMOS and LADS, which are presented in deliverables D6.1 and D5.1, it is clear that they do not fall within the scope of one of the prohibited practices listed above.

5.1.2.2 CYLCOMED Tools as High-Risk Practice?

AI systems with a "**high risk**" are subjected to mandatory requirements and ex-ante conformity assessments as they are deemed to pose a high risk to the health, safety or fundamental rights of individuals (Art. 6 AI Act and Chapter III). Hence, the first step is to determine whether the CYLCOMED AI tools fall under the scope of Article 6 of the AI Act, which lays down classification rules for high-risk AI systems. Pursuant to Article 6(1), irrespective of whether an AI system is placed on the market or put into service, the AI system shall be considered to be high-risk where both of the following conditions are fulfilled:

(a) The AI system **is intended** to be used **as a safety component of a product**, or **the AI system is itself a product**, covered by the Union harmonisation legislation listed in Annex I;
(b) The product whose safety component pursuant to point (a) 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 the putting into service of that product pursuant to the Union harmonisation legislation listed in Annex I

In regard to Article 6(1) points (a) and (b), the AI Act clearly distinguishes two situations. The first situation is in which the **AI system is itself a certain type of product.** If the AI **system is itself a certain type of product, covered** by the legislation listed in Annex I, which is required **to undergo a third-party conformity assessment,** then such an **AI system would be deemed a high-risk AI system.** Since both MDR and IVDR are covered by Annex I, this could be a situation if the AI system is intended by the manufacturer to be used, alone or in combination, for human beings for one or more of the following specific medical purposes defined by the MDR and IVDR, for which is required to undergo a third-party conformity assessment. It is not likely that CYLCOMED AI tools fall under the scope of the aforementioned situation.

In the second scenario, if a product is governed by Annex I and requires a third-party conformity assessment before it is placed on the market or put into service, then the AI system safety component associated with that product will be automatically considered to be a 'high-risk' AI system. To decipher this scenario, it is firstly important to clarify the term **'safety component'**. According to Article 3(14), a **safety component** "means *a component of a product or of a system* ***which fulfils a safety***

Funded by Horizon Europe Framework Programme of the European Union

function *for* ***that product or system, or the failure or malfunctioning of which endangers the health and safety of persons or property***." Hence, if the CYLCOMED AI tools fall under the definition of the safety component of the medical devices (product covered by Annex I), they will be considered high-risk AI systems.

Besides the aforementioned Article, relevant for the CYLCOMED project, is the second paragraph, which states that **AI systems referred to in Annex III shall be considered high-risk**. The high-risk AI systems, as referred to in Annex III, are in the area of (1) biometrics; (2) **critical infrastructure**; (3) education and vocational training; (4) employment, workers management and access to self-employment; (5) access to and enjoyment of essential private services and essential public services and benefits; (6) law enforcement; (7) migration, asylum and border control management; and (7)administration of justice and democratic processes. Hence, if the AI systems fall into the specific areas listed above, they will be deemed a high-risk AI systems.

Regarding the CYLCOMED project, the **critical infrastructure** area is the most relevant. Recital 55 of the AI Act clarifies that, as regards the management and operation of critical infrastructure, it is appropriate to classify as high-risk the AI systems intended to be used as safety components in the management and operation of critical digital infrastructure. Safety components of critical infrastructure, including critical digital infrastructure, are systems used to directly protect the physical integrity of critical infrastructure or the health and safety of persons and property, but which are not necessary in order for the system to function. Besides, it is important to note that the same recital clarifies that components intended to be used solely for cybersecurity purposes should not qualify as safety components. Examples of safety components of such critical infrastructure may include systems for monitoring water pressure or fire alarm controlling systems in cloud computing centres.

it should be mentioned that Art. 6(3) provides a derogation and stipulates that AI systems listed in Annex III are not considered high-risk if they do not pose a significant risk of harm to the health, safety or fundamental rights of natural persons, including by not materially influencing the outcome of decision making. In accordance to Article 6(3) this shall be the case where one or more of the following conditions are fulfilled:

- The AI system is intended to perform a narrow procedural task;
- The AI system is intended to improve the result of a previously completed human activity;
- The AI system is intended to detect decision-making patterns or deviations from prior decision-making patterns and is not meant to replace or influence the previously completed human assessment, without proper human review; or
- The AI system is intended to perform a preparatory task to an assessment relevant for the purposes of the use cases listed in Annex III.

Funded by Horizon Europe Framework Programme of the European Union

Finally, AI systems with **minimal or no risk** would be allowed without additional obligations. This would include, for example, spam filters in a mailbox. AI providers can decide to voluntarily conform to the requirements imposed on high-risk AI systems or issue voluntary codes of conduct. This category does not appear directly relevant for the project at hand.

5.1.3 Key Obligations for High-Risk AI Systems

AI Act imposes various obligations upon providers and deployers of high-risk AI systems. The most important obligations that providers of high-risk AI systems have to comply with are listed below:

- **Establishing and maintaining appropriate AI risk and quality management systems** (AI Act Article 9)
- **Effective data quality and governance** (AI Act Article 10)
- **Maintaining appropriate technical documentation and record-keeping** (AI Act Article 11)
- **Record-keeping events ('logs') over their lifetime** (AI Act Article 12)
- **Transparency and provision of information** (AI Act Article 13)
- **Enabling and conducting human oversight** (AI Act Article 14)
- **Compliance with standards for accuracy, robustness, and cybersecurity for the intended purpose** (AI Act Article 15)

While the providers of high-risk systems are subject to more stringent requirements, AI Act lay down specific rules targeting specifically deployers of these systems. These obligations include, inter alia, the following:

- **Take appropriate technical and organisational measures to ensure they use such systems in accordance with the instructions for use accompanying the systems (**AI Act Article 26(1)**)**
- **Implementing human oversight by people with the appropriate training and competence (**AI Act Article 26(2)**)**
- **Informing the AI system provider of any serious incidents (**AI Act Article 26(5)**)**
- **Retaining the automatically-generated system logs (**AI Act Article 26(6)**)**
- **Complying with GDPR obligations to perform a data protection impact assessment (**AI Act Article 26(9)**)**
- **Informing people, they might be subject to the use of high-risk AI (**AI Act Article 26(11)**)**

Funded by Horizon Europe Framework Programme of the European Union

- **Completing a fundamental rights impact assessment (FRIA) before putting the AI system in use, if the deployer:**
  - **Is a public body or private entity providing public services or**
  - **Provides essential private service that cover creditworthiness evaluation of persons, and risk assessment and pricing in relation to life and health insurance; (**AI Act Article 27)

5.1.4 AI Cybersecurity in the AI Act

AI cybersecurity is covered in the AI Act in Article 15, albeit not as an individual requirement, but together with accuracy and robustness. AI Act Article 15 prescribes that high-risk AI systems shall be designed and developed in such a way that they achieve an appropriate level of accuracy, robustness, and cybersecurity and that they perform consistently in those respects throughout their lifecycle. Furthermore, the technical solutions aiming to ensure the cybersecurity of high-risk AI systems shall be appropriate to the relevant circumstances and the risks. The technical solutions to address AI-specific vulnerabilities shall include, where appropriate, measures to prevent, detect, respond to, resolve and control for attacks trying to manipulate the training data set ('data poisoning') or pre-trained components used in training ('model poisoning'), inputs designed to cause the AI model to make a mistake ('adversarial examples' or 'model evasion'), confidentiality attacks or model flaws(Article 15(5)).

Next, AI Act Recital 76 points out that cybersecurity plays a crucial role in ensuring that AI systems are resilient against attempts to alter their use, behaviour, and performance or compromise their security properties by malicious third parties exploiting the system's vulnerabilities. It acknowledges that cyberattacks against AI systems can leverage AI-specific assets, such as training data sets (e.g. data poisoning) or trained models (e.g. adversarial attacks or membership inference), or exploit vulnerabilities in the AI system's digital assets or the underlying ICT infrastructure. To ensure a level of cybersecurity appropriate to the risks, suitable measures, **such as security controls**, should therefore be taken by the providers of high-risk AI systems, also taking into account as appropriate the underlying ICT infrastructure.

5.2 Ethics Guidelines for Trustworthy AI

In its Communications of 25 April 2018 and 7 December 2018 [311], the European Commission set out its vision for artificial intelligence (AI), which supports "ethical, secure and cutting-edge AI made in Europe".

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, the 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"

Funded by Horizon Europe Framework Programme of the European Union

in April 2019 as practical guidance on how developers, implementers and end-users of AI systems can comply with ethical principles [312].

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".[313] 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" [314]. 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 Figure 9.

Funded by Horizon Europe Framework Programme of the European Union

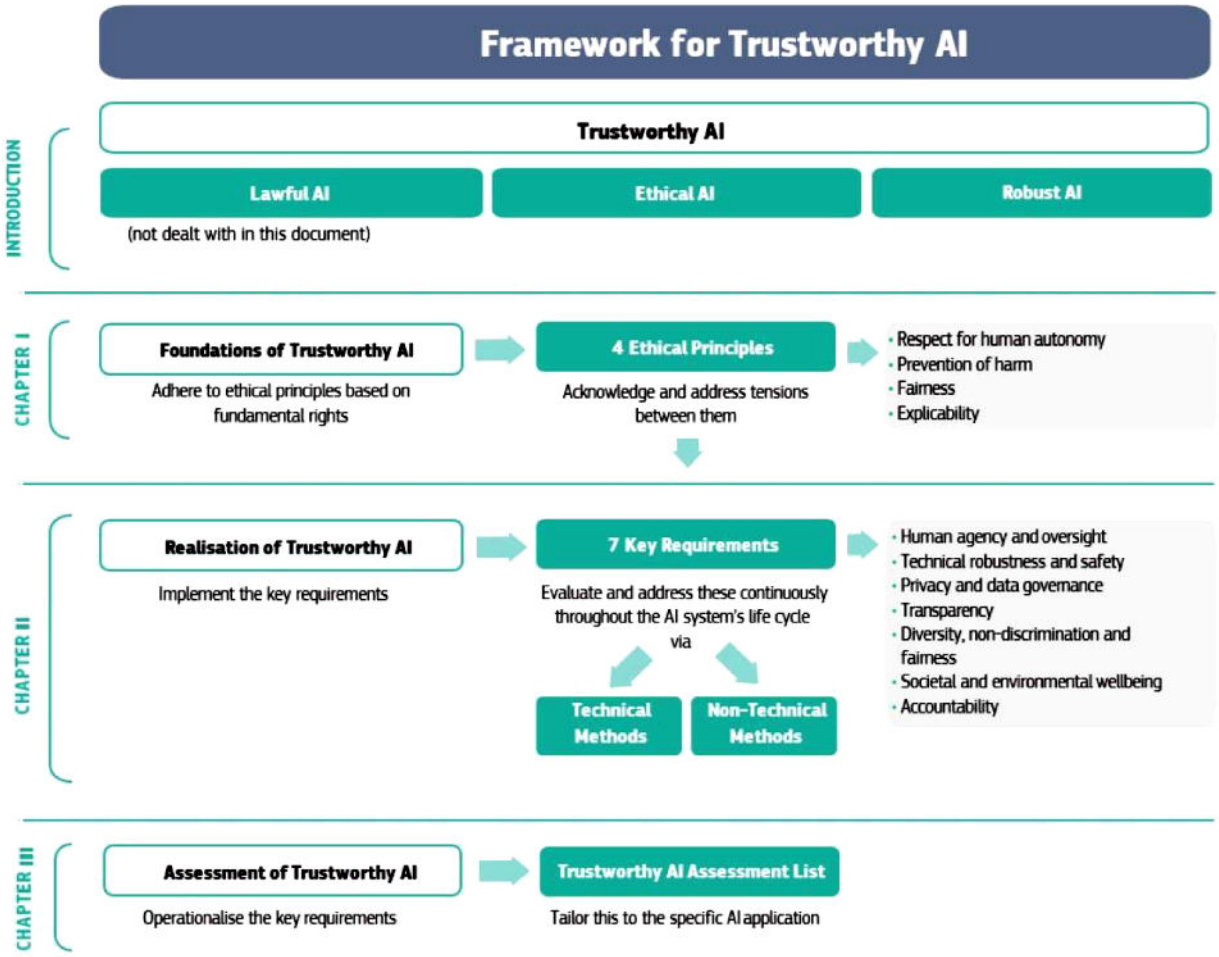

Figure 9 AI HLEG Framework for Trustworthy AI. Source: Ethics Guidelines for Trustworthy AI p.10 [315]

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,

Funded by Horizon Europe Framework Programme of the European Union

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 [316].

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 [317].

In addition, Chapter II covers technical and non-technical methods worth considering ensuring 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 10.

Funded by Horizon Europe Framework Programme of the European Union

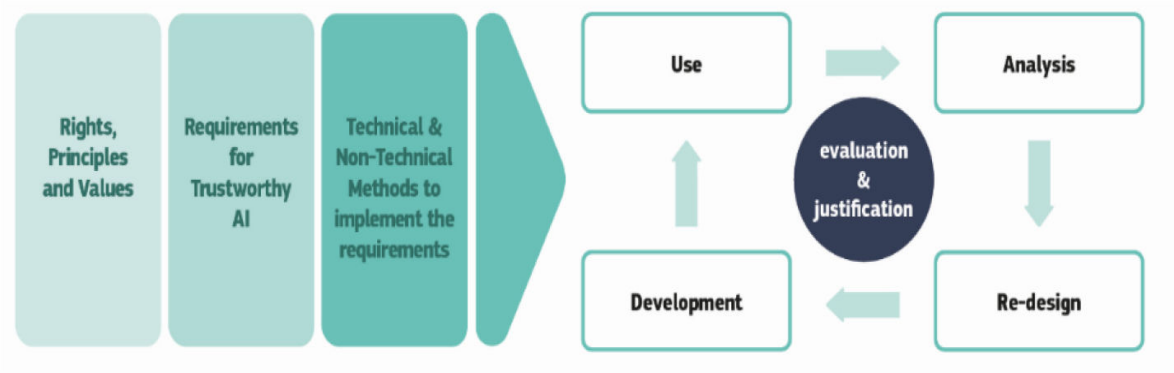

Figure 10 Trustworthy AI Life Cycle. Source: Ethics Guidelines for Trustworthy AI p.20 [318].

