REal-time data monitoring for **S**hared, **A**daptive, **M**ulti-domain and **P**ersonalised prediction and decision making for **L**ong-term Pulmonary care **E**cosystems

D1.4: Ethics Strategy

Dissemination level:	PU
Document type:	Report
Version:	1.0
Date:	27 July 2021

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No 965315. This result reflects only the author's view and the European Commission is not responsible for any use that may be made of the information it contains.

Document Details

Reference No.	965315
Project title	**RE-SAMPLE** - **RE**al-time data monitoring for **S**hared, **A**daptive, **M**ulti-domain and **P**ersonalised prediction and decision making for **L**ong-term Pulmonary care **E**cosystems
Title of deliverable	Ethics Strategy
Due date deliverable	31 July 2021
Work Package	WP1
Document type	Report
Dissemination Level	PU: Public
Approved by	Coordinator
Author(s)	C. Lambrinoudakis, C. Kalloniatis, A. Kanatas, C. Lyvas (UPRC)
Reviewer(s)	C. Masciocchi (GEM), R. Jõgi (TUK)
Total No. of pages	41

Partners

Participant No	Participant organisation name (country)	Participant abbreviation
1 (Coordinator)	University of Twente (NL)	UT
2	Foundation Medisch Spectrum Twente (NL)	MST
3	University of Piraeus Research Center (GR)	UPRC
4	Foundation Tartu University Hospital (EE)	TUK
5	Foundation University Polyclinic Agostino Gemelli IRCCS (IT)	GEM
6	European Hospital and Healthcare Federation (BE)	HOPE
7	German Research Center for Artificial Intelligence GMBH (DE)	DFKI
8	ATOS IT Solutions and Services Iberia SL (ES)	ATOS
9	Roessingh Research and Development BV (NL)	RRD
10	Innovation Sprint (BE)	iSPRINT

Abstract

This deliverable will briefly explain the ethical and regulatory framework that is identified as being relevant to the RE-SAMPLE project. The contents of this deliverable will act as guideline for all the RE-SAMPLE consortium members while executing their tasks in their respective work packages.

RE-SAMPLE's goal is to use Real World Data (RWD) in order to improve the healthcare journey of patients with Chronic Obstructive Pulmonary Disease (COPD) and comorbidities, and to set a standard of care for patients suffering from complex chronic conditions. The data and analyses will also serve as a basis for predictive models that will help patients and their doctors make treatment and lifestyle changes in time to reduce serious complications. Furthermore, doctors, caregivers and patients will acquire a unique insight into common, day-to-day triggers that can lead to health complications, thus mitigating them while reducing their frequency. RE-SAMPLE will gain unique insights into the complex relationships between patients' clinical and non-clinical characteristics, and how these impact disease progression, mental wellbeing, and physical health by using Artificial Intelligence (AI).

The purpose of this deliverable is to take into consideration all the unique characteristics of the RE-SAMPLE project and create a legal and ethical reflection of those findings. First the applicable legal and ethical frameworks are thoroughly investigated. The aforementioned analysis does not take into consideration only the primary and secondary legislation, but also the guidance issued by the European Commission and other EU bodies and agencies. Consequently, its goal is to identify the ethical and legal issues, relevant to the RE-SAMPLE project, and convey them.

The outcome of the first two chapters is reflected in the context of the RE-SAMPLE project in Chapters 4 (for ethics) and 5 (for personal data protection). The purpose is to support the project partners, through their activities, without jeopardizing the compliance with the ethical and legal standards.

Contents

List of Tables

Symbols, definitions, abbreviations, and acronyms

AI	Artificial Intelligence
ALLEA	All European Academies
CCC	Complex Chronic Condition
CIOMS	Council for International Organizations of Medical Sciences
CIPL	Centre for Information Policy Leadership
COPD	Chronic Obstructive Pulmonary Disease
D	Deliverable
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
EASAC	European Academies Science Advisory Council
EGE	European Group on Ethics in Science and New Technologies
EU	European Union
FEAM	Federation of European Academies of Medicine
GDPR	General Data Protection Regulation
OECD	Organisation for Economic Co-operation and Development
PAHO	Pan American Health Organization
WP	Work Package

1. Introduction

This document constitutes deliverable D1.4, which intends to provide to the project partners the necessary background information for the legal compliance and ethics management of the RE-SAMPLE project. The deliverable addresses ethical, legal and security/privacy issues that may arise during the project's life, identifying the requirements that need to be taken into consideration in order for RE-SAMPLE to be and remain fully compliant. It also includes general guidelines, forming an internal policy document on legal and ethics aspects, to be taken into account by all RE-SAMPLE partners throughout the lifetime of the project.

It should be stressed that this report is delivered at an early stage of the project and any findings are of a preliminary nature. The aim is to present the main risks associated with the project and suggest the basic measures that should be undertaken by the projects' partners in order to warrant compliance in the ethics and legal fields. Many of the issues referred to hereunder are the subject of separate WPs and deliverables (for instance GDPR compliance in WP4) and therefore will be further analysed during the lifetime of the project.

The deliverable is divided into various chapters, starting with chapter 2 that presents the ethical principles applicable to research conducted in the EU, with a special emphasis on issues related to health research. Chapter 3 describes the applicable legal framework for the protection of personal data that will be processed by the various project activities, with emphasis on the special categories of personal data that are health data. Chapter 4 maps the ethical principles presented in chapter 2, to the RE-SAMPLE context and provides guidelines for the project partners on how to comply with them. As already mentioned, these guidelines will be adopted as an internal policy by the project partners. Finally, chapter 5 identifies the main legal requirements (as these have been presented in chapter 3) for the protection of personal data that are applicable to RE-SAMPLE. Similarly to the ethical principles, specific guidelines are also provided for fulfilling those requirements.

2. Ethical principles applicable to research conducted in the EU

2.1 What are the major ethical issues in conducting research?

All EU-funded projects should be aligned with ethical principles and ethical compliance. The regulation that established Horizon 2020 scheme [1], and specifically article 19 of the document entitled "Ethical Principles", details the ethics' concerns and principles that should be considered during the execution of research activities. More specifically, the regulation mentions that the ethical framework of Horizon 2020 is defined though five ethical principles:

a) It is mandatory for the research and innovation activities that are carried out in the scope of Horizon 2020 projects to comply with the relevant European Union (EU), international and national legislation. Additionally, they should also comply with the European Convention on Human Rights, its Supplementary Protocols and the Charter of Fundamental Rights of the EU. It should be noted that the principle of proportionality, the right to privacy, the right to the protection of personal data, the right to the physical and mental integrity of a person, the right to non-discrimination and the need to ensure high levels of human health protection need to receive special attention.
b) The Research and Innovation activities executed under the scope of the Horizon 2020 projects need to be exclusively focused on civil applications.
c) The Horizon 2020 scheme defines a list of research fields that are not illegible to be financed. Those are: research activity aiming at human cloning for reproductive purposes; research activity intended to modify the genetic heritage of human beings which could make such changes heritable; research activities intended to create human embryos solely for research or stem cell procurement, including by utilizing somatic cell nuclear transfer.
d) No funding can be granted for research activities in a Member State if they are forbidden by the Member State. Additionally, funding can be granted if the research activities are forbidden by all Member States. It is possible for research on human stem cells, both adult and embryonic, to be financed, heavily relying on the contents of the scientific proposal and especially the legal framework of the involved Member States.
e) The contents of Article 32 paragraph 3 mention fields of research that can be reviewed during the interim evaluation of this article in the light of scientific advances [2].

2.2 Identifying and addressing ethical issues in research

According to the "Ethics and data protection" document published by the European Commission [3], all research proposals that include processing of personal data must provide information about the data protection provisions within the text of the proposal. Additionally, there are higher chances for the project to raise higher ethics risks if it meets the following conditions:

- processing of "special categories" of personal data (formerly known as 'sensitive data').
- processing of personal data concerning children, vulnerable people, or people who have not given their consent to participate in the research.
- monitoring of a publicly accessible area on a large scale and in a systematic way and/or large scale processing of personal data and/or processing operations of high complexity;
- techniques that are vulnerable to misuse or techniques for data processing that are invasive and deemed to pose a risk to the rights and freedoms of research participants; and
- data collection that takes place outside the EU transfer of personal data that are collected in the EU to entities in non-EU countries.

In case the research activities include higher-risk data processing (see Table 1), the partners must provide a detailed analysis of the ethics issues raised by the project methodology.

Table 1: Indicators of data processing operations that may entail higher ethics risks

Types of personal data	- racial or ethnic origin - political opinions, religious or philosophical beliefs - genetic, biometric or health data - sex life or sexual orientation - trade union membership
Data subjects	- Children - vulnerable people - people who have not given their explicit consent to participate in the project
Scale or complexity of data processing	- large-scale processing of personal data - systematic monitoring of a publicly accessible area on a large scale - involvement of multiple datasets and/or service providers, or the combination and analysis of different datasets (i.e. big data)
Data-collection or processing techniques	- privacy-invasive methods or technologies (e.g. the covert observation, surveillance, tracking or deception of individuals) - using camera systems to monitor behaviour or record sensitive information - data mining (including data collected from social media networks), 'web crawling' or social network analysis - profiling individuals or groups (particularly behavioural or psychological profiling) - using artificial intelligence to analyse personal data - using automated decision-making that has a significant impact on the data subject(s)
Involvement of non-EU countries	- transfer of personal data to non-EU countries - collection of personal data outside the EU

The aforementioned analysis should be comprised of:

- an overview of all planned data collection and processing operations;
- identification and analysis of the ethics issues that these raise; and
- an explanation of how you will mitigate these issues in practice.