Examples of technical methods are the architecture for Trustworthy AI, Ethics and the 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 are being developed, deployed, and used adheres to the seven requirements of Trustworthy AI.

Building upon these principles, AI HLEG published the Assessment List for Trustworthy Artificial Intelligence (ALTAI) [319]. More specifically, 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 [320].

- **Human agency and oversight**

  AI systems should support human autonomy and decision-making, as prescribed by the principle of respect for human autonomy. The HLEG points out that when there is a risk that the AI system may negatively affect fundamental rights, an impact assessment should be undertaken. This should be done prior to the system's development. Individuals should also be able to make informed autonomous decisions regarding AI systems and have the knowledge and tools to understand and interact with AI systems. A central place of Individuals in the AI system's functionality means that it must respect their right not to be subject to a decision based solely on automated processing when this produces legal effects on users or similarly significantly affects them.

Funded by Horizon Europe Framework Programme of the European Union

- **Technical robustness and safety**

  This requirement deals with four main issues, namely: 1) security, 2) safety, 3) accuracy, and 4) reliability, fallback plans, and reproducibility. Technical robustness, closely linked to the principle of prevention of harm, requires AI systems to be developed with a preventative approach to risks. They should behave reliably while minimising unintentional and unexpected harm and preventing unacceptable harm.

  For AI systems to be considered secure, possible unintended applications of the AI system (e.g., dual-use applications) and potential abuse of the system by malicious actors, such as data-targeted attacks (data poisoning), model-targeted attacks (model leakage) or software and hardware attacks should be taken into account [321]. Adequate steps should be taken to prevent and mitigate these risks, including safeguards that enable a fallback plan. It must be ensured that the system will be safe and do what it is supposed to do without harming humans or the environment. Accuracy is construed as an AI system's ability to make correct judgements, predictions, recommendations, or decisions based on data or models. It is important that the system can indicate how likely these errors are.

  Reliability requires scrutinising an AI system to prevent unintended harm. Reproducibility describes whether an AI experiment exhibits the same behaviour when repeated under the same conditions. The self-assessment list suggests that AI developers should ask themselves the following questions: "Did you put in place a well-defined process to monitor if the AI system is meeting the intended goals? Did you put in place verification and validation methods and documentation (e.g., logging) to evaluate and ensure different aspects of the AI system's reliability and reproducibility? Did you put in place a proper procedure for handling the cases where the AI system yields results with a low confidence score?" [322].

- **Privacy and data governance**

  AI systems are obligated to ensure privacy and data protection at every stage of their lifecycle. This encompasses not only the data provided by individuals but also the data generated about them during their interactions with the system (e.g. digital facial images and biometric templates). It is essential to guarantee that user data is not processed in a manner that unlawfully or unfairly discriminates against them. The quality and integrity of the data must be maintained rigorously.

  Furthermore, organisations handling personal data must make their data access protocols readily available to ensure transparency. Compliance with data protection legislation is paramount. It is important to address whether the AI system has been trained or developed using personal data, including special categories of personal data (e.g., biometric data). This includes conducting a data protection impact assessment, appointing a data protection officer, implementing privacy by design and by default principles, and upholding the data minimisation principle, especially concerning special categories of personal data.

Funded by Horizon Europe Framework Programme of the European Union

- **Transparency**

  The HLEG Guidelines suggest a tripartite approach to transparency. Firstly, traceability, which involves ensuring detailed documentation of datasets and processes that contribute to the AI system's suggestions. Hence, AI developers should be capable of tracing the data, models, and rules that the AI system utilised to arrive at certain decisions or recommendations. Secondly, explainability is a critical aspect of trustworthy AI. This involves the capacity to elucidate both the AI system's technical processes and related human decisions. The HLEG Guidelines stipulate, "Whenever an AI system has a significant impact on people's lives, it should be possible to demand a suitable explanation of the AI system's decision-making process" [323]. The HLEG further explained that "the degree to which explicability is needed is highly dependent on the context and the severity of the consequences if that output is erroneous or otherwise inaccurate". Third, humans should be informed that they are interacting with an AI system. They should also have the option to have a human interaction instead.

- **Diversity, non-discrimination and fairness**

  Biased data could lead to unintended (in)direct prejudice and discrimination against certain groups or people, potentially exacerbating prejudice and marginalisation. In this context, the HLEG Guidelines highlight the need to avoid unfair bias, foster accessibility, and ensure stakeholder participation throughout the process of implementing AI technology.

- **Societal and environmental wellbeing,**

  The HLEG promotes the sustainability and ecological responsibility of AI systems and encourages their environmental friendliness.

- **Accountability**

  The HLEG highlights the importance of accountability in the AI ecosystem, which "requires the establishment of mechanisms to guarantee responsibility for AI systems and their outcomes, both pre-and post-development, deployment, and utilisation".

  Accountability also necessitates audibility, enabling the evaluation of algorithms, data, and design processes, for instance, through evaluation reports. It includes conducting impact assessments (such as red teaming or Algorithmic Impact Assessments) commensurate with the risk level posed by the AI systems. These assessments should clearly recognise and evaluate potential compromises regarding ethical principles, including fundamental rights. When an unjust

Funded by Horizon Europe Framework Programme of the European Union

negative impact arises, accessible channels must be provided to ensure appropriate redress [324].

Eventually, it is noteworthy that the 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.

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 to AI in the EU.

Funded by Horizon Europe Framework Programme of the European Union

6 Ethical and Legal Frameworks Guiding Clinical Research

CYLCOMED pilot 2 encompasses the real-world deployment in the form of an observational clinical study within existing hospital ecosystems, providing the integration of CYLCOMED tools. It will include the participation of paediatric patients with heart failure. Hence, this section is focused on the analysis of ethical and legal requirements for the children's participation in the clinical studies.

The primary objective of clinical research is to generate generalisable knowledge aimed at improving health and enhancing understanding of human biology.[325] It is an established fact that clinical research involving children and young people, ranging from newborn babies to adolescents, has always been perceived as highly challenging, both from ethical and practical standpoints. The safety of children during research is of paramount importance, as they are often perceived as “vulnerable”. For this reason, it is crucial to implement special protections to prevent any exploitation [326]. While the involvement of children in medical studies bears inconvenience, discomfort, burdens, and risks, especially if the research involves babies or, in the case of testing new medicines, clinical research involving children is essential in understanding childhood diseases and conditions [327].

Nowadays, digital devices, data analytics, and artificial intelligence are revolutionising the landscape of clinical research. These advancements enable the collection of real-time data encompassing various aspects of individuals' health and lifestyle. Moreover, they facilitate the identification of patterns within vast datasets. Remote monitoring technologies (RMTs), including wearables, smartphone applications, and fixed sensors installed at home, play a pivotal role in this transformation. By capturing real-world information about study participants continuously and objectively, RMTs offer unprecedented insights into health behaviours and outcomes [328]. While remote monitoring technologies, such as telemedicine, present exciting prospects for clinical research, their adoption also introduces novel ethical considerations.

The most prominent among these are concerns surrounding privacy and data security. As digital technologies capture and transmit sensitive health-related data, ensuring the confidentiality and integrity of participants' information becomes paramount. For instance, recent scoping review, which included 264 publications focused on ethical consideration in big data trends in biomedical and health research, has revealed that privacy and confidentiality are by far the dominant concern in the ethical domain, followed by informed consent and ethical oversight by independent ethical committees [329]. Striking a balance between leveraging the benefits of remote monitoring technologies and safeguarding individuals' privacy rights poses a significant challenge for research ethics in the digital age [330].

In order to ensure that human rights and the highest ethical standards are respected, many international documents lay down rules aimed at ensuring a strong ethical imperative in research involving children. These human rights and ethical principles are those expressed, for instance, in the Universal Declaration of Human Rights,

Funded by Horizon Europe Framework Programme of the European Union

European Convention on Human Rights, United Nations Convention on the Rights of the Child, the Universal Declaration on Bioethics and Human Rights, the Universal Declaration on the Human Genome and Human Rights, the International Declaration on Human Genetic Data, Declaration of Taipei on Ethical Considerations regarding Health Databases and Biobanks, Declaration of Helsinki and The Oviedo Convention on Human Rights and Biomedicine.

Furthermore, agreed requirements as to what constitutes “ethical practice” in clinical research are also echoed and referred to in the various guidelines and recommendations, such as the ICH E6 guideline on Good Clinical Practice and the ICH E11 guideline on the Clinical Investigation of Medicinal Products in the Pediatric Population, the International ethical guidelines for health-related research involving humans of the Council for International Organizations of Medical Sciences (CIOMS) in collaboration with the World Health Organization (WHO).

Given the large number of international documents and guidance with varying legal force, context and focus, the true challenge lies in translating ethical principles into clinical research and establishing procedures that align with international human rights law while maintaining ethical integrity. Hence, taking principles of biomedical research as the universally accepted framework as the main starting point, this section will further elaborate on the ethical and legal frameworks identified in deliverable D2.1, such as the Declaration of Helsinki, ICH E6 guideline on Good Clinical Practice, Clinical Trial Regulation, as the main frameworks of relevance for the CYLCOMED project. Before embarking on ethical and legal frameworks regarding the involvement of the paediatric population in clinical research studies, it is necessary to ensure terminological consistency and, therefore, introduce the main terminological and definitional terms used by these frameworks. Hence, it is important to clarify the doctrines of informed consent, assent and dissent in a clinical research setting. Furthermore, since freely given informed consent is the foundation of contemporary ethics in clinical research, this section will be focused on the requirement for informed consent laid down by the aforementioned documents, with a specific focus on children/minors in the process of obtaining informed consent.

6.1 Informed consent, Assent and Dissent

Despite the diverse array of ethical and legal requirements governing research encompassed by the aforementioned documents, there has been longstanding consensus on the fundamental principles of ethical research conduct. Key among these is the doctrine of informed consent, which emphasises that individuals must be fully informed and voluntarily consent to participate in research. Additionally, there is a shared understanding that the interests of science and society should never supersede the rights and welfare of individual participants. Furthermore, it is universally recognised that human subjects should never be subjected to unnecessary risks in clinical research [331].

Funded by Horizon Europe Framework Programme of the European Union

6.1.1.1 Informed Consent

Freely given informed consent serves as the cornerstone of contemporary ethics in clinical research. It is a fundamental condition that must be met for a person to participate in a clinical trial. This fundamental principle ensures that individuals voluntarily agree to participate in research after being fully informed about the nature of the study, its potential risks and benefits, and their rights as research participants.[332] The concept of informed consent is founded upon the moral and legal principle of individual autonomy, emphasising individuals' right to make decisions about their own lives [333]. In other words, the doctrine of informed consent serves dual functions in research settings. Legally, it establishes a clear framework for the relationship between researchers and study participants. Ethically, informed consent embodies the principle of respect for persons by ensuring that individuals understand the nature of the research and freely consent to participate without coercion or deception. In essence, informed consent safeguards research subjects from potential harm, including deception, coercion, and exploitation, thereby upholding their autonomy and dignity throughout the research process [334].
The aim of informed consent is to safeguard several values, including non-maleficence, the subject's individual liberty, personal autonomy, and human dignity. It also fosters trust between subjects and investigators, ensuring that subjects have confidence that they will be treated with respect and that any potential harm will be avoided [335].

Informed consent means a “subject's free and voluntary expression of his or her willingness to participate in a particular clinical trial, after having been informed of all aspects of the clinical trial that are relevant to the subject's decision to participate or, in case of minors and of incapacitated subjects, an authorisation or agreement from their legally designated representative to include them in the clinical trial”.

From the discussion above, it can be seen that informed consent relies on three critical and essential elements: voluntarism, information disclosure, and decision-making capacity. These elements are necessary for an ethically valid and genuine informed consent. They must be effectively employed and adequately present when seeking informed consent from a research subject.

6.1.1.2 Assent / Dissent

When an individual lacks the capacity, including legal capacity, to consent to certain actions, they can still be involved in the decision-making process through **assent**. A child's participation in research is rooted in the fundamental right to express their own opinions, as outlined in the Charter of Fundamental Rights of the European Union and the UN Convention on the Rights of the Child. For instance, Article 24. of the Charter stipulates that:

Funded by Horizon Europe Framework Programme of the European Union

> "Children shall have the right to such protection and care as is necessary for their well-being. They **may express their views freely**. Such views shall be taken into consideration on matters which concern them in accordance with their age and maturity".

Likewise, The United Nations Convention on the Rights of the Child upholds several rights for children, including the right to express their opinions in decisions that affect them (Article 12), the right to access and share information (Article 13), the right to freedom of thought, belief, and religion, as long as it does not impede the rights of others (Article 14), and the right to privacy (Article 16).