It is also mandatory that all the referred issues are detailed and addressed in the research protocol that the consortium submits to the research ethics committee. It might also be required for a data protection impact assessment (DPIA) to be conducted in line with Article 35 GDPR and supplementary guidance on DPIAs. In case an institution already has appointed a data protection officer (DPO), they should be involved in all stages of the project in order to provide their advice on data privacy issues. In case of complex, sensitive or large-scale data processing taking place or if there is a possibility for data to be transferred outside the EU, the DPO should be consulted on the compatibility of the data protection arrangements with the host institution's policies and applicable legislation. The opinion and advice of the DPO should be part of the proposal. In case an organisation has not appointed a DPO, a qualified expert can offer his services. Below, Table 2 lists the Ethics issues published by the European Commission and used in the Horizon program.

Table 2: Ethics issues

1. HUMAN EMBRYOS/FOETUSES	
Does your research involve Human Embryonic Stem Cells (hESCs)?	Yes/No
Does your research involve the use of human embryos?	Yes/No
Does your research involve the use of human foetal tissues / cells?	Yes/No
2. HUMANS	
Does your research involve human participants?	Yes/No
Are they volunteers for social or human sciences research?	Yes/No
Are they persons unable to give informed consent?	Yes/No

Are they vulnerable individuals or groups?	Yes/No
Are they children/minors?	Yes/No
Are they patients?	Yes/No
Are they healthy volunteers for medical studies?	Yes/No
Does your research involve physical interventions on the study participants?	Yes/No
Does it involve invasive techniques?	Yes/No
Does it involve collection of biological samples?	Yes/No
If your research involves processing of genetic information, see also section 4.	
3. HUMAN CELLS / TISSUES	
Does your research involve human cells or tissues (other than from Human Embryos/Foetuses, i.e. section 1)?	Yes/No
Are they available commercially?	Yes/No
Are they obtained within this project?	Yes/No
Are they obtained within another project?	Yes/No
Are they deposited in a biobank?	Yes/No
4. PERSONAL DATA	Yes/No
Does your research involve personal data collection and/or processing?	Yes/No
Does it involve the collection and/or processing of sensitive personal data (e.g: health, sexual lifestyle, ethnicity, political opinion, religious or philosophical conviction)?	Yes/No
Does it involve processing of genetic information?	Yes/No
Does it involve tracking or observation of participants?	Yes/No
Does your research involve further processing of previously collected personal data (secondary use)?	Yes/No
5. ANIMALS	
Does your research involve animals?	Yes/No
Are they vertebrates?	Yes/No
Are they non-human primates?	Yes/No
Are they genetically modified?	Yes/No
Are they cloned farm animals?	Yes/No
Are they endangered species?	Yes/No
6. THIRD COUNTRIES	Yes/No
In case non-EU countries are involved, do the research related activities undertaken in these countries raise potential ethics issues?	Yes/No
Do you plan to use local resources (e.g. animal and/or human tissue samples, genetic material, live animals, human remains, materials of historical value, endangered fauna or flora samples, etc.)?	Yes/No
Do you plan to import any material - including personal data - from non-EU countries into the EU?	Yes/No
Do you plan to export any material - including personal data - from the EU to non-EU countries?	Yes/No
In case your research involves low and/or lower middle income countries, are any benefits- sharing actions planned?	Yes/No
Could the situation in the country put the individuals taking part in the research at risk?	Yes/No
7. ENVIRONMENT & HEALTH and SAFETY	
Does your research involve the use of elements that may cause harm to the environment, to animals or plants?	Yes/No

Does your research deal with endangered fauna and/or flora and/or protected areas?	Yes/No
Does your research involve the use of elements that may cause harm to humans, including research staff?	Yes/No
8. DUAL USE	
Does your research involve dual-use items in the sense of Regulation 428/2009, or other items for which an authorisation is required?	Yes/No
9. EXCLUSIVE FOCUS ON CIVIL APPLICATIONS	
Could your research raise concerns regarding the exclusive focus on civil applications?	Yes/No
10. MISUSE	
Does your research have the potential for misuse of research results?	Yes/No
11. OTHER ETHICS ISSUES	
Are there any other ethics issues that should be taken into consideration? Please specify	Yes/No

Consequently, the ethical issues that EU research projects ought to deal with can be summarized as:

- Informed consent;
- Civil application and dual-use;
- Vulnerable subjects including patients, elderly and children;
- Privacy / confidentiality;
- Personal data;
- Potential misuse of research findings;
- Information security.

In 2017 the revised edition of the European Code of Conduct for Research Integrity [4] was published. There, it is stated that research is influenced by fundamental principles of research integrity. These principles are summarized as:

- **Reliability** acts as a factor that ensures the quality of research reflected in the design, the methodology, the analysis and the use of resources.
- **Honesty** in developing, undertaking, reviewing, reporting and communicating research in a transparent, fair, full and unbiased way.
- **Respect** for colleagues, research participants, society, ecosystems, cultural heritage and the environment.
- **Accountability** for all the research lifecycle; from its birth as an idea to the publication stage, for its management and organisation, for training, supervision and mentoring, and for all its wider impacts.

The same document articulates that good research practices correspond to the following contexts:

- Research Environment
- Training, Supervision and Mentoring
- Research Procedures
- Safeguards
- Data Practices and Management
- Collaborative Working
- Publication and Dissemination
- Reviewing, Evaluating and Editing

In 2016 M. D. Wilkinson, et al. published the “The FAIR Guiding Principles for scientific data management and stewardship” [15]. Their work provide guidelines based on four pillars: Findability, Accessibility, Interoperability, and Reusability, thus helping data producers and publishers to maximize the added value gained by contemporary, formal scholarly digital publishing. It should be highlighted that this work does

not apply only to the original "data" widely used, but also to the algorithms, tools, and workflows that led to that data.

There are also the Open Data Mandates which consist of the Open Science [16] and the Open Data [17]. Their goal is to introduce some guidelines that make data accessible and reusable, while being compliant with national and EU legislation. This is a rather challenging process that ensures personal data protection and privacy, while strictly following the main ethical guidelines. The dissemination outputs of every project should also abide by the OpenAIRE Initiative of the European Commission [18], thus making knowledge accessible to the majority of the world while ensuring anonymization, encryption, privacy protection, and data de-identification.

The Organisation for Economic Co-operation and Development (OECD) is an international organisation whose role is to create better policies that foster prosperity, equality, opportunity and well-being for all. The OECD Working Party of Senior Digital Government Officials (E-leaders) co-led by the OECD Digital Government and Data Unit and the Netherland's Ministry of the Interior and Kingdom Relations with the participation from OECD member and partner countries, created the "Good Practice Principles for Data Ethics in the Public Sector" [20]. It supports the ethical use of data in digital government projects, products, and services to ensure they are worthy of citizens' trust. Ten principles for Data Ethics in the Public Sector are introduced in the document and can be summarized in the form of actions as:

1. Manage data with integrity
2. Be aware of and observe relevant government-wide arrangements for trustworthy data access, sharing and use
3. Incorporate data ethical considerations into governmental, organisational and public sector decision-making processes
4. Monitor and retain control over data inputs, in particular, those used to inform the development and training of AI systems, and adopt a risk-based approach to the automation of decisions
5. Be specific about the purpose of data use, especially in the case of personal data
6. Define boundaries for data access, sharing and use
7. Be clear, inclusive and open
8. Publish open data and source code
9. Broaden individuals' and collectives' control over their data
10. Be accountable and proactive in managing risks

2.3 Ethics in health-related research

RE-SAMPLE consortium will act according to the research ethics for health-related research with human participants. As ethics govern the research activities in and out of the EU, they become even more specific when the performed research is related to health. This becomes evident not only from the EU regulation and frameworks but also from the form that needs to be submitted along with the proposal. According to Beauchamp and Childress [5] when human participants are involved in a research process, there are pillars of ethics that should ensure respect for people and human dignity and fair distribution of the benefits and burden of research. The same pillars should also protect the values, rights, and interests of the research participants along with respecting the autonomy of the research participants, beneficence, non-maleficence, and promotion of justice and fairness.

In 1964 World Medical Association during its 18th General Assembly adopted the Declaration of Helsinki [6] that was revised last time in 2013 by the 64th General Assembly. The declaration is a statement of ethical principles which is meant for medical research involving human subjects, including research on identifiable human material and data. Its contents are split into:

- General Principles
- Risks, Burdens and Benefits
- Vulnerable Groups and Individuals
- Scientific Requirements and Research Protocols
- Research Ethics Committees

- Privacy and Confidentiality
- Informed Consent
- Use of Placebo
- Post-Trial Provisions
- Research Registration and Publication and Dissemination of Results
- Unproven Interventions in Clinical Practice

Summarizing the declaration, it prioritizes the health of the patient to research binds medical research to ethical standards that promote and ensure respect for all human subjects and protect their health and rights. It also makes mandatory the timely preparation of the research protocol and its exhaustive check from a transparent committee of experts. It also requests that the participants should be capable of giving informed consent as subjects in medical research.

The Council of Europe on the 04/04/1997, taking into consideration:

- the Universal Declaration of Human Rights proclaimed by the General Assembly of the United Nations on 10 December 1948
- the Protection of Human Rights and Fundamental Freedoms of 4 November 1950
- the European Social Charter of 18 October 1961
- the International Covenant on Civil and Political Rights and the International Covenant on Economic, Social and Cultural Rights of 16 December 1966
- the Convention for the Protection of Individuals concerning the Automatic Processing of Personal Data of 28 January 1981
- Convention on the Rights of the Child of 20 November 1989

signed the "Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine" [7]. The convention's goal is to promote international cooperation in the fields of biology and medicine while at the same time setting some rules in order to safeguard human dignity and the fundamental rights and freedoms of the individual. One whole chapter is devoted to the importance of the consent given by the test subject's free will. For persons without the ability to consent, the convention allows the intervention to be carried out for their direct benefit. Even in cases of mental disorders, if the process does not harm the well-being of the human subject and the results of the research activities have the potential to improve their condition, the intervention rule applies. Additionally, it protects all participants from discrimination and requires they have been properly informed of their rights and have been legally safeguarded.

The importance of ethical issues regarding health-related research was also acknowledged by the Council for International Organizations of Medical Sciences (CIOMS) which joined forces with the World Health Organization (WHO) and published the "International Ethical Guidelines for Health-related Research Involving Humans" [8]. It was first published in 1982 and later revised in 1993, 2002 and last in 2016. As there was close cooperation with the World Medical Association during the revision process, it was ensured that the final draft was in line with the Declaration of Helsinki [6]. The very first guideline is entitled "SCIENTIFIC AND SOCIAL VALUE AND RESPECT FOR RIGHTS". There, the authors take into serious consideration, the social and scientific values of the research, the qualifications of the research personnel, the respect for rights and welfare, and how the results of the research are disseminated. Except the settings under which the research activities are taking place, the majority of the guidelines are focused on the individuals who take place in the research. Specifically, the guidelines emphasize the individuals' social value and respect for rights, risks and benefits, health, and of course the process through which data are collected. Of course, one more consent is extremely important and special reference is made to individuals who are unable to give their consent, as well as children and pregnant women.

In 1990 the International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use (ICH) was created. Its role is to bring together the regulatory authorities and pharmaceutical industry to discuss scientific and technical aspects of pharmaceuticals, thus developing some guidelines. One of them is the "INTEGRATED ADDENDUM TO ICH E6(R1): GUIDELINE FOR GOOD

CLINICAL PRACTICE E6(R2)" (ICH-GCP) [11], initially published in 1995 and revised in 1996 and 2016 when the parental guideline was updated. The ICH-GCP is a harmonized standard, whose goal is to protect the rights, safety and welfare of human subjects while minimizing human exposure to investigational products. The ICH-GCP is also willing to improve the quality of data and accelerate the marketing process of new drugs, thus decreasing the cost to sponsors and the public. If a project is compliant with the aforementioned standard, then public assurance is provided that the rights, safety and well-being of trial subjects are going to be protected. Additionally, they are going to be consistent with the principles of the Declaration of Helsinki, while producing credible clinical trial data.

The European Commission also turned their attention to the Clinical trials and the involvement of human subjects by publishing the Directive 2001/20/EC [9] in 2001 that was amended in 2006 and 2009. The Directive is also influenced by the Helsinki Declaration. For subjects participating in clinical trials, the directive requires the "informed consent", a decision which must be represented in written form, and has also to be dated and signed after the participants have been briefly informed about their participation. Should the participant be unable to give their consent orally or in writing, the directive takes into consideration the exceptional case and requires at least one witness.
On the 16th of April 2014, the EU published the "Clinical trials - Regulation EU No 536/2014" [10], which was set to replace the previous Clinical Trials Directive. The specific regulation's ambition is to make clinical trials data more transparent. It also supports that all information contained in the EU database will be publicly accessible unless its confidentiality can be justified on the basis of:

- Protection of commercially confidential information
- Protection of personal data
- Protection of confidential communication between EU countries
- Ensuring effective supervision of the conduct of clinical trials by EU countries

The European Medicine Agency helped with the supported transparency of the regulation by adding two sets of requirements to the functional specifications for applying the exceptions:

- Features to support making information public
- Disclosure rules describing the practical implementation of the transparency rule

"Clinical trials - Regulation EU No 536/2014" [10], corresponds mainly to the clinical trials conducted inside the EU. In case the trials despite taking place outside the EU, are submitted for marketing authorization in the EU, then they need to follow the provisions of the Clinical Trials Directive [9].

The European Commission in 1991 created the European Group on Ethics in Science and New Technologies (EGE), an independent, multi-disciplinary body whose role is to advise on all policies where ethical, societal and fundamental rights issues intersect with the development of science and new technologies. EGE group has published two documents, the "Ethics of information and communication technologies" [12] in 2012 and the "Ethical issues of healthcare in the information society" [13] in 2018 where the following ethical issues are being identified:

- Human dignity
- Autonomy
- Justice
- Beneficence & non-maleficence
- Solidarity
- Confidentiality/Trust
- Self-determination
- Accountability
- Principle of legitimate purpose
- Security
- Participation
- Transparency

The Internet Healthcare Coalition, founded in 1997 is an international, non-partisan, non-profit organization dedicated to promoting quality healthcare resources on the Internet. Their goal among others is to educate

healthcare consumers, health professionals, and others about the evolving ethical issues which are related to the quality of Internet health resources and information. The Internet Healthcare Coalition in collaboration with the World Health Organisation (WHO) and the Pan American Health Organization (PAHO) published in 2000 the e-Health Code of Ethics [14]. The latter is willing to communicate to all the people around the world an understanding of how important it is to manage their health data or the health data of those in their care through the internet and acquire a good understanding of the potential risks. The most recent version of the e-Health Code of Ethics sets forth the following guiding principles:

- Accountability
- Responsible Partnering
- Professionalism in online Health Care
- Privacy
- Informed Consent
- Quality
- Honesty
- Candour

Despite the interest of the international organizations about the ethical aspects of medical experiments, other significant efforts have been recorded as well within national borders. The Gemelli University Hospital IRCCS created a code of ethics in 2015 and revised it within the next year [19]. The Ethics Code expresses the principles, values, and the ethical responsibilities that represent the binding criteria for the entire organization. These are the fundamental principles indicated by the Magisterium of the Catholic Church regarding bioethics and they are mandatory for every employee and collaborator.

More recently, the European Academies Science Advisory Council (EASAC) with the help of All European Academies (ALLEA) and Federation of European Academies of Medicine (FEAM) published on April 2021 the "International Sharing of Personal Health Data for Research" [21] which is an effort to the barriers of transferring public sector data outside the EU/EEA. With a deep understanding of how important sharing of data for medical research and especially for improved health care and disease prevention (e.g. COVID-19) and the impediments introduced by GDPR, this work is an attempt to solve them and help academic researchers, healthcare professionals, and others in the public sector.

2.4 Ethics and AI

AI is the imitation of human intelligence by machines that are programmed to perform specific tasks. This allows automation of actions which offers a significant acceleration in research activities compared to being performed only by humans. However, as AI is applied across all research sectors including health-related research, ethical questions arise regarding its proper use and application.

In 2018 IEEE Advancing Technology for Humanity published the "Ethically Aligned Design: A Vision for Prioritizing Human Wellbeing with Artificial Intelligence and Autonomous Systems" [22]. The IEEE committee responsible for this work, identified high-level ethical concerns applying to all types of AI that:

1. Embody the highest ideals of human rights.
2. Prioritize the maximum benefit to humanity and the natural environment.
3. Mitigate risks and negative impacts as AI evolve as socio-technical systems.

During the same year, the Savannah Law Review was published with the subject area "Deus ex Machina: Regulating Cybersecurity and Artificial Intelligence for Patients of the Future" [23]. The authors of this work highlight the importance of the use of AI in the form of machine learning, implemented in medical devices. Their applications and especially the unsupervised learning is revolutionary if we consider the fact that the machines are not biased as it is usually happening with humans, thus making their results way more accurate. However, they also demand large volumes of data to reach the desired level of accuracy. According to the authors, the collection of those data resents a plethora of potential patient safety concerns along with cybersecurity concerns as the attack surface has become significantly broader. Therefore, the

gaps introduced by the new technologies are investigated in the scope of U.S. and E.U. regulatory frameworks.

The report by Datatilsynet on "Artificial intelligence and privacy" [24] is motivated by the ethical dilemmas that will appear soon. Those concern the effort to identify the balance between considerable social advances in the name of AI and fundamental privacy rights. A special chapter is devoted to the relationship between AI and GDPR. More specifically the authors analyse the algorithmic bias of AI in the scope of the fairness principle and the principle of purpose limitation. Additionally, they explain the contradictions revealed between the data minimization and the data hunger of the AI algorithms as well as the transparent processing and the black-box approach. The proposed solution to overcome those obstacles is privacy-by-design system implementations and the DPIAs. The same view shared the publication of the 2019 high-level expert group on AI, set up by the European Commission published "A Definition of AI: Main Capabilities and Disciplines" [25].

Later the same year, the European Commission published the "Ethics Guidelines for trustworthy AI" [26] which is aligned with its vision to ethical, secure and cutting-edge AI made in Europe. According to the manuscript, the trustworthy AI is built on top of three mandatory components:

- It is lawful, thus complying with all applicable laws and regulations;
- It is ethical, thus ensuring adherence to ethical principles and values; and
- It is socially and technically robust, since, AI systems have the potential to cause unintentional harm.

It is mentioned that trustworthy AI systems should improve individual and collective wellbeing. There are four ethical imperatives that every AI practitioner should adhere to:

i. Respect for human autonomy
ii. Prevention of harm
iii. Fairness
iv. Explicability

Professor Lilian Mitrou in her work "Data Protection, Artificial Intelligence and Cognitive Services" published in 2019 [27] questions if GDPR is suitable to deal with the newly introduced privacy and data protection rights considerations in the light of the AI developments. She concludes that due to the technology agnostic regulatory approach, GDPR can meet our expectations with regard to AI implementations. It is highlighted that for any research approach an authentic consent should exist for research ethics along with the social accountability of developers and the global academic cooperation. As the foundation of an AI ethical framework is identified the inviolability of human dignity and autonomy, as individuals should not be deprived from the right to exercise influence over decision-making processes that significantly affect them. Along with autonomy also comes self-determination that refers to the freedom of choice over the use of AI, a choice that must be informed and free.

Following the same mentality, in November 2019 the European Data Protection Board published the "Guidelines 4/2019 on Article 25 Data Protection by Design and by Default" which was revised in October 2020 [28]. It is introduced that the data controller has the obligation to estimate the processing's wider impact on individuals' rights and dignity. Furthermore, GDPR Article 25 stipulates that a controller must "*implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimization, in an effective manner*". Recently, The Centre for Information Policy Leadership (CIPL) published the "CIPL Recommendations on Adopting a Risk-Based Approach to Regulating Artificial Intelligence in the EU" with a vision for an effective and future-proof AI framework that benefits individuals, organizations, regulators, society, and the economy. It is mentioned that all risky AI use cases should be reviewed, thus improving the AI practices [29]. Except the ethical impact assessment, the report also emphasizes the importance of ethics and fairness training to technology teams.