Assenting involves a similar process to informed consent and allows individuals to express their agreement or willingness to participate in an action or activity [336]. The term "assent" is used widely within both international declarations on research ethics and in some national legislation to encompass this involvement in the decision-making process regarding participation in clinical research studies but with very different meanings and implications. The assent procedure aims to facilitate the minor's understanding, to the extent possible, of what their participation in the decision-making process entails. It ensures that minors are provided with information appropriate to their level of comprehension, allowing them to meaningfully participate in decisions regarding their involvement in research [337]. These vary from "the emergent capacity to agree" of a three-year-old to the "knowing agreement" of an adolescent who has not yet reached the legally established age of consent but who nevertheless has the capacity to make their own decisions. In other words, assent revolves around respecting children's evolving capacity, which involves aiding them in comprehending their condition and treatment at a level suitable for their developmental stage and engaging them in relevant decision-making processes [338].

> **"Assent"** is a term used to express the willingness to participate in research by persons who are, by definition, too young to give informed consent but who are old enough to understand the proposed research in general, its expected risks and possible benefits and the activities expected of them as subjects [339].

However, assent by itself is not sufficient. If assent is given, informed consent must still be obtained from the subject's parents or guardian. Eventually, it is important to point out that considerable disagreement among experts remains about many fundamental components of assent, including the definition of assent, the age at which investigators should solicit assent from children, who should be involved in the assent process, how to resolve disputes between children and their parents; the relationship between assent and consent; the quantity and quality of information to disclose to children and their families; how much and what information children desire and need, the necessity and methods for assessing both children's understanding of disclosed

Funded by Horizon Europe Framework Programme of the European Union

information and of the assent process itself; and what constitutes an effective, practical, and realistically applicable decision-making model [340].

6.1.1.3 Dissent

Dissent is refusal to grant or subsequent withdrawal of consent or assent [341]. There is a similar variation in how a child's 'dissent' should be handled: in particular, whether it should be 'considered' or 'respected'.

6.1.2 Ethical Principles In Biomedical Ethics

Although the documents mentioned above might differ and emphasise specific ethical requirements, they share common grounds. They all build on four cardinal ethical principles that should be adhered to when performing research, namely: beneficence, non-maleficence, respect for autonomy and justice. While some of these principles, such as beneficence and nonmaleficence, can be traced back to the time of Hippocrates, "to help and do no harm," [342], the principles established by Beauchamp and Childress in modern times are classic principles widely recognised in medical ethics [343].

• **Autonomy:** The principle of respecting autonomy underscores the importance of honouring an individual's choices and refraining from interfering with their decision-making process. It safeguards the inherent right to self-determination, empowering individuals to make deliberate and voluntary decisions free from external influence. Examples of duties aligned with respecting autonomy include truthfulness and maintaining confidentiality to preserve privacy. Adhering to the principle necessitates healthcare providers to disclose pertinent medical information and treatment options, enabling patients to exercise self-determination. It supports practices such as informed consent, truthfulness, and confidentiality, serving as a vital mechanism for upholding and honouring an individual's autonomy [344][345][346].
• **Non-maleficence:** Non-maleficence entails the duty to prevent harm. The principle of non-maleficence dictates refraining from causing harm to others, encompassing the duty to avoid creating risks of harm to individuals. This principle underpins various moral rules, including refraining from causing pain or suffering, incapacitating, causing offense, and depriving others of life's necessities. For instance, in practice, non-maleficence guides physicians to carefully assess the benefits and burdens of all interventions and treatments, avoiding those that are excessively burdensome and selecting the most suitable course of action for the patient [347][348][349].
• **Beneficence:** Beneficence, as an ethical obligation, involves maximising benefits while minimising harm, complementing the principle of non-maleficence, which mandates refraining from causing harm. It requires

Funded by Horizon Europe Framework Programme of the European Union

actively contributing to the well-being and welfare of others, extending beyond professional roles to encompass all individuals. For example, it includes protecting the rights and freedoms of others by addressing adverse conditions that may impede them. In the realm of research, it necessitates ensuring that risks are reasonable in relation to expected benefits, that research designs are robust, and that investigators are competent to both conduct the research and safeguard the welfare of participants. Unlike non-maleficence, which focuses on avoiding harm, beneficence emphasises the positive duty to benefit patients and promote their welfare [350][351][352].
• **Justice:** The principle of justice is closely linked with the concept of fairness, which aligns with the aspiration to ensure equal and just opportunities for all individuals. In clinical ethics, distributive justice, which focuses on the fair allocation of resources, holds particular significance. Distributive justice pertains to ensuring the fair, equitable, and suitable distribution of healthcare resources. For example, distributive justice significantly influences the selection of research participants. Criteria should directly align with the research's objectives rather than being solely based on the ease of obtaining consent. Conversely, this principle also mandates that groups likely to benefit from the research are not unfairly excluded [353][354][355].

In light of these principles, a growing consensus is shaping the essential elements vital for ethical conduct in clinical research. These encompass the scientific value and robustness of the study, ensuring a favourable balance between risks and benefits, fair selection of participants, the crucial aspect of informed consent, independent review processes, and, above all, the utmost respect for the rights and well-being of research subjects [356].

6.1.3 Declaration of Helsinki

The Declaration of Helsinki is one of the most influential and well-known international statements on the ethical principles that should be applied in medical research involving human subjects [357]. Although the Declaration text underwent seven revisions, along with two notes of clarification from 2002 and 2004, with the most recent revisions taking place in October 2013, it still remains ‘the most widely recognised source of ethical guidance for biomedical research” [358] and the “cornerstone” document pertaining to medical research ethics [359]. It was developed by the World Medical Association (WMA) as a statement of ethical principles for medical research involving human subjects, including research on identifiable human material and data [360]. While the Declaration encompasses a number of critical human research ethics codes of practice, it remains a relatively concise document, spanning only five pages and 37 Articles. Despite its brevity, the Declaration encapsulates fundamental principles and guidelines essential for the ethical conduct of research involving human

Funded by Horizon Europe Framework Programme of the European Union

subjects. It is important to note that the Helsinki Declaration principles concern all types of medical research [361].

The 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. It highlights 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 been obtained to ensure the appropriateness of design before initiating research [362]. The Declaration of Helsinki was the first set of international research guidelines that required research participants to provide **informed consent**, which is one of the most prominent requirements of the Declaration. In accordance with the Declaration Article 25, participation in medical research by individuals capable of giving informed consent must be voluntary. While consulting family members or community leaders may be appropriate, no individual capable of giving informed consent should be enrolled in a research study unless they freely agree to participate. Furthermore, Article 26 outlines the requirements for informed consent in medical research involving human subjects who are capable of giving informed consent. It stipulates that potential subjects must be provided with comprehensive information regarding various aspects of the study, including its objectives, methods, funding sources, conflicts of interest, researcher affiliations, anticipated benefits and risks, potential discomfort, post-study provisions, and other relevant details. Additionally, potential subjects must be informed of their right to refuse participation or to withdraw consent at any time without facing any repercussions. In cases where a potential research subject is unable to provide informed consent, the physician must obtain consent from their legally authorised representative.

Apart from the informed consent of the legally authorised representative, the Declaration of Helsinki obliges physicians to seek **assent** in certain cases. This applies when a potential research subject, deemed incapable of giving informed consent, can provide assent to decisions regarding participation in research. However, apart from this obligatory requirement, the Declaration **does not provide more clarification on assent**. Likewise, while the Declaration stipulates that the potential subject's dissent should be respected, it does not elaborate further on the practical implications of expressed dissent.

Next, the Declaration explicitly refers to "vulnerable groups and individuals" in its text and uses this umbrella term without further elaboration on who is encompassed by this term. Therefore, it does not contain any specific reference to children or minors, making only the distinction between those capable or incapable of giving informed consent. It stipulates the general rule that special consideration and protection should be afforded to vulnerable groups and individuals in medical research to prevent the risk of harm or wrongdoing.

Funded by Horizon Europe Framework Programme of the European Union

6.1.4 ICH Guideline for Good Clinical Practice (E6)

ICH Guideline for Good Clinical Practice (ICH-GCP) is an international ethical and scientific quality standard for designing, conducting, recording and reporting trials that involve the participation of human subjects [363]. ICH-GCP guidelines have been established to set an ethical and scientific quality standard for trials involving human subjects, in alignment with the principles outlined in the Declaration of Helsinki.[364] Compliance with ICH-GCP provides public assurance that the rights, safety, and well-being of research subjects are protected and respected, consistent with the principles enunciated in the Declaration of Helsinki and other internationally recognised ethical guidelines, and ensures the integrity of clinical research data [365]. One of the main goals of ICH-GCP is to establish a standardised framework within the European Union (EU), Japan, and the United States, promoting the mutual acceptance of clinical data by regulatory authorities in these jurisdictions [366].

While ICH-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 research settings since its primary purpose is to safeguard human rights and ensure safety and well-being of trial subjects [367]. It enforces tight guidelines on the 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. ICH-GCP aims to ensure that the studies are scientifically robust and that the clinical properties of the investigational product are properly documented. The following 13 key principles constitute the foundation of the ICH-GCP:

1. Clinical trials must adhere to the Declaration of Helsinki, ICH-GCP, and regulatory requirements.
2. Before initiation, potential risks must be balanced against foreseeable benefits for subjects and society.
3. Priority must be given to the rights, safety, and well-being of human subjects over scientific or societal interests.
4. Sufficient clinical and nonclinical information on investigational products must support proposed trials.
5. Clear and comprehensive protocols should outline scientific clinical trial procedures.
6. Trials must receive approval or a favorable opinion from an institutional review board (IRB)/independent ethics committee (IEC) based on the protocol.
7. Qualified physicians are responsible for subjects' medical care and decisions.
8. All trial participants should be educated, trained, and experienced in their roles.

Funded by Horizon Europe Framework Programme of the European Union

9. Voluntary informed consent must be obtained from participants before their involvement.
10. Trial information should be accurately recorded, managed, and available for reporting and verification.
11. Privacy and confidentiality of subjects' records must comply with relevant regulatory requirements.
12. Good manufacturing practice (GMP) standards should guide the production, handling, and storage of investigational products, consistent with approved protocols.
13. Implement special systems and procedures to ensure trial details are effectively managed and documented.

ICH-GCP also provides clear guidance on the **informed consent** requirements that need to be signed by the study participant before their involvement. ICH-GCP defines informed consent as the "*process by which a subject voluntarily confirms his or her willingness to participate in a particular trial, after having been informed of all aspects of the trial that are relevant to the subject's decision to participate (1.28)*." GCP acknowledges the need to incorporate essential elements of informed consent in the discussion, written consent forms, and other information provided to study participants. This encompasses, but is not restricted to:

- Title of the protocol;
- Identity of the sponsor;
- Identity of the clinical investigator and institutional affiliation of the investigator;
- Source of research funding (e.g. public, private, or both);
- That the trial involves research;
- That the subject's participation in the trial is voluntary and that the subject may refuse to participate or withdraw from the trial, at any time, without penalty or loss of benefits to which the subject is otherwise entitled;
- The purpose of the trial;
- The trial treatment(s) and the probability for random assignment to each treatment;
- The trial procedures to be followed, including all invasive procedures;
- The subject's responsibilities;
- Those aspects of the trial that are experimental;
- The reasonably foreseeable risks or inconveniences to the subject and, when applicable, to an embryo, fetus or nursing infant;

Funded by Horizon Europe Framework Programme of the European Union

- The reasonably expected benefits. When there is no intended clinical benefit to the subject, the subject should be made aware of this;
- The alternative procedure(s) or course(s) of treatment that may be available to the subject, and their important potential benefits and risks;
- The compensation and/or treatment available to the subject in the event of trial-related injury;
- The anticipated prorated money or other forms of payment (e.g. material goods), if any, to the subject for participating in the trial;
- The anticipated expenses, if any, to the subject for participating in the trial. This may include expenses to the subject for routine medical care for conditions that are not within the scope of the research;
- That the monitor(s), the auditor(s), the IEC/IRB, and the regulatory authority(-ies) will be granted direct access to the subject's original medical records for verification of clinical trial procedures and/or data, without violating the confidentiality of the subject, to the extent permitted by the applicable laws and regulations and that, by signing a written informed consent form, the subject or the subject's legally authorized representative is authorizing such access;
- That records identifying the subject will be kept confidential and, to the extent permitted by the applicable laws and/or regulations, will not be made publicly available. If the results of the trial are published, the subject's identity will remain confidential;
- The potential risks should confidentiality measures be compromised (e.g. stigma, loss of reputation, potential loss of insurability);
- That the subject or the subject's legally authorized representative will be informed in a timely manner if information becomes available that may be relevant to the subject's willingness to continue participation in the trial;
- The person(s) to contact for further information regarding the trial and the rights of research subjects, and whom to contact in the event of trial-related injury;
- The foreseeable circumstances and/or reasons under which the subject's participation in the trial may be terminated;
- The expected duration of the subject's participation in the trial;
- The approximate number of subjects involved in the trial.

ICH-GCP places specific importance on communicating the informed consent. The investigator must communicate the information, whether orally or in writing, using language that aligns with the individual's level of understanding. Prior to participation in the trial, the subject or the subject's legally acceptable representative should receive a copy of the signed and dated written informed consent form and any other written information provided to the subjects. Although ICH-GCP contains a reference to the "vulnerable subjects" by giving examples of vulnerable categories, including here minors and subjects incapable of giving informed consent, it is interesting to note that ICH-GCP does not contain any specific reference to children/minors in terms of

Funded by Horizon Europe Framework Programme of the European Union

participation in clinical research study and the possibility of giving assent. It is, therefore, silent on the extent to which children may be considered capable of giving informed consent for themselves. Moreover, **it does not address the concept of assent and dissent at all.**

ICH-GCP only make a distinction between the trial subject and the subject's legally acceptable representative in cases where the trial subject is unable to sign informed consent. It specifically addresses two distinct cases, namely where a subject is unable to read or if a legally acceptable representative is unable to read and emergency situations when prior consent of the subject is not possible. Apart from these cases, it does not provide any further guidance on children/minors' participation in clinical study. However, ICH-GCP stipulates that any involvement of vulnerable categories should be subjected to special attention and scrutiny by the Ethics Committee.