3. Personal data protection - Regulation EU 2016/679

3.1 Background and purpose

The protection of natural persons in relation to processing of their personal data is a fundamental right protected under article 8(1) of the Charter of Fundamental rights of the EU, as well as under article 16 (1) of the Treaty on the Functioning of the EU.

Data protection in Europe was, until recently, regulated by the Data Protection Directive 95/46/EC. However, constant technological developments, digitalisation and globalisation, as well as people intension to share a huge amount of data online, have challenged the data protection regime and have called for a reform that will warrant a strong and coherent data protection framework in the EU. Effective protection of personal data throughout the Union, strengthening of the subjects' rights when processing of their personal data takes place, setting in detail data controllers' obligations and warranting free flow of personal data within the Union are only some of the issues the new General Data Protection Regulation (GDPR) aims to address.

The GDPR is the successor of Directive 95/46/EC of 24 October 1995. GDPR entered into force in May 2016 and became fully enforceable in May 2018 throughout the EU. GDPR, contrary to the recently repealed Data Protection Directive, is a regulatory tool of broad and direct effect that intends to address any inconsistency in national laws and to succeed a harmonised data approach among Member States.

GDPR regulates the processing by an individual, a company or an organization of personal data relating to individuals in the EU. The Regulation does not apply to the processing of personal data of deceased persons or of legal entities. Its provisions do not apply to data processing by an individual for purely personal reasons or for activities carried out in one's home provided there is no connection to a professional or commercial activity.

3.2 Definitions

The basic definitions under the GDPR, as of more relevance to the RE-SAMPLE project, include:

a) Personal Data
The definition of "personal data" is included in Article 4(1) of the GDPR: **personal data** means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. The notion of "identifiability" is further analysed in the Regulation and more specifically in Recital 26 where a proportionality test is used in order to assess each time what data may pertain to identifiable individuals. The recital reads as follows: "*To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain 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*". If the test is not passed, then such data are considered anonymous and the law does not apply on them.

b) Special categories of data
Special attention should be given to categories of data that do not fall under the generic definition of personal data mentioned above. These include:

- **genetic data** that include personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

- **biometric data** that include personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data; and
- **data concerning health** that refer to 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. The first two categories constitute additions in the data protection field that come as a result of scientific developments in their respective fields.

The above categories of data fall under the definition of special categories of personal data. It should be mentioned that the term sensitive data that was used in the Directive is replaced in the new Regulation by the term "special categories of personal data". According to article 9 (1) of the GDPR "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". Exceptions to this rule are included in par. 2 of the same Article 9, as outlined below under (d).

c) Pseudonymisation

Another definition that should be included in this analysis as of relevance to the RE-SAMPLE project is that of "pseudonymisation". The term is a new entry in the text of the GDPR. In essence, pseudonymisation means "*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 such additional information is kept separately and subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable person*" (Art. 4(5)). For the avoidance of any doubt regarding whether or not pseudonymised data should be treated as personal data recital 26 of the GDPR clarifies that: "*personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person*". What matters in practice is not the process of pseudonymisation as such but whether the natural person could be, at the end of the day, be identified.

d) "Processing" of personal data

A definition of "processing" of personal data is provided under Article 4(2) of the Regulation. Processing therefore 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*". The processing principles are described below under section 3.3.

The Regulation makes explicit reference to processing of special categories of personal data in its article 9. In this context, apart from the basic principles that should apply to any processing of personal data, in the event that special categories of data are concerned, processing shall be prohibited. **Article 9(2) however names the exceptions to this general prohibition. In particular, paragraph 1 shall not apply if one of the following applies:**

a. the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;
b. 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;
c. 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;

d. processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
e. processing relates to personal data which are manifestly made public by the data subject;
f. processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
g. 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;
h. 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 referred to in paragraph 3;
i. 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;
j. 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.

e) Controllers – processors – joint controllers – recipients

The definition of a **controller** is provided under article 4(7) of the GDPR. According to said provision controller means 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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law". New addition introduced by the Regulation is the explicit reference to the notion of joint controllers. Article 26 of the Regulation states that "Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation […]".

Article 4(8) defines a **processor** as "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller".

Finally, a **recipient** is defined under article 4(9). In particular, "recipient' means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not".

3.3 The GDPR processing principles

3.3.1 The personal data processing principles in general

Principles relating to processing of personal data are listed in Article 5 of the GDPR. If one wanted to compare the old legislative framework with the new one, one would reach the conclusion that the processing principles remain, in their essence, the same, however they have been worded in a more solid way. In addition, the principles of transparency and accountability have been added to the list of principles, thus contributing further to individual protection during processing of personal data.

In this context Article 5 of the Regulation reads as follows:

1. Personal data shall be:

a. processed lawfully, fairly and in a transparent manner in relation to the data subject (‘**lawfulness, fairness and transparency’**)

b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (‘purpose limitation’);

c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);

d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’);

e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (‘storage limitation’)

f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures (‘integrity and confidentiality’).

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘accountability’).

To sum up, the processing principles provided under the GDPR are the principles of:

- **lawfulness, fairness and transparency**
- **limited purpose**
- **data minimisation**
- **accuracy**
- **storage limitation**
- **integrity and confidentiality**
- **accountability**

3.3.2 Fair, lawful and transparent processing

a) Lawfulness

According to Article 5.1(a) of the EU GDPR, "*personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject (lawfulness, fairness and transparency)*". This principle of lawfulness of processing is further defined in its Article 6, where it is stated that "*processing of personal data shall be lawful only if and to the extent that at least one of the following applies: (a) the data subject has given consent to the processing of their personal data for one or more specific purposes; (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; (c) processing is necessary for compliance with a legal obligation to which the controller is subject; (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person; (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such 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. This shall not apply to processing carried out by public authorities in the performance of their tasks*". Consequently, the principle of lawfulness of the processing requires that one of the above legal bases and not cumulatively all six of them, needs to apply in order for the processing to be conducted lawfully. Consequently, the lawful grounds for processing operations are six:

- consent,
- performance of a contract,
- compliance with a legal obligation,
- protection of vital interests,
- public interest,
- overriding interest of the controller.

b) Transparency

As far as **the principle of transparency** is concerned, article 5.1(a) of the GDPR states that personal data must also be processed in a transparent manner. Further guidance on what transparency exactly means is provided in Recital 39: *"[…] It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed. Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing. In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data.".*

3.3.3 The principle of accountability

As already mentioned, the principle of accountability is a new addition under the GDPR. According to Article 5.2 of the EU GDPR, "*the controller shall be responsible for and be able to demonstrate compliance with paragraph 1 [the basic personal data processing principles]*". Consequently, it is the data controller's obligation to undertake the necessary measures, both organisational, technical or other in order to be ready, to demonstrate that the data protection law has been observed. Internal policies, appointment of a DPO or conducting DPIAs are some examples of compliance with the principle of accountability.

3.3.4 Individual consent

As indicated above under Chapter 1 (ethical principles), informed consent of the subjects participating in a research is the first and perhaps the most important part of conducting research ethically. When it comes to personal data processing in particular, individual consent is arguably the most important legal ground for processing personal data lawfully. It's the only legal ground that lies exclusively upon the individual's personal decision to have his/her personal data processed.

A definition of consent is provided under article 4(11) of the GDPR: consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

More details on the specific criteria which individual consent should meet are provided under recital 32 of the GDPR: "*Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided*".

Additional conditions for consent are listed in article 7 of the Regulation. In more detail:

- the controller shall be responsible to demonstrate that the data subject has consented to processing of his or her personal data;
- if consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters;
- the data subject shall be free to withdraw his/her consent at any time;
- When the performance of a contract is conditional on consent to the processing of personal data that is not necessary for the performance of that contract, it should always be examined whether the consent has indeed be provided freely;

The Regulation refers separately to the conditions applicable to child's consent in relation to information society services (Article 8 of the GDPR).

3.4 The GDPR rights afforded to individuals (data subjects)

3.4.1 General

Rights of the data subject are dealt with in Chapter III of the GDPR. In particular, Article 12 sets the way (the "modalities") that rights listed in the next articles are to be exercised:

- any information to the data subjects should be provided by the controller in a transparent and easily accessible form;
- the information shall be provided in writing;
- the controller shall facilitate the exercise of the data subjects' rights;
- the controller shall also provide information on action taken on a request under Articles 15-22 to the data subject without undue delay;
- if the controller does not take action on the request of the data subject, the controller shall inform the data subject of the reasons for not taking action;
- information shall be provided for free.

The rights attributed to data subjects are regulated under articles 13 to 21 and are the right to information, the right of access, the right to rectification, the right to erasure (right to be forgotten), the right to restriction of processing, the right to data portability, and the right to object.

3.4.2 The right to information

The right to information is regulated in two articles, namely Articles 13 and 14. Distinction is made between cases where the information was obtained from the data subject and other cases. In this context, article 13 regulates the case where personal data have been collected form the data subject. In this case, the controller shall at the time when personal data are obtained, provide the data subject with the following information:

a. the identity and the contact details of the controller and, where applicable, of the controller's representative;
b. the contact details of the DPO , where applicable;
c. the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
d. where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;
e. the recipients or categories of recipients of the personal data, if any;
f. where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

Paragraph 2 of Article 13 lists the additional information the controller needs to provide to the data subject when collecting his/her personal data, such as the period for which the personal data will be stored, the existence of the right to request access to the data or erasure, the right to withdraw consent at any time etc.

Article 14 lists the information to be provided to the data subject where personal data have not been obtained from the data subject itself. Paragraph 5 of article 14 sets some exemptions of the controllers' obligation to provide information, for instance when the provision of such information proves impossible or would involve a disproportionate effort or where personal data must remain confidential etc.

3.4.3 The right to access the data

The right of access by the data subject is regulated under article 15 of the Regulation. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him/her are being processed and if yes, access to such data as well as information regarding, among others, the purpose of processing, the recipients to whom the data have been or will be disclosed the existence of the right to request rectification, the right to lodge a complaint and others, the right to request rectification etc. Paragraph 3 of article 15 sets the subject's right to request a copy of his/her personal data from the controller.

It is noted that the right to rectification is regulated separately in article 16. In particular, the data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her.

3.4.4 The right to erasure (right to be forgotten)

Article 17 of the Regulation grants individuals the right to have their personal information deleted by data controllers if specific conditions as these are listed in its paragraph 1 are met. For instance, the personal data have been unlawfully processed or they are no longer necessary in relation to the purpose for which they were collected, or the data subject has withdrawn his/her consent and others. In the event that the controller has made such data public, reasonable steps (including technical measures) will be taken to notify controllers who are processing the personal data accordingly. Finally, the "right to be forgotten" (actually,

to erasure of data) will not be applicable if it contrasts with the rights of freedom of expression and information as well as for several other, more expected, legal grounds (compliance with a legal obligation, public interest, archiving purposes, etc., as set in paragraph 3).

3.4.5 The right to restriction of the processing

Article 18 of the Regulation regulates the right to restriction of the personal data processing. The conditions under which a data subject may exercise his/her rights are listed in the first paragraph of article 18 and include, for instance, the contest by the data subject of the accuracy of the personal data processed by the controller or the claim that the processing is unlawful and therefore the data subject opposes the erasure of his/her personal data. Recital 67 mentions some methods the controller may use to restrict the processing of personal data, such as, 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.

3.4.6 The right to data portability

Data portability is dealt with under article 20 of the GDPR and includes the data subject's right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided. The right to data portability is provided to data subjects under two conditions:

a. the processing is carried out by automated means;
b. the processing is based on consent or on a contract.

3.4.7 The right to object

The right to object is laid down in Article 21 of the GDPR. Recital 69 of the Regulation clarifies the conditions under which a data subject may object to his/her data being processed. The recital reads as follows: Where personal data might lawfully be processed because 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, or on grounds of the legitimate interests of a controller or a third party, a data subject should, nevertheless, be entitled to object to the processing of any personal data relating to his or her particular situation. It should be for the controller to demonstrate that its compelling legitimate interest overrides the interests or the fundamental rights and freedoms of the data subject. In other words, the exercise by an individual of its right to object to its personal data being processed by a controller essentially includes a balancing of rights and legitimate interests: on the one hand an individual is interested in having its data no longer processed and on the other hand a controller may have an interest in continuing to process such data despite the individuals' objections.

3.5 Security of personal data

3.5.1 Security of the personal data processing

Security of the processing is regulated under article 32 of the GDPR. Both the controller and the processor need to implement technical and organisational measures to ensure a level of security including among others:

a. the pseudonymisation and encryption of personal data;
b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c. the ability to restore the availability and access to personal data in timely manner in the event of a physical or technical incident;
d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of processing.

All measures should be proportionate to the risk involved and the severity for the rights and freedoms of natural persons in the event of a personal data breach.

3.5.2 Data Breach Notifications

Articles 32 and 33 regulate the process of notifying to the supervisory authority a personal data breach. A "personal data breach" is defined in the text of the GDPR, in Article 4(12), as "*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed*". When this happens, controllers shall, according to article 33, par. 1 "*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*". The obligation of notification burdens the processor as well, who, shall notify the controller without undue delay after becoming aware of a personal data breach (article 33 par.2). Paragraph 3 lists the minimum information the notification must contain, such as the nature of the data breach, the name and contact details of the DPO, the likely consequences of the personal data breach and the measures taken or proposed to be taken by the controller to address the personal data breach.

Whereas article 33 deals with the notification of a breach to the supervisory authority, article 34 regulates the communication of a data breach to the data subject. This obligation burdens the controller in any case where the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons. The communication to the data subject shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in article 33(2). Paragraph 3 of article 34 sets the conditions under which the communication to the data subject is not required. In particular par. 3 reads as follows "*The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met: a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise; c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner".*

3.6 Data protection impact assessment

The "tool" of the impact assessment is a new entry under the GDPR. It is suggested as an extra security measure in all cases where a type of processing is likely to result in high risk to the rights and freedoms of natural persons. The assessment of the impact of the envisaged processing operations on the protection of personal data is carried out by the processor prior to the processing. Par. 3 of the article 35 specifically lists the case where a DPIA shall be required:

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

Paragraph 7 of article 35 lists the minimum content of the assessment. In particular, it should contain:

- a description of the processing and its purposes;
- an assessment of the necessity and proportionality of the processing in relation to the purpose of the processing;
- an assessment of the risks to the rights and freedoms of data subjects;
- the measures envisaged to address the risks, including security measures and mechanisms, to ensure the protection of personal data and to demonstrate compliance with the GDPR.

4. Ethics in the RE-SAMPLE project

4.1 RE-SAMPLE's particularities

As already presented in Chapter 2, all EU-funded projects need to comply with ethical principles, as well as with any applicable international, EU and national law. To this effect, it should be ensured that the RE-SAMPLE project meets the relevant compliance standards. For better evaluating the ethical and legal concerns the RE-SAMPLE project may raise, it is important to examine some of its particularities. More specifically, **three parameters should be mainly considered:**

a. Its focus on the healthcare sector;
b. Processing of special categories of data will take place during the project execution;
c. Use of AI/ machine learning models for analysing clinical and other patient data in order to identify predictors for the health status / disease progression of patients.

As far as the first parameter is concerned, it is clear from the project description that RE-SAMPLE will systematically address cybersecurity issues and threats in the health sector and will also ensure GDPR compliance. It is unquestionable that hospitals and health care centres are prime targets for cybercriminals, especially concerning data theft, denial-of-service and ransomware. Therefore, in comparison to other cybersecurity solutions, RE-SAMPLE will raise extra security, privacy and ethical concerns due to the sensitive character of the "market" it addresses. Issues related to vulnerable subjects (patients), informed consent as far as their participation in the project is concerned and the processing of their personal data, confidentiality (patients' confidential information), misuse of the project's findings and of course security issues are some of the parameters that will be examined below and are closely connected to the project's description and specifications.

The second parameter is directly related to the first one and refers to the processing of personal data that will take place while executing the project. In particular, RE-SAMPLE will involve the processing of specifically health data. Again, some serious concerns regarding the lawfulness of the processing, individual consent, the rights of the individuals whose data are being processed and of course the security of the personal data that have been collected are some of the issues that will be addressed.

In regard with the third parameter, even though RE-SAMPLE will employ AI for identifying specific disease predictors for the patients, this cannot be considered an "automatic decision" as it will be evaluated by the healthcare professionals who will take the final decision. Furthermore, the project will take all the necessary actions in order to protect the data and comply with the "Ethics Guidelines for trustworthy AI" [26].

4.2 RE-SAMPLE and ethics: compliance with ethical principles

4.2.1 The European Commission's checklist

As already mentioned in Chapter 2 of this deliverable, the task of identifying ethical issues and risks in research and of suggesting measures to minimise or prevent them, is the key for safeguarding that research will indeed be conducted and completed in accordance with ethical principles and values.

Based on the Commission's guidelines on how to complete an ethics self-assessment Table 3, the first step that needs to be taken in order to ensure that the RE-SAMPLE project is ethically compliant, is to check if the project falls within any of the following categories of research and if yes what extra measures should be undertaken to that direction.

Table 3: RE-SAMPLE Ethics self-assessment

1. HUMAN EMBRYOS/FOETUSES	
Does your research involve Human Embryonic Stem Cells (hESCs)?	No
Does your research involve the use of human embryos?	No
Does your research involve the use of human foetal tissues / cells?	No
2. HUMANS	

Does your research involve human participants?	Yes
Are they volunteers for social or human sciences research?	No
Are they persons unable to give informed consent?	No
Are they vulnerable individuals or groups?	No
Are they children/minors?	No
Are they patients?	Yes
Are they healthy volunteers for medical studies?	No
Does your research involve physical interventions on the study participants?	Yes
Does it involve invasive techniques?	Yes
Does it involve collection of biological samples?	Yes
If your research involves processing of genetic information, see also section 4.	
3. HUMAN CELLS / TISSUES	
Does your research involve human cells or tissues (other than from Human Embryos/Foetuses, i.e. section 1)?	No
4. PERSONAL DATA	
Does your research involve personal data collection and/or processing?	Yes
Does it involve the collection and/or processing of sensitive personal data (e.g: health, sexual lifestyle, ethnicity, political opinion, religious or philosophical conviction)?	Yes
Does it involve processing of genetic information?	No
Does it involve tracking or observation of participants?	Yes
Does your research involve further processing of previously collected personal data (secondary use)?	Yes
5. ANIMALS	
Does your research involve animals?	No
6. THIRD COUNTRIES	
In case non-EU countries are involved, do the research related activities undertaken in these countries raise potential ethics issues?	No
Do you plan to use local resources (e.g. animal and/or human tissue samples, genetic material, live animals, human remains, materials of historical value, endangered fauna or flora samples, etc.)?	No
Do you plan to import any material - including personal data - from non-EU countries into the EU?	No
Do you plan to export any material - including personal data - from the EU to non-EU countries?	No
In case your research involves low and/or lower middle income countries, are any benefits-sharing actions planned?	No
Could the situation in the country put the individuals taking part in the research at risk?	No
7. ENVIRONMENT & HEALTH and SAFETY	
Does your research involve the use of elements that may cause harm to the environment, to animals or plants?	No
Does your research deal with endangered fauna and/or flora and/or protected areas?	No
Does your research involve the use of elements that may cause harm to humans, including research staff?	No
8. DUAL USE	No
Does your research involve dual-use items in the sense of Regulation 428/2009, or other items for which an authorisation is required?	No
9. EXCLUSIVE FOCUS ON CIVIL APPLICATIONS	

Could your research raise concerns regarding the exclusive focus on civil applications?	No
10. MISUSE	
Does your research have the potential for misuse of research results?	No
11. OTHER ETHICS ISSUES	
Are there any other ethics issues that should be taken into consideration? Please specify	No

Based on the above checklist the main ethical concern raised is the one concerning processing of personal data and potential misuse of research findings for unethical purposes.