6.1.5 International Ethical Guidelines for Health-Related Research Involving Humans (CIOMS Guidelines)

CIOMS Guidance is issued by the Council for the International Organizations of Medical Sciences (**CIOMS**) in association with the World Health Organization (WHO) [368]. The first version of the CIOMS Guidelines was issued in 1982 with the objective of providing globally recognised ethical principles and detailed commentary on how universal ethical standards should be applied. Since its inception, the CIOMS Guidelines have undergone four revisions, with the most recent being in 2016. This document combines and replaces the 2002 CIOMS International Ethical Guidelines for Biomedical Research Involving Human Subjects and the 2009 CIOMS International Guidelines for Ethical Review of Epidemiological Studies [369]. The present scope is confined to the classic activities falling within the purview of health-related research involving human subjects. These encompass a spectrum of activities, including observational studies, clinical trials, biobanking initiatives, and epidemiological investigations. The CIOMS guidelines primarily address a number of important areas related to research ethics, such as the scientific rigour and ethical justification of research endeavours, the requirements for ethical review and obtaining informed consent, the identification and mitigation of vulnerabilities among individuals, groups, communities, and populations involved in research [370].

While CIOMS guidelines 9 address the informed consent of research participants who possess the capacity to provide such consent, these overarching requirements closely resemble those outlined in the Declaration of Helsinki and ICH-GCP. Therefore, they will not be extensively examined to prevent redundancy and duplication of content. On the other hand, the CIOMS guidelines encompass a distinct guideline specifically addressing the involvement of children as research participants. It recognises that due to their unique physiologies and healthcare requirements, children and adolescents warrant special attention from both researchers and research ethics committees. Guideline 17 stipulates that research involving children may proceed only if:

Funded by Horizon Europe Framework Programme of the European Union

- "A parent or a legally authorised representative of the child or adolescent has given permission and
- The agreement (assent) of the child or adolescent has been obtained in keeping with the child's or adolescent's capacity after having been provided with adequate information about the research tailored to the child's or adolescent's level of maturity."

The CIOMS guidelines establish that, as a general rule, the decision of a child or adolescent to refuse participation or withdraw from the research **must be respected**. However, exceptions may arise where research participation is deemed the most suitable medical course for the child or adolescent in extraordinary circumstances. CIOMS's commentary on the guideline delves deeper into these headline concepts. CIOMS's commentary clarifies that children and adolescents, being legally minors, are unable to provide legally binding informed consent. However, they may have the capacity to offer assent. Assent entails the meaningful engagement of the child or adolescent in discussions regarding the research in alignment with their individual capacities. Therefore, guidelines oblige researchers to actively involve the child or adolescent in the decision-making process, utilising information appropriate to their age. It is crucial to inform the child or adolescent about the research and secure their assent, preferably documented in writing for literate children. The assent process should consider not just the child's age but also their specific circumstances, life experiences, emotional and psychological maturity, intellectual abilities, and family context.

6.1.6 Clinical Trials Regulation

The first deliverable identified the Clinical Trial Directive and Clinical Trial Regulation as legislative acts of relevance for the CYLCOMED project. Although the clinical study design for the implementation of the CYLCOMED Pilot 2 falls outside the Clinical trials legislation, which will be clarified below, it is important to extend the analysis in this deliverable due to the high ethical standards laid down by this Regulation, which can serve as guiding principles for the Consortium partners. Therefore, while the analysis will mainly focus on ethical norms laid down by the CTR, it will also present the key pillars of the CTR.

6.1.6.1 Introduction

Since 2001, the Clinical Trial Directive (CTD) [371] has regulated the conduct of clinical trials in the EU. The CTD aimed to standardise rules and notably improve patient protection in clinical trials in compliance with good clinical practice ICH-GCP. Although CTD has brought about important improvements in the safety and ethical soundness of clinical trials in the EU and in the reliability of clinical trials, the Commission's Impact

Funded by Horizon Europe Framework Programme of the European Union

Assessment report on the revision of the “Clinical Trials Directive” acknowledges that the CTD is the most heavily criticised piece of legislation of the entire EU acquis for pharmaceuticals [372]. The Report states, inter alia, that criticism has centred on the overly cumbersome and bureaucratic regulatory framework in the EU, which failed to achieve genuine harmonisation of administrative requirements. Increased costs for conducting clinical trials, delays in launching a clinical trial, separate submissions, diverging assessments, and regulatory supervision of applications for clinical trials are some of the identified issues that hampered the implementation of CTD and the achievement of its main goals. In order to overcome the identified shortcomings of CTD, it has been repealed by the Clinical Trials Regulation (CRT). Although CTR was adopted in 2014, its application depended on the development of a fully functional EU clinical trials portal and database, which has become fully functional since 31 January 2022.

The CRT, also known as the European Union (EU) pharmaceutical legislation, officially came into effect on January 31, 2022. Clinical Trials Regulation aims to achieve an internal market with regard to clinical trials and medicinal products for human use, taking as a base a high level of health protection. At the same time, this regulation sets high standards of quality and safety for medicinal products in order to meet common safety concerns regarding these products [373]. In other words, it’s primary objective is to create a conducive environment within the EU for conducting large-scale clinical research, emphasising rigorous standards of public transparency and ensuring the safety of clinical trial participants.

The CRT, in comparison to CTD, has brought many novelties. For instance, CTR is a vertical legislative act directly applicable to all Member States without the need to be transposed into national laws, thus ensuring that the rules for assessing clinical trial applications and conducting clinical trials are identical throughout the EU. CRT not only repealed the Clinical Trials Directive (CTD) but also national implementing legislation in the EU Member States that previously governed clinical trials in the EU until the CTR’s entry into application.

Secondly, CRT facilitates the submission of multinational clinical trials. For instance, under the Directive normative framework, clinical trial sponsors were required to submit separate clinical trial applications to national competent authorities and ethics committees in each country to obtain regulatory approval for conducting a clinical trial. In contrast, the CRT enables sponsors to submit a single online application through a unified platform called the Clinical Trials Information System (CTIS) for approval to conduct clinical trials in multiple European countries, streamlining the process of multinational trials. The rationale behind this, as stated by CRT Recital 4, is procedural simplification and the avoidance of multiple submissions containing largely identical information. It encourages the submission of a single application dossier to all relevant Member States through a centralised submission portal. Thus, the Regulation enhances efficiency by enabling EU Member States to collectively evaluate and authorise such applications via the Clinical Trials Information System.

Funded by Horizon Europe Framework Programme of the European Union

Furthermore, CTD introduces a streamlined application procedure for all clinical trials conducted in Europe via an online portal “Clinical Trials Information System (CTIS)”. CTIS is the online system for the regulatory submission, authorisation and supervision of clinical trials in the European Union and the European Economic Area. It supports interactions between clinical trial sponsors (researchers or companies that run a clinical trial and collect and analyse the data) and regulatory authorities in the EU Member States and EEA countries throughout the lifecycle of a clinical trial. Clinical trial sponsors can use CTIS to apply for authorisation to run a clinical trial in up to 30 EEA countries via a single online application. They can also carry out tasks including liaising with national regulators while a trial is ongoing and recording clinical trial results. National regulators can use CTIS to collaborate on the evaluation and authorisation of a clinical trial in several EU/EEA countries. Additionally, the framework has embedded tools to grant citizens access to the ongoing trials. European Medicines Agency (EMA) maintains this website in collaboration with the EU Member States, EEA countries, and the European Commission.

Yet, it is important to note that until 30 January 2023, clinical trial sponsors could choose whether to apply to start a clinical trial via the Clinical Trials Information System or under the Clinical Trials Directive. However, from 31 January 2023 onwards, all new initial CTAs should be submitted under the CTR. Additionally, as of 31st January 2025, all ongoing clinical trials with an active site in the EU/EEA should be conducted under the CTR [374]. In order to be prepared for submitting applications and notifications via CTIS, sponsors are advised to check the training modules for CTIS [375], the CTIS sponsor handbook [376] with details on how to use CTIS and the overview of structured data to be completed in CTIS [377].

6.1.6.2 Scope of Application

The term "clinical research" can be ambiguous and subject to an array of interpretations, as it encompasses a broad range of activities within the healthcare and medical fields. It can refer to investigations aimed at understanding disease mechanisms, evaluating treatment effectiveness, assessing healthcare interventions, or studying health outcomes in populations. Additionally, clinical research may involve observational studies, clinical trials, epidemiological research, translational research, and other methodologies. The interpretation of “clinical research” often depends on the context in which it is used and the specific objectives of the study or investigation [378][379]. In recent times, clinical research has often been equated with drug research, particularly focusing on clinical trials. However, clinical research encompasses a broader spectrum, extending to all types of studies involving human participants aimed at generating new knowledge for diagnosis, treatment, and prevention in the realm of human health and diseases. This encompasses a wide range of disciplines, from molecular genetics to epidemiology and public health research, reflecting the diverse avenues through which advancements in healthcare are pursued [380]. Hence, it is crucial to provide clarity on the definition of a clinical trial and the

Funded by Horizon Europe Framework Programme of the European Union

scope of regulation it entails. Therefore, Articles 2(2) (1 and 2) of the Clinical Trials Regulation provide a definition of a "*clinical study*" as well as a "*clinical trial*".

A 'Clinical study' means any investigation in relation to humans intended:

(a) To discover or verify the clinical, pharmacological or other pharmacodynamic effects of one or more medicinal products;

(b) To identify any adverse reactions to one or more medicinal products; or

(c) To study the absorption, distribution, metabolism and excretion of one or more medicinal products; with the objective of ascertaining the safety and/or efficacy of those medicinal products.

According to article 2(2) of the CTR, "Clinical trial' means a clinical study which fulfils any of the following conditions:

(a) The assignment of the subject to a particular therapeutic strategy is decided in advance and does not fall within normal clinical practice of the Member State concerned;

(b) The decision to prescribe the investigational medicinal products is taken together with the decision to include the subject in the clinical study; or

(c) Diagnostic or monitoring procedures in addition to normal clinical practice are applied to the subjects.

The key question to address in determining whether a clinical research study falls within the scope of the CRT is defining what constitutes a "medical product". Medicinal product is defined in Article 1(2) of Directive 2001/83/EC [381].

According to Article 1(2) "medicinal product" is defined as follows:

(a) Any substance or combination of substances presented as having properties for treating or preventing disease in human beings; or

(b) Any substance or combination of substances which may be used in or administered to human beings either with a view to restoring, correcting or modifying physiological functions by exerting a pharmacological, immunological or metabolic action, or to making a medical diagnosis."

A substance is thus a medicinal product either by virtue of its "presentation" or its "function". A substance constitutes a medicinal product if it falls within either of these

Funded by Horizon Europe Framework Programme of the European Union

two categories. However, it is important to note that the classification of a substance as a medicinal product is the exclusive responsibility of the member states. Sponsors are, therefore, advised to seek guidance from the relevant member states if there is uncertainty regarding the status of a research product.

Next, in borderline cases, it is challenging to make a distinction between a medicinal product and other products, such as cosmetic products, medical devices and food supplements, due to their similarities in real-life cases. Borderline cases are those for which it is not clear from the outset whether a given product is a medical product, medical device, or food supplement, or not. Hence, in order to establish the “borderline” between a medicinal product and other products, the Commission has provided additional guidelines for the borderline between medicinal products and cosmetic products, medicinal products and medical devices, and guidelines for distinguishing medicinal products and food supplements [382][383].

Furthermore, when a study involves a medical device, the Expert Group on Clinical Trials provided an opinion that a medical device can play a role in different contexts In terms of EU regulation for clinical trials [384]. In cases where the object of the study is a combination of a medical device and a medicinal product, the regulatory status of the product must be determined in accordance with the definitions outlined in the applicable legislation (e.g. MDR and IVDR). The principal mode of action plays a crucial role in this determination. If the assessment reveals that the product under study is a medicinal product, the regulatory framework of the Clinical Trials Regulation applies. Conversely, if the assessment indicates that the product is a medical device, the Clinical Trials Regulation does not apply. For instance, the Expert Group on Clinical Trials provided an example involving a prefilled syringe, which would typically be classified as a medicinal product due to its integral 'delivery product'. Consequently, an interventional study involving such a product would be considered a clinical trial and fall within the regulatory framework of the Clinical Trials Regulation.

In another common scenario, the focus of the study remains a medicinal product, yet medical devices are utilised during the clinical trial without being the primary subject of investigation. In such instances, the Clinical Trials Regulation remains applicable. However, it's essential to ensure that these medical devices, despite not being the primary focus of the study, comply with EU regulations regarding their placement on the market and putting into service medical devices.

Lastly, the Expert Group on Clinical Trials provides an example where the study involves two separate products: one medicinal product and one medical device. These products may be administered or used on subjects within the same group or in different groups. An example scenario is a study comparing a warming medical device applied to the skin with a warming medicinal product applied topically. In such cases, the Clinical Trials Regulation applies to the aspect of the study involving the medicinal product as the primary subject. However, regarding medical devices as the primary subject, the Clinical Trials Regulation does not apply. Instead, the EU rules applicable to medical devices would govern.