4.2.2 List of ethical issues in the RE-SAMPLE project

4.2.2.1 Research protocols and informed consent

Considering that during the research work of RE-SAMPLE there will be participation of patients (in various clinical studies that will be conducted), the project partners should ensure that prior to each study with patients' participation there will be "study package" that will have been approved by the appropriate ethics committee of the participating pilot Hospital (Data Controller). This study package should include:

- a study protocol,
- a patient information letter in the local language,
- an informed consent form in the local language,
- the registration number of the ethical committee,
- questionnaires, curricula vitae, and hospital-specific forms for ethical consideration (e.g. hospital costs of measurements)

Further details for the "study package" can be found in deliverables D5.1 and D9.1 H-Requirements.

Acquiring informed consent from the data subjects (patients) participating in the research is absolutely necessary in order to conduct research ethically. A valid consent should be:

a. freely given
b. obtained in advance
c. in writing
d. based on adequate and accurate information
e. freely withdrawn

Furthermore, it should include at least the following information:

- The purposes of the research and information about what will happen with the results of the research.
- The experimental procedures and a detailed description of the involvement of the participants, including the expected duration, and all the relevant procedures.
- All foreseeable risks or discomforts expected to occur for the research subjects during and after their participation.
- All benefits to the participants or to others which may reasonably be expected to occur.
- The insurance guarantees for the participants during and after participation and information on the foreseen treatments and compensations. Alternative procedures or treatments that might be advantageous to the participant need to be disclosed.
- Procedures in case of incidental findings.
- A description of the procedures adopted to guarantee the participant's privacy: the levels of confidentiality, the measures to protect the data, the duration of the storage of the data and what will happen with the data or samples at the end of the research.
- Contact details for researchers who can be contacted at any time to answer pertinent questions about the research and the participant's rights and that can be contacted in the event of a research related injury.

- A clear statement that the participation is voluntary, that the refusal to participate will involve no penalty or loss of benefits to which the participant would otherwise be entitled and that the participant may decide, at any time, to discontinue participation without penalty.
- Information about the organisation and funding of the research project

4.2.2.2 Civil application and dual use

All research activities carried out under the Horizon 2020 shall have an exclusive focus on civil application. The RE-SAMPLE project has a clear civil application use. Consequently, any further elaboration on potential dual use is considered unnecessary.

4.2.2.3 Vulnerable subjects

According to the Commission's European textbook on ethics in research, three main areas stand out as indications of subjects' vulnerability:

- Subjects who lack competence will be unable to protect their interests by choosing to give or withhold consent;
- If the voluntariness of the subjects' consent is compromised, this may similarly prevent them from choosing to give or withhold consent in a way that would protect their interests;
- The physical (or psychological) condition of some subjects leaves them especially liable to harm, for example as a result of frailty through age, disability, or illness.

Participation of people belonging to such categories in the RE-SAMPLE project **is not anticipated** for the project's duration.

4.2.2.4 Privacy / Confidentiality

The notions of Privacy and Confidentiality are considered related notions in research ethics. Both definitions suggest protection of a person's life, decision-making and personal information. In the case of the RE-SAMPLE project both principles should be considered. The reason for that is evidently connected to the involvement of human subjects in the RE-SAMPLE research. Respect for privacy indicates that the participants' decision to be involved in the first place and during the research should be respected. At the same time respect for the participants' private life should always be a main concern of the researchers/ RE-SAMPLE partners. The illness of the participants (patients) makes this obligation even more vital, given that, on the on hand these people may be exposed to higher risk of privacy violations and on the other hand any possible breach may entail serious concerns for the participants' wellbeing.

As with participants' private life, their personal information should also be treated with respect and with a high degree of confidentiality. The principle of confidentiality and how it could be protected in the context of the RE-SAMPLE project is closely connected to the data protection principle and therefore it will be examined thoroughly in the next chapter. It is however stressed that safeguarding confidentiality reinforces trust, and trust is crucial, when the subject decides to share with the project his/her valuable medical information.

Some of the major requirements that should be satisfied to comply with the principles of privacy and confidentiality are the following:

- the subject's informed consent should be acquired and be updated at all stages of the RE-SAMPLE project in the event of a change. The contents of the informed consent have been discussed in section 4.2.2.1;
- the subject needs to be always aware that he/she is part of a research;
- the consent should be freely withdrawn at all stages of the research;
- safeguard that the environment where the research takes place is appropriate. For instance, if the participants are being interviewed, that they will be able to do so in a private place;
- if family members of the participants are involved in the RE-SAMPLE research indirectly, that their privacy should be also respected;

- apply data protection mechanisms (indicatively: privacy by design and security by design methodologies). This will be examined below in section 4.2.2.5;
- take security measures for the protection of network and information systems;
- if there is the need to disclose confidential information acquire the prior written consent of the data subject;
- make sure that everybody involved in the process is bound by confidentiality obligations (either by law or by virtue of a non-disclosure agreement);
- take the necessary precautions to keep such information confidential even after the project has ended.

4.2.2.5 Protection of personal data

As already pointed out, the protection of personal data is a major ethic issue that needs to be addressed in all EU-funded projects. During the processing, specific measures should be adopted in order for the processing to be lawful and at the same time in order to safeguard the security of the personal data collected and of course of the data subjects' rights.

The nature of the data (health data) that will be processed during the RE-SAMPLE project makes the data protection parameter even more crucial. Therefore, extra requirements should apply to keep such data secure.

In RE-SAMPLE, and specifically in WP4, the data controllers (participating Hospitals) will be assisted to comply with the data protection legislation. More specifically, during the design phase of the RE-SAMPLE platform, the appropriate techniques will be adopted in order to fulfil the data protection by design and by default principles. Furthermore, it will be ensured that only personal data that are absolutely necessary for serving a specific purpose of processing are collected and processed, that they are stored for a predefined period of time, that the data subjects may easily exercise their rights as these are provided under the Regulation etc.

In addition, a DPIA study will be conducted in order to identify the most important risks against the freedoms and rights of the data subjects, the expected impact that a privacy violation incident may have on them and, thus, select the most appropriate countermeasures for protecting the data.

Finally, the appropriate Privacy Policies will be developed, taking into account the existing policies that the Hospitals may already have in force.

4.2.2.6 Information security

Information security has three dimensions: confidentiality, integrity, and availability of information. Information security plays an important role when it comes to research ethics. Keeping information, provided or generated during a project, safe, in other words safeguarding the integrity, confidentiality and availability of such information, should always be a high priority for everyone involved in research.
It has been already demonstrated that information, including sensitive information, such as medical data, plays an important role in the RE-SAMPLE project.

Information security will be achieved through the adoption of the appropriate organisational and technical measures. The specific measures will be the identified in WP4 of the project.

4.2.2.7 Trusted AI / Machine Learning

A cornerstone in RE-SAMPLE is the use of machine learning (ML) to get to suitable predictive models for the prognostics of multi-morbid exacerbations of Complex Chronic Conditions (CCCs). The used ML algorithms will be fed with patients' health data, both in the training of ML models as well as in their evaluation to compute predictions. Because of this central role of ML, WP3 of the project pays special attention to securing data while being processed in ML algorithms. This will be done through privacy-preserving approach of ML algorithms that allow for the training of models and their evaluation on

encrypted data in order to safeguard the data privacy of patients also during the use of it. To this end the project plans to go beyond the state-of-the-art in privacy-preserving ML by developing a tailored approach based on secure multiparty computation that allows for a fine-tuned trade-off between privacy, efficiency, and prediction performance.

5. Personal data protection in the RE-SAMPLE project

5.1 GDPR

This chapter sets out the data protection-related requirements for the RE-SAMPLE project. This means that the requirements listed below aim to, ultimately, ensure the GDPR compliance of the platform. The issue of GDPR compliance and transparency, in this respect, are of paramount importance, as they will set the correct example and will foster trust in the use of the platform from the end users as well as from the patients. In order to achieve said GDPR-compliance, organisational and technical security and privacy requirements need to be considered in the design and the development stages of all platform components as well as during all intermediate studies conducted for the elicitation of user related requirements (user requirements, retrospective data analysis, cohort study).

This chapter is therefore structured in two parts, dealing with privacy requirements for the design stage on the one hand and for the development stage on the other hand. While the requirements covered below are not exhaustive, it does provide an overview of the most important elements that need to be considered in order to make sure that the RE-SAMPLE platform itself complies with the GDPR. Specific analysis of the proposed organisational and technical security and privacy requirements will be conducted in the context of WP4 as an iterative analysis based on the ongoing findings depicted from WP2, WP3 and WP5 respectively. In this section an overview of basic GDPR related principles and primitive requirements driven through the ethical aspects of RE-SAMPLE project are described.

5.2 Design Phase

The role of controllers, whose specific obligations are set out in Article 25 of the GDPR described in section 2.4, is also of paramount importance in the design phase during which processing activities are envisaged.

Consequently, the RE-SAMPLE Partners have been required to consider appropriate measures and safeguards already when designing the Platform. The present section covers the key considerations that have been made in this phase.

The GDPR does not explicitly mention specific type of measures that need to be implemented to comply with this Article 25. It does however provide the factors that need to be taken into account when assessing and selecting the appropriate measures and safeguards. Determining 'appropriate' measures should notably be done "*taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing*"[1]

5.2.1 Determining the processing activities and their scope

The first element that needs to be considered, when designing RE-SAMPLE, is to specify the scope of all the processing activities that will be implemented and which will involve processing of personal data. In order to help the RE-SAMPLE partners with this preliminary assessment, the following list contains some key questions that will assist them to determine the scope and the details of the envisaged processing activities (if any). Please note that the list is not exhaustive and that other issues may need to be taken into account, in light of the specific context.

- Will any personal data be processed in the context of a specific RE-SAMPLE processing activity?
- Will any special categories of personal data be processed in the context of a specific RE-SAMPLE processing activity?
- For each of the processing activities envisaged, how will the personal data be collected?

[1] GDPR, art. 25(1)

- If personal data will be processed in the context of a specific RE-SAMPLE processing activity, determine the categories of personal data (including special categories of personal data) that will be processed.
- What is the purpose of each RE-SAMPLE processing activity?
- Will the personal data processed, for any of the processing activities envisaged, be disclosed to any recipients? If so, which personal data and to which recipients?
- If the personal data will be disclosed to recipients, are these recipients processors, controllers or joint-controllers?
- If the personal data will be disclosed to recipients, are these recipients located inside or outside the EU/EEA?
- What are the means used for the processing of any personal data?

The above elements merely provide the context in which the controller should consider the safeguards that should be adopted in order to comply with the data protection principles and the GDPR in general. Following this initial assessment of the processing activities, the rest of this Chapter will address certain key issues / questions that must be considered in order to ensure that the processing is in line with the data protection principles and complies with the other GDPR requirements.

5.2.2 The Data Protection Principle

The fundamental principles of the GDPR, listed and detailed in section 3.3, must also be taken into account during the design phase of RE-SAMPLE. The following list contains a number of key questions that will support the RE-SAMPLE Partners to ensure that any of the envisaged processing activities (determined on the basis of the checklist above) are in line with the fundamental data protection principles, or to determine the type of measures that should be taken in order to satisfy these data protection principles.

- How is it ensured that the data subjects, whose personal data is processed by RE-SAMPLE, are informed in a clear and simple manner about those processing activities?
- Has an appropriate legal basis been determined for each of the envisaged processing activities? In case of processing of special categories of personal data, which specific condition, under Article 9 of GDPR, is applicable?
- Have you specified the purpose for which each envisaged RE-SAMPLE processing activity is conducted?
- As regards the categories of personal data that will be processed by each specific processing activity, does this only include personal data that are adequate, relevant and limited to what is necessary in relation to the purposes for which they would be processed?
- Is it possible to carry out the processing using anonymized data?
- Is it possible that certain personal data that will be processed will become outdated at some point? If so, has it been considered how to keep this personal data up to date?
- Is it possible that certain personal data that will be processed are inaccurate? If so, has it been considered how these data can be rectified?
- Will all personal data that is collected in the context of RE-SAMPLE, only be kept in identifiable form to the extent strictly necessary in relation to the purpose(s) for which they are collected? Would this be the case in respect of (i) the amount of personal data collected; (ii) the extent of their processing; (iii) the period of their storage; and (iv) their accessibility? In other words: have appropriate retention periods been established for all categories of personal data?
- If personal data are kept in an identifiable form longer than strictly necessary in relation to the purposes for which they are collected, are these personal data processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of appropriate technical and organizational measures to safeguard the rights and freedoms of the data subject?
- Which accountability tools have been put in place to demonstrate compliance with the GDPR requirements?

5.2.3 Meeting Other GDPR Requirements

Apart from the obligation to introduce measures that implement the fundamental data protection principles, Article 25 of GDPR also stipulates that a controller must "*implement appropriate technical and organisational measures, such as pseudonymisation, which are designed […] to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects*". In the following sections, we will address the most important categories of GDPR requirements that need to be considered in the context of the RE-SAMPLE project.

5.2.3.1 Lawfulness of processing

For every RE-SAMPLE activity that involves processing of personal data it must be ensured that an appropriate legal basis has been determined. The GDPR sets out six different grounds for processing activities to be lawful, only one of which is relevant in the context of RE-SAMPLE: processing on the basis of consent.

5.2.3.2 Informing the Individuals

When processing personal data, through the RE-SAMPLE processing activities, it is necessary to ensure that the individual (data subject) knows about the processing and is informed of his or her rights under the GDPR. The GDPR provides a list of all information that must be provided to individuals. That information must be provided at the time when the personal data are collected. It should moreover be provided in a manner that is easily accessible and to the point, using clear and plain language.

Data subjects are typically informed of processing of their personal data through a privacy policy. This will be a crucial element for ensuring and demonstrating compliance of the RE-SAMPLE offered services with privacy requirements, as the privacy policy is easily accessible and visible to all.

5.2.3.3 Data Subjects' Rights

The GDPR gives a number of rights to individuals whose personal data are processed: the right of information, the right of access, the right to rectification, the right to erasure, the right to restriction of processing, the right to data portability, the right to object and the right not to be subject to automated decision-making. It should be ensured that individuals whose personal data are processed in the context of RE-SAMPLE are able to exercise these rights in an easy manner.

Thus the project should establish how the data subjects' rights will be dealt with; for instance through a dedicated central system for handling data subject requests such as a dedicated email address or web page.

5.2.3.4 Contractual Relations

It should be verified whether, in the context of RE-SAMPLE, third parties will be also involved in the processing of the personal data collected by the consortium and if so, whether this is truly necessary. If that is indeed the case, it is necessary to determine the status of that third party with respect to the personal data, i.e. controller, joint controller, or (sub)processor.

5.2.3.5 International Transfers

The GDPR provides for a general principle according to which the transfer of personal data to any country outside the European Economic Area ("EEA") is prohibited unless that third country ensures an adequate level of privacy protection. So far, the European Commission has recognised Andorra, Argentina, Canada (commercial organisations), Faeroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay and the United States of America (limited to the Privacy Shield framework) as providing adequate protection. In these cases, personal data can move freely as if it were a transfer within the EEA. The RE-SAMPLE Partners must therefore consider whether any such international transfer outside the EEA to a third country not offering an adequate level of protection is necessary. This would for instance be the case when deciding to rely on a US-based cloud service provider that does not adhere to the

EU-US Privacy Shield framework. In this case, personal data cannot be transferred freely without additional measures being in place.

5.2.4 Security of Processing

In addition to the legal and procedural requirements imposed by GDPR, it is crucial during the RE-SAMPLE design phase to identify all the security requirements that should be satisfied in order to achieve the required level of protection for the system and for the personal data being processed. While the requirements listed below are not exhaustive, they provide an overview of the most important elements that need to be considered in order to minimise the risk that any of the personal data is lost, unlawfully accessed, corrupted or in any way misused.

It is thus the responsibility of the RE-SAMPLE partners to implement appropriate security measures to prevent the personal data they process from being compromised in any way. This means that the partners will need to:

- Determine who is responsible for ensuring security of processing
- Make sure the appropriate organisational and technical security measures are in place
- Make sure that technical measures are backed up by robust security and privacy policies and reliable, well-trained employees
- Be able to respond to and remedy any breach of security swiftly and effectively.

According to GDPR, the data controller is responsible to determine the appropriate level of security for each one of the processing activities. The required protection level differs for each processing activity, as it depends on the actual risks faced by the processing activity in question but also on the severity of the impact that a potential security may have. Thus, before deciding what security measures to implement, the RE-SAMPLE partners need to conduct a risk assessment. To this respect, the following questions should be considered:

- Has a risk assessment been conducted to determine the appropriate level of security for each of the different processing activities envisaged in the context of RE-SAMPLE?
- Have the nature, scope, context and purposes of each of the envisaged processing activities been taken into account in the context of such a risk assessment?
- Has it been assessed, in the context of such risk assessment, how valuable, sensitive or confidential the processed personal data is to the individuals concerned?
- Has it been assessed, in the context of such risk assessment, what damage could potentially be caused to those individuals if a personal data breach were to occur? This includes in particular the risk of accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.
- Have the state of the art and the costs of implementation been taken into account in the context of such risk assessment?
- Has this risk assessment been documented and included in the relevant accountability file?

5.3 Development Phase

Once the initial privacy considerations have been made in the design phase of RE-SAMPLE, these considerations need to be translated into concrete measures and safeguards in the development phase. The present section is structured in the same manner as section 5.2 above. For each of the aspects addressed in that section, a list of questions is provided to help the RE-SAMPLE partners ensure that RE-SAMPLE is developed in a privacy-compliant manner. What follows constitutes a checklist to be considered in light of the activities of WP4 of the RE-SAMPLE Project.

5.3.1 General Considerations

Before addressing the specific processing aspects, it is important to consider several issues that may affect the choice of the protection measures that will be adopted. Indicatively, the RE-SAMPLE partners will notably have to:

- choose the appropriate measure among those available (i.e. within the 'state of the art')
- consider the cost of implementation

- consider the specific risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing
- Note that, when making the above assessment and considering specific measures, the factors relating to the state of the art of available technology and relating to the cost of implementation must not be interpreted in such a way that the measures chosen do not sufficiently mitigate existing risks and the resulting protection is not adequate. It should however be noted that less extensive measures may be required in case e.g. the extent of a certain processing activity is very limited and is considered to constitute a low risk to the rights and freedoms of individuals.

5.3.2 The Data protection principles

Without being exhaustive, this subsection includes a checklists to ensure compliance of the RE-SAMPLE platform with the data protection principles and the main GDPR requirements.