Funded by Horizon Europe Framework Programme of the European Union

Furthermore, the Expert Group on Clinical Trials highlights that a study may entail the administration of a medicinal product, yet the primary focus of investigation pertains exclusively to the physiology of the body rather than the administered medicinal product itself. However, such studies do not fall under the definition of “clinical trials” as outlined in Article 2(2)(2) of the Clinical Trials Regulation (CTR). Consequently, the medicinal product administered in these studies does not qualify as an investigational medicinal product under Article 2(2)(5) of the CTR. As a result, these studies are not subject to regulation at the EU level. It is left to the discretion of Member States to determine whether and how they wish to regulate such studies. Moreover, the CTR does not apply to non-interventional studies, which are, according to article 2(2)(4) of the Clinical Trials Regulation, defined as a *"clinical study other than a clinical trial." Hence,* a study is non-interventional as long as it does not fulfil any of the conditions defining a clinical trial. In many European countries, non-interventional studies are still commonly referred to as observational studies [385].

6.1.6.3 Informed Consent in Clinical Trials

The protection of subjects and informed consent are of the utmost importance in clinical trials. The CTR has taken a significant step forward by devoting an entire Chapter V to this critical subject matter. This change substantively strengthens the safeguards in place and ensures greater participant safety compared with the repealed Directive. However, it is important to note that while CTR sets out various minimum requirements in regard to informed consent, according to Article 29(8), the Regulation is without prejudice to national law requiring that, in addition to the informed consent given by the legally designated representative, a minor who is capable of forming an opinion and assessing the information given to him or her, shall also assent in order to participate in a clinical trial. Hence detailed requirements for consent may differ between EU countries.

The CRT Article 2(21) defines Informed consent as “a subject's free and voluntary expression of his or her willingness to participate in a particular clinical trial, after having been informed of all aspects of the clinical trial that are relevant to the subject's decision to participate or, in case of minors and of incapacitated subjects, an authorisation or agreement from their legally designated representative to include them in the clinical trial”. The CTR’s Article 29 sets out conditions which need to be met in regard to informed consent. Namely, it requires that informed consent must be written, dated and signed by the person performing the interview and by the subject or, where the subject is not able to give informed consent, his or her legally designated representative after having been duly informed. Where the subject is unable to write, consent may be given and recorded through appropriate alternative means in the presence of at least one impartial witness. In that case, the witness shall sign and date the informed consent document. The subject or, where the subject is not able to give informed consent, his or her legally designated representative shall be provided with a copy of the document (or the record) by which informed consent has been given. The informed consent shall be documented. Adequate time shall be given for the subject

Funded by Horizon Europe Framework Programme of the European Union

or his or her legally designated representative to consider his or her decision to participate in the clinical trial.

In contrast to the repealed Directive, CRT specifically addresses the minor's participation in the trials, thus significantly strengthening the importance of their role in the study. The CRT stresses the significance of considering minors' wishes regarding their involvement in clinical trials. The Regulation mandates their active involvement with the aim of treating them as developing autonomous beings whose maturity gradually evolves with age and experience and whose will should be taken seriously [386]. The CRT Article 2(3)(18) defines a “Minor as the subject who is, according to the law of the Member State concerned, under the age of legal competence to give informed consent”. Each minor should partake in the informed consent process alongside their parents or legally designated representative in a manner that aligns with their age and level of maturity, as stipulated in Article 32(2) of the Clinical Trials Regulation.

The CRT also mandates specific requirements regarding the information that should be provided to both children and their legally designated representatives regarding the proposed research. These requirements are as follows:

- Information for the participant or for the legally designated representative must “be kept comprehensive, concise, clear, relevant and understandable to a layperson [387],
- Minors must receive information about the study “in a way adapted to their age and mental maturity and from investigators or members of the investigating team who are trained or experienced in working with children” [388].

Besides, the CTR sets out minimum requirements with respect to the way in which minors should be involved in a decision to take part (or not take part) in research:

- A minor should “take part in the informed consent procedure in a way adapted to his or her age and mental maturity” [389],
- It is open for member states' laws to specifically stipulate that “a minor who is capable of forming an opinion and assessing the information given to him or her shall also assent in order to participate in a clinical trial” [390] and
- “The explicit wish of a minor who is capable of forming an opinion and assessing the information” provided to refuse participation in, or to withdraw from, the clinical trial at any time should be “*respected*” by the investigator [391].

Further guidance on “informed consent” is provided by the **EC Guidance note on informed consent** [392]. This document lays down rules on, inter alia, obtaining the consent of a parent/legal representative and, where appropriate, the assent of the

Funded by Horizon Europe Framework Programme of the European Union

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, it is defined as follows:

> "***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*".[393]

EC Guidance note states that while **informed consent must be obtained from the parents or legal representative** when the child is able to give assent, the investigator **must also obtain that assent**. A child's refusal to participate or continue participating in the research should always be respected. Other requirements encompassed by the EC Guidance note are presented in Table 15.

Informed Consent and Information sheets are comprehensive and separate for parents/legal representative and for children.
Information sheets must be in accordance to the age of children: • **Information for children five years and under should be predominantly pictorial.** • **For pre-adolescent (aged up to 16) information sheets should explain briefly and in simple terms the background and aim of the study, so the child can consider assent. It also should contain an explanation that their parents will be asked for consent.** • **If an adolescent aged 16 to 18 is no longer a minor as defined in national law, or is an "emancipated minor", then written informed consent is required from these individuals.**
Assent of the child who is able to give must be required.
Information sheets should indicate how the study will affect the child at home, school or other activities.

Table 15 Informed Consent Requirements [394]

While international documents establish ethical requirements for assent, including the Clinical Trials Regulation, they do not specify the age threshold for minors in terms of maturity to provide assent. Instead, they delegate this matter to national regulations, resulting in varying interpretations and practical implementations across different jurisdictions. Undoubtedly, much of the debate about child assent centres around the question of when children become capable of providing assent. Recommendations of

Funded by Horizon Europe Framework Programme of the European Union

the European Commission expert group on clinical trials for the implementation of CTR guidance sheds more light on this matter [395]. The document offers recommendations concerning various ethical considerations in clinical trials involving minors, spanning from birth to the age of legal competence, to provide informed consent. These recommendations aim to ensure the protection of minors participating in clinical research, safeguard their rights and welfare, and uphold ethical standards throughout the trial process.

While the document primarily focuses on offering recommendations for ethical considerations in paediatric interventional clinical trials falling under the provisions of the Clinical Trials Regulation on medicinal products for human use, it is important to note that these recommendations are applicable to other types of paediatric trials and studies as well. This broader applicability stems from the fact that the recommendations are rooted in ethical principles derived from various international documents, thus ensuring their relevance and validity across a broad spectrum of paediatric research.

According to the Guidance document, participation and agreement/assent according to age groups and level of maturity are as follows (Table 16):

Newborns and infants **(from birth to 2 years of age)**	**In this age group, it is not possible to obtain agreement, and understanding of research is not expected.** **Providing information to the child is mostly aimed at preparing the child for the procedures to come.**
Pre-schoolers **(2-5 years of age)**	**Within this age group, there is the emergent capacity to provide agreement.** Age and maturity appropriate information is needed for all children who have some capacity of understanding, even if the evaluation concludes that agreement is not obtainable. Since textual information is not usable by most of these children, other types of visual information should be provided to ensure that the child is properly informed, e.g. videos, pictograms, cartoons or drawings, which can be taken home and discussed with the parents/legally designated representative.
Schoolers **(6-9 years of age)**	**Within this age group there is a growing capacity to provide agreement.** Even though they are able to read and write, understanding can be enhanced by making use of

Funded by Horizon Europe Framework Programme of the European Union

	visuals, such as videos, pictograms, cartoons and drawings. Children of this age group should be well informed, and agreement obtained preferably in writing. Their dissent should be respected, as they are capable of forming an opinion of their own.
Adolescents **(10-18 years of age)**	This group is treated differently across Member States. Some Member States consider that adolescents above a certain age are no longer minors and have the legal competence to give informed consent on research participation. In other Member States, national law requires assent from all or part of this group. **Information should be provided, and agreement from an adolescent who is still a minor should be sought and respected**.

Table 16 Participation and Agreement/Assent According to Age Groups and Level of Maturity [396].

The processes for informing the child and seeking assent should be clearly defined in advance of the research and documented for each child. While assent may not be possible in all age groups (e.g., neonates) or in all research conditions (e.g., research in emergency situations), the information process provided to the child and the child's response should be documented.

To ensure age-appropriate comprehension and facilitate assent, an expert group on clinical trials recommends that the separate materials should be tailored for children, utilising language and communication tools such as visuals, cartoons, and videos suitable for their age and maturity level. More specifically, separate information sheets for adults and children and separate consent and assent forms should be used in order to provide age-appropriate information in language and wording appropriate to age, psychological and intellectual maturity. The assent information sheets and assent forms should be age-appropriate and should include the provision of information on the purpose of the trial and potential benefits and harms in terms that are honest but not frightening.[397] Technically, the assent document is designed to explain to the child, in language that they can comprehend, the essence of what is planned in the research. It also emphasises the child's right to decline participation or change their mind at any point during the research process [398].

Here, it is important to mention "*Assent/Informed Consent Guidance for Paediatric Clinical Trials with Medicinal Products in Europe*", developed by the European Network of Pediatric Research at the European Medicines Agency (Enpr-EMA), which provides practical instructions for legal and ethical requirements for informed consent and assent for children of all age groups [399]. Although not legally binding, this document

Funded by Horizon Europe Framework Programme of the European Union

is intended to be used as an overview tool of the contents for assent/informed consent forms for all stakeholders (such as patients, sponsors and investigators) to support the conduct of high quality pediatric clinical trials in Europe across all pediatric age groups, from birth to less than 18 years of age.

A total of 30 main subject elements necessary for the consent process in legal, ethical, or regulatory texts were categorised into two tables based on their nature. The first table comprises general elements applicable to all trials (5 elements), while the second table encompasses trial-specific topics (25 elements), which may vary depending on trial design. All subject elements were taken into account for four paediatric age groups (0–2; 2–5; 6–9; 10–18) and legal representative(s) as defined in the EU ethics guideline. A total of 30 identified main subject elements required for the consent process in legal, ethical or regulatory texts were divided into two tables based on the nature of the requirement. The first table is applicable to all trials (5 general elements), and the second table includes trial-specific topics (25 elements), which can vary between trial designs (table 1). All subject elements were considered for four paediatric age groups (0–2; 2–5; 6–9; 10–18) and legal representative(s) as defined in the EU ethics guideline. Given the existing national legal differences in requirements for consent and assent documents, this guide has the potential to elevate ethical standards and streamline the harmonisation of paediatric consent and assent documents across Europe [400].

6.1.6.4 Withdrawal of the Consent

“Withdrawal of consent” is the patient’s voluntary termination of informed consent to participate in a clinical trial at any point during the conduct of the study” [401]. In all situations, parents or legal representatives should be informed of their right to refuse participation in a clinical trial and are entitled to freely withdraw their informed consent without providing reasons. They should be reassured that withdrawing from the trial will not adversely affect the child, result in any detriment, or impact the ongoing treatment. This ensures that parents or legal representatives can make decisions in the best interest of the child without any undue pressure or consequences [402]. It is crucial to emphasise that even after a child withdraws from a trial, the investigator remains responsible for reporting any trial-related events. Additionally, the investigator must ensure that the child receives appropriate treatment and follow-up care. This underscores the ongoing commitment to the child's welfare and ensures that their well-being is prioritised even after their withdrawal from the trial.

6.1.7 Ethics Committees

International standards require research involving humans to undergo an ethics review by a research ethics committee. The ethics committee (EC) plays a vital role in overseeing clinical trials, ensuring that the rights, safety, and well-being of participants are protected. This role is particularly crucial for vulnerable participants who are most in need of such protection. “An Ethics Committee (EC) is an independent body

Funded by Horizon Europe Framework Programme of the European Union

composed of members with expertise in both scientific and non-scientific arenas which functions to ensure the protection of human rights and the well-being of research subjects based on six basic principles of autonomy, justice, beneficence, nonmaleficence, confidentiality, and honesty" [403]. It is important to note that various terms are used to refer to ethics committees tasked with reviewing human clinical trial protocols. These include the ethics committee (EC), research ethics committee (REC), and institutional review board (IRB). Despite the different names, these committees share the common objective of ensuring the ethical conduct of research involving human participants and safeguarding their rights and welfare [404].

Over the past 30 years, two primary types of ethics committees have emerged as dominant within healthcare institutions: research ethics committees (RECs) and healthcare ethics committees (HECs). However, it is important to distinguish between a research ethics committee (REC) and a hospital ethics committee (HEC). Research ethics committees primarily concentrate on the review of medical research involving human subjects, ensuring that studies adhere to ethical standards and safeguard the rights and welfare of participants. On the other hand, healthcare ethics committees primarily address moral issues arising in standard patient care, providing guidance and oversight on ethical dilemmas encountered in clinical practice. These committees play distinct yet complementary roles in promoting ethical conduct and upholding ethical standards within healthcare settings [405].

Various approaches to research ethics review are employed across different countries. In some Member States, the review process may occur solely at the institutional level, while in others, it may take place at both national and institutional levels. Additionally, certain countries may conduct reviews at a regional level. These diverse approaches reflect the range of mechanisms utilised to ensure the ethical oversight of research activities within specific jurisdictions.

The Declaration of Helsinki, Good Clinical Practice Guidelines, CIOMS, Clinical Trials Regulation (CTR), and other international and national instruments, such as the Oviedo Convention, mandate the ethical review of research before its initiation. Researchers are obligated to submit their proposals for ethical review before commencing any research involving human participants. Depending on the nature and context of the research, additional layers of review and scrutiny may be required, as stipulated by the national laws of Member States. This comprehensive ethical review process ensures the protection of participants' rights, safety, and welfare, as well as upholding the integrity and quality of research conducted.

The implementation of requirements outlined in international declarations to protect research participants varies across different countries and types of research. However, these implementations typically incorporate two critical elements: peer review of the proposed study protocol and ethical review by an independent research ethics committee (REC) or institutional review board (IRB). Peer review involves the evaluation of the study protocol by experts in the field to assess its scientific merit, methodological rigour, and feasibility. An ethical review conducted by an REC or IRB focuses on ensuring that the study adheres to ethical principles and safeguards the

Funded by Horizon Europe Framework Programme of the European Union

rights, welfare, and dignity of research participants [406]. For instance, the Declaration of Helsinki mandates that the design and performance of each research study involving human subjects must be clearly described and justified in a research protocol and that draft research protocols undergo review by an independent ethics committee. This requirement is applicable to all medical research involving human participants, irrespective of their age. More specifically, Article 23 of the Declaration of Helsinki sets out that:

> *"Research protocol must be submitted for consideration, comment, guidance and approval to the concerned research ethics committee before the study begins. This committee must be transparent in its functioning, must be independent of the researcher, the sponsor and any other undue influence and must be duly qualified. It must take into consideration the laws and regulations of the country or countries in which the research is to be performed as well as applicable international norms and standards but these must not be allowed to reduce or eliminate any of the protections for research subjects set forth in this Declaration."*

It is important to note that the Helsinki Declaration is the ethical standard for the International Committee of Medical Journal Editors [407] "When reporting experiments on human subjects, authors should indicate whether the procedures followed were in accordance with the ethical standards of the responsible committee on human experimentation (institutional and national) and with the Helsinki Declaration" [408]. Therefore, in addition to ethical concerns, failure to adhere to the requirements outlined in the Declaration of Helsinki can hinder the publication of research findings. The prime example is a rejection of several French observational studies by US peer-reviewed journals because their protocols have not been submitted to an Institutional Review Board/Independent Ethics Committee (IRB/IEC) [409].

Likewise, CIOMS mandates that all proposals for health-related research involving humans must undergo submission to a research ethics committee (Guideline 23). This requirement underscores the importance of ethical review in ensuring the protection of participants' rights and welfare, as well as upholding ethical standards in research conduct. The CIOMS specifies that:

> *"All proposals to conduct health-related research involving humans must be submitted to a research ethics committee to determine whether they qualify for ethical review and to assess their ethical acceptability unless they qualify for an exemption from ethical review (which may depend upon the nature of the research and upon applicable law or regulations). The researcher must obtain approval or clearance from such a committee before beginning the research. The research ethics committee should conduct further reviews as necessary, for example, when there are significant changes in the protocol."*

The ICH Good Clinical Practice (GCP) guidelines provide guidance on the operation of an Ethics Committee (EC) and delineate its responsibilities. These guidelines

Funded by Horizon Europe Framework Programme of the European Union

address various aspects, including the composition, function, operations, procedures, responsibilities, record-keeping, contents of informed consent, and reporting of adverse events. Furthermore, the ICH GCP states:

> "A trial should be conducted in compliance with the protocol that has received prior institutional review board (IRB)/independent ethics committee (IEC) approval/favourable opinion."

From the discussion above, it can be noted that no single human research ethics guide can provide universal answers to all ethical issues, nor can a single guide reflect the large diversity of legal requirements. Moreover, the significant challenge is how to translate various legal and ethical requirements into real-life scenarios. However, some important recommendations should be taken into account.

- Firstly, all types of medical research involving humans always require an independent ethics review before the study begins. Obtaining ethical approval, particularly in medical sciences, should be an inherent moral obligation for researchers.
- Secondly, in order to comply with the best practices, assent should be requested whenever it is necessary to make a decision involving the health and well-being of the minor. Participation in clinical research should always be grounded on informed consent, as explained above. Moreover, in order to comply with the best practices, assent should be requested whenever it is necessary to make a decision involving the health and well-being of the minor.
- In situations where tensions or clear contradictions arise among the provisions of various guidelines pertaining to clinical research, conflicts should be resolved by striking a balance between competing principles. This should be done while prioritising the "highest ethical standards," which offer greater assurances, with the overarching goal of safeguarding the health and rights of the child.
- In that sense, ethical principles ethical principles in biomedical ethics, namely beneficence, non-maleficence, respect for autonomy and justice, should be fundamental guiding principles in conducting any clinical research.

Funded by Horizon Europe Framework Programme of the European Union

7 Conclusion

The purpose of deliverable D2.2 (developed in the context of task T2.2) is to comprehensively analyse the applicable legal and ethical framework within the context of CYLCOMED design. In other words, it aims to provide the recommendations and input for the WP4 “Risk Management for CMDs”, WP5 “Cybersecurity Toolbox Design and Implementation”, and WP6 “Integration and Validation with Real-world Applications”, as well as guidance for legal and ethical compliance. It elaborates on various legal and ethical frameworks applicable to developing the CYLCOMED cybersecurity toolbox and implementing CYLCOMED pilots. Moreover, it seeks to provide recommendations for the CYLCOMED Consortium partners to facilitate overall legal and ethical compliance.

This deliverable highlighted the extensive and diverse range of EU policy initiatives relevant to the CYLCOMED ecosystem. The Ethical and Legal Inventory focused on six key themes pertinent to CYLCOMED: privacy and data protection, regulatory frameworks for cybersecurity, regulatory frameworks for medical devices, artificial intelligence, and ethics in clinical studies.

Chapter 2 elaborated on the requirements applicable to the processing of personal data under the GDPR. It explained the conditions for processing personal data, including the legal bases and situations allowing the processing of health-related data, emphasising the importance of adhering to GDPR requirements for the CYLCOMED project.

Chapters 3 and 4 aimed to capture the essence of regulatory frameworks governing the cybersecurity of medical devices, acknowledging the complexity arising from various legislative frameworks potentially falling within the project's scope.

Chapter 5 provided an overview of AI governance in the EU, mainly focusing on the AI Act and its obligations regarding CYLCOMED tools. It highlighted the significance of ethical principles such as human oversight, transparency, and accountability in designing and developing AI-based technologies.

Emphasising the fundamental role of ethics in the CYLCOMED project, consortium members were urged to uphold ethical norms throughout developing technical solutions. Hence, Chapter 6 outlined the primary sources of EU guidance and requirements regarding clinical trials and research ethics, stressing the importance of adhering to ethical principles, including human dignity, protection of health and research integrity.

Given the dynamic legal landscape and ongoing development of CYLCOMED technical solutions, this deliverable is not a one-time effort but serves as a foundational step in legal research. It lays the groundwork for forthcoming ethical and legal studies deliverables, aiming to provide targeted guidance to partners and draw regulatory conclusions from interdisciplinary research within CYLCOMED.

Funded by Horizon Europe Framework Programme of the European Union

References

[1] CYLCOMED, “D2.1 Analysis of Ethical, Legal and Data Protection Frameworks”, 2023.

[2] CYLCOMED, “D5.1 CYLCOMED toolbox prototype”, 2024.

[3] CYLCOMED, “D6.1 Pilot planning and evaluation strategy incl. clinical trial submission package”, 2023.

[4] CYLCOMED, “D5.1 CYLCOMED toolbox prototype”, 2024.

[5] CYLCOMED, “D6.1 Pilot planning and evaluation strategy incl. clinical trial submission package”, 2023.

[6] 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

[7] 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

[8] Supra note [4].

[9] 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

[10] 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

[11] 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.

[12] Ibid.

[13] European Commission. July 2021. “Ethics and data protection”. Available at: ethics-and-data-protection_he_en.pdf (europa.eu)

[14] 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.

[15] Article 29 Working Party, “Opinion 4/2007 on the concept of personal data” (2007) 01248/07/EN.

[16] Supra note [13], p6.

[17] Judgment of 17 July 2014, YS and Others, C-141/12 and C-372/12, EU:C:2014:2081, paragraph 38.

[18] Judgment of 6 November 2003, Lindqvist, C-101/01, EU:C:2003:596.

[19] Judgment of 19 October 2016, Breyer C-582/14, EU:C:2016:779.

[20] Judgment of 17 October 2013, Schwarz, C-291/12, EU:C:2013:670.

[21] Judgment of the Court of 20 May 2003, Rechnungshof, C-465/00, C-138/01 and C-139/01, EU:C:2003:294.

[22] Supra note [13].

[23] Supra note [13], p9.

[24] Supra note [13], p12.

Funded by Horizon Europe Framework Programme of the European Union

[25] Bargiotti, Leda, Inge Gielis, Bram Verdegem, Pieter Breyne, Francesco Pignatelli, Paul Smits, and Ray Boguslawski. *Guidelines for public administrations on location privacy: European Union Location Framework*. No. JRC103110. Joint Research Centre (Seville site), 2016.

[26] Recital 26 GDPR

[27] Information Commissioner's Office (ICO) Guide. October, 2022. "What is personal data?". Available at: what-is-personal-data-1-0.pdf (ico.org.uk)

[28] Recital 27 GDPR

[29] Judgment of 9 November 2010, Schecke, C-92/09, EU:C:2010:662, paragraph 53.

[30] Recital 27 sentence 2 GDPR

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

[32] WP29, Advice paper on special categories of data ("sensitive data"), April 2011; WP29, Annex to Letter from the WP29 to the European Commission, DG CONNECT on mHealth, 5 February 2015.

[33] Judgment of 13 May 2014, Google Spain SL, C-131/12, EU:C:2014:317, paragraph 28.

[34] Judgment of 10 July 2018, Jehovan Todistajat, C-25/17, EU:C:2018:551, paragraph 55.

[35] 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)

[36] Supra note [33].

[37] Information Commissioner's Office (ICO) Guide. 17 October 2022. "Controllers and Processors". Available at: Controllers and processors | ICO

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

[39] Supra note [32], paragraph 75.

[40] Supra note [33], p24.

[41] Supra note [33].

[42] Supra note [33].

[43] Article 28(10) GDPR.

[44] Supra note [33], p30.

[45] Supra note [33], p32

[46] Supra note [33], p33

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

[48] 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

[49] Supra note [46], p12.

[50] Recital 39 GDPR.

[51] Supra note [46], p15.

[52]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

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

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

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

Funded by Horizon Europe Framework Programme of the European Union

[57] Data Protection Commission. "Guidance on Anonymisation and Pseudonymisation." *Retrieved November* 7, no. 2019 (2019): 2019-06.

[58] Article 29 Working Party. April 2014. „Opinion 05/2014 on Anonymisation Techniques".

[59] Supra note [56].

[60] EDPB. February, 2021. "Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research".

[61] Information Commissioner's Office (ICO) Guide. October, 2022. "Introduction to anonymisation: Draft anonymisation, pseudonymisation and privacy enhancing technologies guidance."

[62] Supra note [56].

[63] Ohm, Paul. "Broken promises of privacy: Responding to the surprising failure of anonymization." *UCLA l. Rev.* 57 (2009): 1701.

[64] ENISA. December, 2019. "Pseudonymisation techniques and best practices".

[65] GDPR Article 4(5),

[66] ENISA. January, 2019. "Recommendations on shaping technology according to GDPR provisions - An overview on data pseudonymisation".

[67] Council of Europe, Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 2018, para. 18.

[68] Supra note [62].

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

[70] 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).

[71] Recital 46 GDPR.

[72] Recital 45 GDPR.

[73] 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

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

[75] Recital 42 GDPR.

[76] Recital 32 GDPR

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

[78] Article 7(3) GDPR.

[79] Supra note [75].

[80] Cole, A. and Towse, A. (2018) Legal barriers to the better use of health data to deliver pharmaceutical innovation. OHE Consulting Report, London: Office of Health Economics.

[81] EDPB. February, 2021. "Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research".

[82] GDPR Recital 159.

[83] Taylor Wessing. March, 2023 "Data Protection Law in Clinical Trials –Local Country Report". Available at: tw23_data-protection-law_local-country-report_en_230418.pdf (taylorwessing.com)

[84] Supra note [81].

[85] Supra note [75].

[86] EDPB Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials

Funded by Horizon Europe Framework Programme of the European Union

[87] The European Data Protection Supervisor (EDPS). January, 2020. “Preliminary Opinion on Data Protection and Scientific Research”.

[88] EDPB. February, 2021. “Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research”.

[89] European Commission. “Question and Answers on the interplay between the Clinical Trials Regulation and the General Data Protection Regulation”.

[90] Supra note [84].

[91] Supra note [87].

[92] Supra note [87].

[93] Article 29 Working Party. April, 2018. “Guidelines on consent under Regulation 2016/679”.

[94] GDPR Article 8(1).

[95] Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (codification) (Text with EEA relevance). Available at: Directive - 2015/1535 - EN - EUR-Lex (europa.eu)

[96] Tosoni, Luca. "Article 4 (25). Information society service." In The EU General Data Protection Regulation (GDPR). Oxford University Press.

[97] Supra note [93], Annex I, p10.

[98] Information Commissioner’s Office (ICO) Guide. March, 2018. “Children and the GDPR”.

[99] Supra note [75], p27.

[100] Supra note [75].

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

[102] Article 12(1) GDPR

[103] EDPB. April 2018. “Guidelines on Transparency under Regulation 2016/679”, p12.

[104] Supra note [101], p12.

[105] Supra note [101].

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

[107] GDPR Recital 58

[108] Supra note [101].

[109] Article 8 (2).

[110] GDPR Recital 63.

[111] Supra note [108].

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

[113] GDPR Recital 63.

[114] Supra note [110], p28.

[115] Supra note [110], p43.

[116] Supra note [110], p43.

[117] GDPR Article 12(5).

[118] GDPR Article 15(4)

[119] GDPR Article 23.

[120] Judgment of 13 May 2014, Google Spain SL, C-131/12, EU:C:2014:317

Funded by Horizon Europe Framework Programme of the European Union

[122] GDPR, Article 18(2).

[123] WP29 "Guidelines on the right to data portability", p18.

[124] GDPR Recital 68.

[125] European Parliamentary Research Service 'The impact of the General Data Protection Regulation (GDPR) on artificial intelligence' (2020), p. 57.

[126] GDPR Article 21(1).

[127] GDPR Article 21(3).

[128] GDPR Article 21(5).

[129] GDPR Article 21(6).

[130] GDPR, Article 21(2).

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

[132] Supra note [129], p6.

[133] Information Commissioner's Office (ICO) Guide. October, 2022. "Automated decision-making and profiling".

[134] GDPR, Article 22(4)

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

[136] Supra note [133], p. 6

[137] Supra note [133], p. 7

[138] Supra note [133].

[139] See for more Recital 91 GDPR.

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

[141] 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

[142] Article 35(1) and (2) GDPR. It is the obligation of the data controller and data processor to ensure that the data protection officer is involved – properly and in a timely manner – in all issues in relation to the protection of personal data (see Article 38 (1) GDPR).

[143] Supra note [139], p.9.

[144] Supra note [139], p7-9.

[145] GDPR Recital 75.

[146] Supra note [139], p.9.

[147] The national trade association of the pharmaceutical industry in Spain (Farmaindustria). February 2022. Code of Conduct Regulating the Processing of Personal Data in Clinical Trials and Other Clinical Research and Pharmacovigilance Activities.

[148] GDPR Article 36(1).

[149] Dara Hallinan, Nicholas Martin, "*Fundamental Rights, the Normative Keystone of DPIA*", European Data Protection Law Review, Volume 6 (2020), Issue 2, pp. 178-193.

[150] EU Fundamental Rights Agency (FRA), "*Getting The Future Right Artificial Intelligence And Fundamental Rights*", 2021, https://staging.fra.europa.eu/sites/default/files/fra_uploads/fra-2021-artificial-intelligence-summary_en.pdf , p.6.

[151] "*Entities using facial recognition technologies have to carry out impact assessments prior to the processing, as the use of these technologies involves the processing of biometric data and presents high risks for the fundamental*

Funded by Horizon Europe Framework Programme of the European Union

[152] WORKING PARTY 29 POSITION PAPER on the derogations from the obligation to maintain records of processing activities pursuant to Article 30(5) GDPR.

[153] GDPR Recital 85.

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

[155] GDPR Article 34.

[156] 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

[157] 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

[158] Explanatory memorandum p1.

[159] Article 1(3)(a) EHDS proposal

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

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

[162] EDHS Article 44.

[163] EDHS Article 36.

[164] EDHS Articles 56, 57 and 58.

[165] Fåhraeus, David, Jane Reichel, and Santa Slokenberga. "The European Health Data Space: Challenges and Opportunities." (2024).

[166] Marelli, Luca, Marthe Stevens, Tamar Sharon, Ine Van Hoyweghen, Martin Boeckhout, Ilaria Colussi, Alexander Degelsegger-Márquez et al. "The European health data space: Too big to succeed?." *Health policy* 135 (2023): 104861.

[167] Supra note [164].

[168] Supra note [164].

[169] EDHS Article 3(9).

[170] EDHS Article 4(4)

[171] Supra note [163].

[172]Marcus, J.S. et al., 2022, The European Health Data Space, Publication for the committee on Industry, Research and Energy (ITRE), Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg.

[173] EDPB-EDPS Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space. July 2022. Available at: https://www.edps.europa.eu/system/files/2023-04/22-07-12_edpb_edps_joint-opinion_europeanhealthdataspace_en.pdf

[174] Biasin, Elisabetta, Burcu Yasar, and Erik Kamenjasevic. "New cybersecurity requirements for medical devices in the eu: the forthcoming european health data space, data act, and artificial intelligence act." *Law, Tech. & Hum.* 5 (2023): 43.

[175] EDHS Article 2(2)(m).

[176] EDHS Article 2(2)(n).

[177] Supra note [172].

[178] Konnoth, Craig. "Are Electronic Health Records Medical Devices?" Chapter. In *The Future of Medical Device Regulation: Innovation and Protection*, edited by I. Glenn Cohen, Timo Minssen, W. Nicholson Price II, Christopher

[179] European Coordination Committee of the Radiological, Electromedical and Healthcare IT Industry (COCIR). "COCIR Feedback – Proposal for a European Health Data Space." July 27, 2022. Available at: https://www.cocir.org/fileadmin/Position_Papers_2022/20220727_COCIR_Feedback_EHDS.pdf

[180] European Coordination Committee of the Radiological, Electromedical and Healthcare IT Industry (COCIR). "COCIR Feedback – Proposal for a European Health Data Space." July 27, 2022. Available at: https://www.cocir.org/fileadmin/Position_Papers_2022/20220727_COCIR_Feedback_EHDS.pdf p. 3.

[181] MedTech Europe. "MedTech Europe's Position on the Proposed European Health Data Space Regulation," February 22, 2023.

[182] EDPB-EDPS Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space. July 2022. Available at: https://www.edps.europa.eu/system/files/2023-04/22-07-12_edpb_edps_joint-opinion_europeanhealthdataspace_en.pdf

[183] Terzis, Petros, and O. E. Santamaria Echeverria. "Interoperability and governance in the European Health Data Space regulation." *Medical Law International* 23, no. 4 (2023): 368-376.

[184] Kiseleva, Anastasiya, and Paul De Hert. "Creating a European Health Data Space: obstacles in four key legal area." *EPLR* 5 (2021): 21.

[185] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act).

[186] European Parliament. May, 2023. EU Legislation in progress, Briefing: Data Act.

[187] European Commission "Data Act explained". Available at: Data Act explained | Shaping Europe's digital future (europa.eu)

[188] Supra note [185]

[189] Colangelo, Giuseppe. "European Proposal for a Data Act–A First Assessment." *CERRE Evaluation Paper* (2022).

[190] Supra note [187].

[191] Data Act Article 2(5)

[192] Data Act Recital 17.

[193] Data Act Recital 6.

[194] Biasin, Elisabetta. "The Data Act will concern eHealth apps and Medical Devices" Blog Post, 19 MAY 2022. Available at: The Data Act will concern eHealth apps and Medical Devices - CiTiP blog (kuleuven.be)

[195] CMS Law-Now^{tm}. January, 2024. "Adapting to the new EU Data Act: implications for medical devices and other health devices"

[196] Recital 14 of Data Act.

[197] Supra note [193].

[198] Supra note [192].

[199] Kerber, Wolfgang. "Governance of IoT Data: Why the EU Data Act Will Not Fulfill Its Objectives." GRUR International 72, no. 2 (2023): 120-135.

[200] Recital 8 of Data Act.

[201] Supra note [193].

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

[203] 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

[204] 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

[205] 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

[206] 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)

[207] Casarosa, F. Cybersecurity certification of Artificial Intelligence: a missed opportunity to coordinate between the Artificial Intelligence Act and the Cybersecurity Act. *Int. Cybersecur. Law Rev.* **3**, 115–130 (2022).

[208] CSA Article 5.

[209] CSA Article 6.

[210] CSA Article 7.

[211] CSA Article 8.

[212] CSA Article 9.

[213] Kohler, C. The EU Cybersecurity Act and European standards: an introduction to the role of European standardization. *Int. Cybersecur. Law Rev.* **1**, 7–12 (2020).

[214] CSA Recital 69.

[215] CSA Article 46.

[216] CSA Article 52(1).

[217] CSA Article 54.

[218] CSA Recital 86.

[219] CSA Recital 88.

[220] CSA Recital 89.

[221] A. Khurshid, R. Alsaaidi, M. Aslam and S. Raza, "EU Cybersecurity Act and IoT Certification: Landscape, Perspective and a Proposed Template Scheme," in IEEE Access, vol. 10, pp. 129932-129948, 2022.

[222] Casarosa, F. Cybersecurity certification of Artificial Intelligence: a missed opportunity to coordinate between the Artificial Intelligence Act and the Cybersecurity Act. Int. Cybersecur. Law Rev. 3, 115–130 (2022).

[223] CSA Article 56(2).

[224] EU Cybersecurity Certification Framework. Available: https://www.enisa.europa.eu/topics/standards/certification

[225] European Commission Implementing Regulation on the adoption of a European Common Criteria-based cybersecurity certification scheme laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC).

[226] EUCC Recital 1.

[227] EUCC Article 4.

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

[229] 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).

[230] 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 &

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

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

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

[234] 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

[235] 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)

[236] 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)

[237] 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

[238] European Parliamentary Research Service (EPRS)(2023). The NIS2 Directive: A high common level of cybersecurity in the EU. The 'EU Legislationin Progress' briefing 2023-02-08. BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf

[239] 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)**

[240] 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)

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

[242] 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).

[243] 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, 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."

[244] 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).

[245] 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).

[246] Supra note [233].

[247] Supra note [233].

[248] CISCO Public White Paper. May, 2023. "Transforming NIS2 Challenges into Strategic Opportunities:A Cisco Perspective". Available at: EU_NIS2_white_paper_080124 (cisco.com)

[249] Supra note [246].

[250] NIS2 Article 24.

[251] NIS2 Article 41.

Funded by Horizon Europe Framework Programme of the European Union

[253] 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

[254] RED Article 2(1)(1).

[255] 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

[256] RED Article 1(3).

[257] RED Article 3(1)(2).

[258] 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)

[259] Supra note [256], p. 72.

[260] 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)

[261] RED Delegated Act, Art 1(1).

[262] RED Delegated Act 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.

[263] 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

[264] European Commission. March, 2024. “Second Report on the operation of Radio Equipment Directive 2014/53/EU”.

[265] European Commission. October, 2021. “Questions and Answers: Strengthening cybersecurity of wireless devices and products.”

[266] 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.

[267] ENISA ADVISORY GROUP. September, 2019. “Opinion Consumers and IoT security”. Available at: final-opinion-enisa-ag-consumer-iot-perspective-09.2019 (europa.eu)

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

[269] European Parliament. Novemberm 2023. EU Legislation in progress -Briefing. Cyber Resilience Act. p.4

[270] CRA Explanatory memorandum.

[271] CRA Article 2(2).

[272] The European Data Protection Supervisor (EDPS). November, 2022. “Opinion 23/2022 on the 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.

[273] CRA Article 2(7)

[274] CRA Article 7(2)

[275] For more see Annex IV.

[276] CRA Article 13(2).

[277] CRA Article 14(8).

[278]

Funded by Horizon Europe Framework Programme of the European Union

[279] Shatrov, Kosta, and Carl R. Blankart. "After the Four-year Transition Period: Is the European Union's Medical Device Regulation of 2017 Likely to Achieve Its Main Goals?" Health Policy 126, no. 12 (2022): 1233-1240.

[280] MDR Article 1.

[281] 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

[282] LUDVIGSEN, Kaspar, Shishir NAGARAJA, and Angela DALY. "When Is Software a Medical Device? Understanding and Determining the 'Intention' and Requirements for Software as a Medical Device in European Union Law." *European Journal of Risk Regulation* 13, no. 1 (2022): 78–93. https://doi.org/10.1017/err.2021.45.

[283] Tang, Antony, Aldeida Aleti, Janet Burge, and Hans van Vliet. "What makes software design effective?." *Design Studies* 31, no. 6 (2010): 614-640.

[284] The Medical Device Coordination Group (MDCG), established under the Article 103 of MDR, serves as a new body facilitating collaboration among various regulators. However, it is important to note that the MDCG is not the central authority on its own.

[285] 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)

[286] Judgment of the Court of 7 December 2017, Snitem, Case C-329/16, ECLI:EU:C:2017:947.

[287] Timo Minssen, Marc Mimler, Vivian Mak, When Does Stand-Alone Software Qualify as a Medical Device in the European Union?—The Cjeu's Decision in *Snitem* and What it Implies for the Next Generation of Medical Devices, *Medical Law Review*, Volume 28, Issue 3, Summer 2020, Pages 615–624, https://doi.org/10.1093/medlaw/fwaa012

[288] 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.

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

[290] 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

[291] MDR Article 2(65).

[292] MDR Article 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;"

[293] 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).

[294] IVDR Article 1(1).

[295] 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

[296] Medical Device Coordination Group. December, 2019. "Guidance on Cybersecurity for medical devices". (MDCG 2019-16 Rev.1). Available at: md_cybersecurity_en.pdf (europa.eu)

[297] 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

[298] Supra note [295], p1.

Funded by Horizon Europe Framework Programme of the European Union

[299] Supra note [294].

[300] 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

[301] Supra note [294].

[302] 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

[303] Milojevic, Dusko. "Is it time to update the Medical Device Coordination Group's Guidance on Cybersecurity for Medical Devices?" Blog Post, 14 NOVEMBER 2023. Available at: Is it time to update the Medical Device Coordination Group's Guidance on Cybersecurity for Medical Devices? - CiTiP blog (kuleuven.be)

[304] 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

[305] Vallor et al. "An Introduction to Cybersecurity Ethics". Available at: IntroToCybersecurityEthics.pdf (scu.edu)

[306] Milojevic, Dusko. "Is it time to update the Medical Device Coordination Group's Guidance on Cybersecurity for Medical Devices?" Blog Post, 14 NOVEMBER 2023. Available at: Is it time to update the Medical Device Coordination Group's Guidance on Cybersecurity for Medical Devices? - CiTiP blog (kuleuven.be)

[307] Milojevic, Dusko. "Is it time to update the Medical Device Coordination Group's Guidance on Cybersecurity for Medical Devices?" Blog Post, 14 NOVEMBER 2023. Available at: Is it time to update the Medical Device Coordination Group's Guidance on Cybersecurity for Medical Devices? - CiTiP blog (kuleuven.be)

[308] *EU Parliament proposed to change the notion of "user" to "deployers".*

[309] M. Veale & F. Borgesius, "Demystifying the Draft EU Artificial Intelligence Act", *CRI* 2021, 97-112; European Commission, "Regulatory framework proposal on artificial intelligence", 29 September 2022, https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai.

[310] *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*

[311] 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.

[312] 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

[313] Supra note [310], p4.

[314] Supra note [310].

[315] Supra note [310].

[316] Supra note [310], p10-11.

[317] Supra note [310], p11-13.

[318] Supra note [310].

[319] 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

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

[321] European union Agency for Cybersecurity, "Multilayer Framework for Good Cybersecurity Practices for AI", June 2023.

[322] *Ibid, p. 11.*

Funded by Horizon Europe Framework Programme of the European Union

[323] Ibid, p14.

[324] Ibid, p14.

[325] Altavilla, Annagrazia. "Ethical key issues and fundamental rights in paediatric research." *European journal of clinical pharmacology* 67 (2011): 117-123.

[326] Bioethics, Nuffield Council. "Children and clinical research: ethical issues." *London: Nuffield Council on Bioethics* (2015).

[327] Ward, R. M., and S. E. Kern. "Clinical trials in neonates: a therapeutic imperative." *Clinical Pharmacology & Therapeutics* 86, no. 6 (2009): 585-587.

[328] Muurling, Marijn, Anna MG Pasmooij, Ivan Koychev, Dora Roik, Lutz Froelich, Emilia Schwertner, Dorota Religa et al. "Ethical challenges of using remote monitoring technologies for clinical research: A case study of the role of local research ethics committees in the RADAR-AD study." *Plos one* 18, no. 7 (2023): e0285807.

[329] Ienca, Marcello, Agata Ferretti, Samia Hurst, Milo Puhan, Christian Lovis, and Effy Vayena. "Considerations for ethics review of big data health research: A scoping review." PloS one 13, no. 10 (2018): e0204937.

[330] Martinez-Martin, Nicole, Zelun Luo, Amit Kaushal, Ehsan Adeli, Albert Haque, Sara S. Kelly, Sarah Wieten et al. "Ethical issues in using ambient intelligence in health-care settings." The lancet digital health 3, no. 2 (2021): e115-e123.

[331] Bos, Wendy, Krista Tromp, Dick Tibboel, and Wim Pinxten. "Ethical aspects of clinical research with minors." European journal of pediatrics 172 (2013): 859-866.

[332] Supra note [323].

[333] Levesque, Roger JR, ed. Encyclopedia of adolescence. Springer Science & Business Media, 2011.

[334] Supra note [329].

[335] Resnik, David B. *The ethics of research with human subjects: Protecting people, advancing science, promoting trust*. Vol. 74. Springer, 2018.

[336] Supra note [329].

[337] Cotrim, Hortense, Cristina Granja, Ana Sofia Carvalho, Carlos Cotrim, and Rui Martins. "Children's understanding of informed assents in research studies." In Healthcare, vol. 9, no. 7, p. 871. MDPI, 2021.

[338] Unguru, Yoram. "Pediatric decision-making: informed consent, parental permission, and child assent." *Clinical ethics in pediatrics: A case-based textbook* (2011): 1-6.

[339] Supra note [335].

[340] Roth-Cline, M., Gerson, J., Bright, P., Lee, C. S., & Nelson, R. M. (2011). Ethical considerations in conducting pediatric research. *Handbook of experimental pharmacology*, *205*, 219–244. https://doi.org/10.1007/978-3-642-20195-0_11

[341] Modi, Neena, Jyotsna Vohra, Jennifer Preston, Catherine Elliott, William Van't Hoff, Jane Coad, Faith Gibson et al. "Guidance on clinical research involving infants, children and young people: an update for researchers and research ethics committees." Archives of disease in childhood 99, no. 10 (2014): 887-891.

[342] Varkey B. (2021). Principles of Clinical Ethics and Their Application to Practice. Medical principles and practice : international journal of the Kuwait University, Health Science Centre, 30(1), 17–28.

[343] Beauchamp, Tom L., and James F. Childress. Principles of biomedical ethics. Oxford University Press, USA, 2001.

[344] Tom L. Beauchamp, James F. Childress (2013) Principles of Biomedical Ethics, 7th Edition.

[345] Supra note [323].

[346] Supra note [340].

[347] Supra note [342].

[348] Supra note [323].

Funded by Horizon Europe Framework Programme of the European Union

[350] Supra note [342].

[351] Supra note [323].

[352] Supra note [340].

[353] Supra note [342].

[354] Supra note [323].

[355] Supra note [340].

[356] Supra note [323].

[357] Schmidt, Ulf. *History and theory of human experimentation: the declaration of Helsinki and modern medical ethics*. Vol. 2. Franz Steiner Verlag, 2007.

[358] Macklin, R. "Future challenges for the Declaration of Helsinki: Maintaining credibility in the face of ethical controversies." Address to Scientific Session, World Medical Association General Assembly (2003).

[359] Crawley, F. P. "The limits of the declaration of Helsinki." *Address to Scientific Session. World Medical Association General Assembly: Helsinki* (2012).

[360] World Medical Association Declaration of Helsinki – Ethical Principles for Medical Research Involving Human Subjects. Available at: WMA Declaration of Helsinki – Ethical Principles for Medical Research Involving Human Subjects – WMA – The World Medical Association

[361] 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

[362] 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.

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

[364] Mentz, Robert J., Adrian F. Hernandez, Lisa G. Berdan, Tyrus Rorick, Emily C. O'Brien, Jenny C. Ibarra, Lesley H. Curtis, and Eric D. Peterson. "Good clinical practice guidance and pragmatic clinical trials: balancing the best of both worlds." *Circulation* 133, no. 9 (2016): 872-880.

[365] World Health Organization. "Handbook for good clinical research practice (GCP): guidance for implementation." (2005).

[366] Castelino, Lovely Joylen, V. Anoop Narayanan, Swapnil Dylan Fernandes, Pankaj Kumar, and D. S. Sandeep. "Good clinical practices: an Indian perspective." *Research journal of Pharmacy and Technology* 11, no. 7 (2018): 3209-3215.

[367] Switula, Dorota. "Principles of good clinical practice (GCP) in clinical research." *Science and engineering ethics* 6, no. 1 (2000): 71-77.

[368] Council for International Organizations of Medical Sciences. "International ethical guidelines for health-related research involving humans." (2016). Available at: 2016 International ethical guidelines for health-related research involving humans - CIOMS

[369] Williams, J. R. "The 2016 CIOMS guidelines and public-health research ethics." *South African Journal of Bioethics and Law* 10, no. 2 (2017): 93-95.

[370] Macrae, Duncan J. "The Council for International Organizations and Medical Sciences (CIOMS) guidelines on ethics of clinical trials." *Proceedings of the American thoracic society* 4, no. 2 (2007): 176-179.

[371] European Union. 2001. 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: Directive - 2001/20 - EN - EUR-Lex (europa.eu)

Funded by Horizon Europe Framework Programme of the European Union

[372] European Commission. 2012. “Impact assessment report on the revision of the “Clinical Trials Directive” 2001/20/E”. Available at: https://health.ec.europa.eu/system/files/2016-11/impact_assessment_part1_en_0.pdf

[373] Ibid, CTR Recital 82

[374] European Commission. “Guidance for the Transition of Clinical Trials from the Clinical Trials Directive to the Clinical Trials Regulation”. 21 December 2023. Available at: 10c83e6b-2587-420d-9204-d49c2f75f476_en (europa.eu)

[375] EMA Clinical Trials Information System (CTIS): online modular training programme. Available at: Clinical Trials Information System (CTIS): online training modules | European Medicines Agency (europa.eu)

[376] EMA Clinical Trials Information System (CTIS) – Sponsor Handbook. Available at: CTIS Sponsor Handbook 2023_v.3.03_DRAFT (europa.eu)

[377] Overview structured data CTIS. Available at: clinical-trial-information-system-ctis-structured-data-form-initial-application-additional-member-state-concerned-substantial-modification-non-substantial-modification_en.xlsx (live.com)

[378] Bioethics, Nuffield Council. "Children and clinical research: ethical issues." London: ESP Colour Ltd (2015).

[379] Röhrig, Bernd, Jean-Baptist Du Prel, Daniel Wachtlin, and Maria Blettner. "Types of study in medical research: part 3 of a series on evaluation of scientific publications." Deutsches Arzteblatt International 106, no. 15 (2009): 262.

[380] Muthuswamy, Vasantha. "Ethical issues in clinical research." Perspectives in clinical research 4, no. 1 (2013): 9-13.

[381] 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.

[382] Working Group on Cosmetic Products. November 2023. “Manual of the Working group on cosmetic products (sub-group on borderline products) on the scope of application of the cosmetics regulation (EC) No 1223/2009”. Available at: Borderline products - European Commission (europa.eu)

[383] Borderline and Classification Working Group. December 2022. “Manual on borderline and classification for medical devices under Regulation (EU) 2017/745 on medical devices and Regulation (EU) 2017/746 on in vitro diagnostic medical devices”. Available at: md_borderline_manual_12-2022_en.pdf (europa.eu)

[384] Expert Group on Clinical Trials. March 2024. “The rules governing medicinal products in the European Union VOLUME 10 - Guidance documents applying to clinical trials”. Available at: EudraLex - Volume 10 - European Commission (europa.eu)

[385] Ramirez, Isabelle. "Navigating the maze of requirements for obtaining approval of non-interventional studies (NIS) in the European Union." GMS German Medical Science 13 (2015).

[386] European Commission expert group on clinical trials. “Ethical considerations for clinical trials on medicinal products conducted with minors”. 18 September 2017. Available at: 2017_09_18_ethical_consid_ct_with_minors_0.pdf (europa.eu)

[387] CTR Article 29(2)(b)

[388] CTR Article 32(1)(b)

[389] CTR Article 32(2).

[390] CTR Article 29(8).

[391] CTR Article 32(1)(c).

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

[393] Supra note [390], p1.

[394] Supra note [390].

[395] European Commission Expert group on clinical trials for the implementation of Regulation (EU) No 536/2014 on

Funded by Horizon Europe Framework Programme of the European Union

medicinal products conducted with minors". Available at: 2017_09_18_ethical_consid_ct_with_minors_0.pdf (europa.eu)

[396] Supra note [393].

[397] Supra note [393].

[398] Leibson, T., & Koren, G. (2015). Informed consent in pediatric research. *Paediatric drugs*, *17*(1), 5–11.

[399] The European network of paediatric research at the European medicines Agency (Enpr-EMA). January 2021. "*Assent / Informed Consent Guidance for Paediatric Clinical Trials with Medicinal Products in Europe*". Available at: Enpr-EMA Assent_Consent Guidance Document_VERSION 8_15.11.2019_final_pf (europa.eu)

[400] Lepola, Pirkko, Maxine Kindred, Viviana Giannuzzi, Heidi Glosli, Martine Dehlinger-Kremer, Harris Dalrymple, David Neubauer et al. "Informed consent and assent guide for paediatric clinical trials in Europe." *Archives of Disease in Childhood* 107, no. 6 (2022): 582-590.

[401] Gabriel, André P., and Charles P. Mercado. "Data retention after a patient withdraws consent in clinical trials." *Open access Journal of clinical trials* (2011): 15-19.

[402] European Commission Expert group on clinical trials for the implementation of Regulation (EU) No 536/2014 on clinical trials on medicinal products for human use. September 2017. "Ethical considerations for clinical trials on medicinal products conducted with minors". Available at: 2017_09_18_ethical_consid_ct_with_minors_0.pdf (europa.eu)

[403] Mehta, Pankti, Olena Zimba, Armen Yuri Gasparyan, Birzhan Seiil, and Marlen Yessirkepov. "Ethics committees: structure, roles, and issues." *Journal of Korean Medical Science* 38, no. 25 (2023).

[404] Karlberg, Johan Petter Einar, and Marjorie A. Speers. *Reviewing clinical trials: a guide for the ethics committee*. Hong Kong, 2010.

[405] Steinkamp, Norbert, Bert Gordijn, Ana Borovecki, Eugenijus Gefenas, Jozef Glasa, Marc Guerrier, Tom Meulenbergs, Joanna Różyńska, and Anne Slowther. "Regulation of healthcare ethics committees in Europe." *Medicine, Health Care and Philosophy* 10 (2007): 461-475.

[406] Bioethics, Nuffield Council. "Children and clinical research: ethical issues." London: ESP Colour Ltd (2015).

[407] Claudot, Frédérique, François Alla, Jeanne Fresson, Thierry Calvez, Henry Coudane, and Catherine Bonaïti-Pellié. "Ethics and observational studies in medical research: various rules in a common framework." *International journal of epidemiology* 38, no. 4 (2009): 1104-1108.

[408] International Committee of Medical Journal Editors. Uniform Requirements for Manuscripts Submitted to Biomedical Journals: Writing and Editing for Biomedical Publication. Available at: http://www.icmje.org/

[409] Lemaire, Francois. "Do all types of human research need ethics committee approval?." *American journal of respiratory and critical care medicine* 174, no. 4 (2006): 363-364.

Funded by Horizon Europe Framework Programme of the European Union