- Is the processing recorded / logged so as to be able to identify misuse of the data? If so, is the recording/log tamper-proof?
- In case personal data are automatically (or otherwise, e.g. on request) anonymised or pseudonymised the following criteria should be addressed: when that happens (timing), on what parameter does the decision to anonymise or pseudonymise personal data depend? How are pseudonymous data secured against too-easy re- identification?
- Are measures taken to avoid the creation of temporary shadow files (e.g. through unnecessary logging)? If such temporary shadow files are needed, how well are they protected against unauthorized access?
- If data are (intended to be) passed on to other controllers (or processors), are measures taken to filter out data that are not needed by the recipients?
- Are data disclosed internally only to those who need access and how is this ensured?
- Will any third party recipients be informed that they should only use the data for the purpose(s) for which they are provided? Are they asked to warrant that they will do so? Are such warranties binding? Can they be invoked by the data subjects?
- Is there a guarantee that all personal data, the actual personal data used and any back-ups, are erased or de-identified (really anonymised) when they are no longer needed for the purpose for which they were held? How is this done and verified?
- Can data that is no longer needed for the original purpose, but that cannot be erased due to retention rules (e.g. documentary reasons, tax regulations etc.) be blocked or otherwise excluded from regular processing?
- Which steps are taken to ensure that personal data that are inaccurate are erased or rectified without delay?
- What technical and organizational measures will be implemented to be able to demonstrate that processing is performed in accordance with the GDPR?
- Has an internal accountability file been created allowing the RE-SAMPLE partners to document and demonstrate GDPR compliance? The accountability file should contain, among others, records of processing activities, a list of IT systems, a list of data processors (and related contracts), an inventory of security measures, a data breach handling policy, requests from and responses to individuals, the information provided to individuals (policies) and any privacy-related risk assessments.
- Are risk assessments (such as DPIAs) conducted whenever required under the GDPR and are these risk assessments documented?

5.3.3 Meeting other GDPR requirements

This subsection provides a list of key questions that will support the RE-SAMPLE partners to implement the appropriate safeguards, into the envisaged processing activities, and thus ensure compliance with the most important GDPR requirements.

5.3.3.1 Legal Ground for Processing

- Is it ensured that the legal basis for the processing of personal data (informed consent for the RE-SAMPLE case) is explicitly explained to (and asked by) the data subjects?
- If so: Does the consent meets the associated legal requirements? This means that consent is (i) freely given, (ii) sufficiently specific, by setting out the purpose(s) of the various phases of the processing, (iii) informed, and (iv) unambiguously given by way of a statement or a clear affirmative action of the data subject?
- Where appropriate, are separate consents obtained for distinct processing purposes?
- How will it be demonstrated that the data subject has consented to the processing of his/her personal data?
- How is it ensured that consent can be withdrawn just as easily as it can be given?
- Is it ensured, when relying on legitimate interests, that decision-making in relation to the balance between the interests of the controllers (or relevant third party) and the rights of data subjects, is documented?

5.3.3.2 Transparency: privacy notice

- Is transparency, in respect of the data subjects, ensured with regard to the data processing (e.g. where appropriate data flow, data location, ways of transmission etc.)?
- Is an informative, up-to-date and understandable, well-indexed and/or searchable privacy notice in place, containing a description of RE-SAMPLE and the processing activities conducted in the context thereof? Is it simple to access the privacy notice? How will this be updated?
- Is the basic concept underpinning service clearly set out?
- Is there a privacy notice that provides sufficient information on relevant privacy issues resulting from the use of RE-SAMPLE (including e.g. use of cookies, processing of IP addresses)?
- Does the privacy notice provide specific and meaningful information about the processing of personal data instead of mere blanket confirmations of legal compliance?
- Is the concept of "highlight notices" (providing some high-level information at a glance) used?
- Is the privacy notice available in one or multiple languages?
- Has the personal data been obtained directly from the individuals (data subjects) or not? If so: has all the information appearing in the left column of Table 4 been provided to the data subjects? If not: has all the information appearing in the right column of Table 4 been provided to the data subjects?
- Is the information provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language?
- Where possible, is the information provided in combination with (standardised) icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing?
- Are there special measures to enhance transparency? Can specific processing steps be clarified to the individual?
- Does the privacy notice inform about all relevant aspects of the processing activities as required under Article 13 or 14 GDPR (see table below)?

Table 4: Information per case

Information to be provided	Data obtained from data subject	Data not obtained from data subject
Identity and contact details of controller, representative and DPO if any	□	□
Purposes and legal basis of the processing	□	□
Categories of personal data concerned		□
Any recipients / categories of recipients	□	□
The source and, if applicable, whether it came from publicly accessible sources		□
The existence of each of the data subject rights	□	□
The right to complain to a supervisory authority	□	□
Details of any transfers to a third country and safeguards	□	□
Retention periods or criteria used to determine retention	□	□
The right to withdraw consent at any time (where relevant)	□	□
The legitimate interests pursued by the controller or third party (where relevant)	□	□
Whether the provision of data is a statutory or contractual requirement, whether the data subject is obliged to provide it, the consequences of not providing it	□	
The existence of automated decision making, information about the logic involved, its significance and envisaged consequences	□	□

5.3.3.3 Data Subjects' Rights

- Has an internal procedure been established to handle data subject requests?
- Has it been assessed how to authenticate the data subject's identity, as well as when and how to verify such identity?
- Are there template for responses to access requests from data subjects?
- Are there procedures that allow the data subject to exercise their rights? Has this been verified for each of the different rights?
- Has it been assessed whether RE-SAMPLE needs a central system for dealing with data subject requests such as a dedicated email address or web page, and if so, has it been ensured that data subjects are informed thereof in the privacy policy?

5.3.3.4 Contractual Relations

- Has it been ensured that RE-SAMPLE data processors (if any) provide sufficient guarantees to comply with the GDPR?
- Where necessary, has a data processing agreement (containing at least the mandatory minimum content) been concluded with all service providers that will be acting as data processors?
- Where necessary, has an agreement of joint controllers been concluded?

5.3.3.5 International Transfers

- In case an international data transfer is conducted to a US-based organization, is it verified whether this organization adheres to the EU-U.S. Privacy Shield?
- In case an international data transfer is conducted to an organization established in a third country not ensuring an adequate level of protection, that is not a US organization certified under the EU-U.S. Privacy Shield, are SCCs foreseen / put in place?

6. Conclusions

The main purpose of the current deliverable is to provide to the project partners the necessary background information for the legal compliance and ethics management of the RE-SAMPLE project. To this end, it highlights the main ethical, legal and security/privacy issues that may arise during the project's life, and provides general guidelines, forming an internal policy document on legal and ethics aspects, to be considered by all RE-SAMPLE partners throughout the lifetime of the project.

Since this deliverable has been completed at an early stage of the project, additional requirements may arise during the course of the project. Any new requirements or/and the associated procedures/safeguards for fulfilling the requirements will be addressed in separate WPs and deliverables (for instance GDPR compliance in WP4) of the project.

7. References

[1]. Regulation (EU) No 1291/2013 of the European Parliament and of the Council of 11 December 2013 establishing Horizon 2020 - the Framework Programme for Research and Innovation (2014-2020) and repealing Decision No 1982/2006/EC.

[2]. Article 32(3) of the Regulation states that "By 31 December 2017, and taking into account the ex-post evaluation of the Seventh Framework Programme to be completed by 31 December 2015 and the review of the EIT, the Commission shall carry out, with the assistance of independent experts, selected on the basis of a transparent process, an interim evaluation of Horizon 2020, its specific programme, including the European Research Council (ERC), and the activities of the EIT [….]".

[3]. Ethics and data protection, European Commission, 14 November 2018

[4]. [ONLINE] The European Code of Conduct for research integrity (European Code of Conduct for Research Integrity of ALLEA (All European Academies), available at http://ec.europa.eu/research/participants/data/ref/h2020/other/hi/h2020-ethics_code-of-conduct_en.pdf , last accessed on 12/5/2021

[5]. Beauchamp TL, Childress JF. Principles of biomedical ethics (8th edition). Oxford University Press. 2019

[6]. World Medical Association. (2009). Declaration of Helsinki. Ethical principles for medical research involving human subjects. Jahrbuch Für Wissenschaft Und Ethik, 14(1), 233-238.

[7]. [ONLINE] Council of Europe, "Convention for the protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine", available at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/164 , last accessed on 12/5/2021

[8]. [ONLINE] Council for International Organisations of Medical Sciences (CIOMS) in collaboration with the World Health Organisation (WHO), "International ethical guidelines for health-related research involving humans (4th edition)", available at https://cioms.ch/wp-content/uploads/2017/01/WEB-CIOMS-EthicalGuidelines.pdf , last accessed on 12/5/2021

[9]. [ONLINE] European Commission, "Clinical trials - Directive 2001/20/EC", available at https://ec.europa.eu/health/human-use/clinical-trials/directive_en , last accessed on 12/5/2021

[10]. [ONLINE] European Commission, "Clinical trials - Regulation EU No 536/2014", available at https://ec.europa.eu/health/human-use/clinical-trials/regulation_en , last accessed on 12/5/2021

[11]. [ONLINE] International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use (ICH), "INTEGRATED ADDENDUM TO ICH E6(R1): GUIDELINE FOR GOOD CLINICAL PRACTICE E6(R2)", last accessed on 12/5/2021

[12]. [ONLINE] European Group on Ethics in Science and New Technologies, European Group on Ethics in Scioence and New Technologies, "Ethics of information and communication tecnologies", Publication Office of the EU (2012). https://op.europa.eu/en/publication-detail/-/publication/c35a8ab5-a21d-41ff-b654-8cd6d41f6794/language-en/format-PDF/source-77404276 , last accessed on 12/5/2021

[13]. [ONLINE] European Group on Ethics in Science and New Technologies, European Group on Ethics in Science and New Technologies, "Ethical issues of healthcare in the information society", Publication Office of the EU (2018). https://op.europa.eu/en/publication-detail/-/publication/ea106948-e6f5-11e8-b690-01aa75ed71a1/language-en , , last accessed on 12/5/2021

[14]. H. Rippen and A. Risk, "e-Health Code of Ethics (May 24)", J Med Internet Res., 2 (2000). https://www.jmir.org/2000/2/e9/

[15]. M. D. Wilkinson, et al., "FAIR Guiding Principles for scientific data management and stewardship", Scientific Data, 3 (2016). https://www.nature.com/articles/sdata201618

[16]. [ONLINE] "Open Science into Research Practice", The #OpenScienceClinique (2018). https://www.fosteropenscience.eu/sites/default/files/pdf/47783.pdf , last accessed on 12/5/2021

[17]. [ONLINE] E. Mendez, et al., "Progress on Open Science: Towards a Shared Research Knowledge System: Final Report of the Open Science Policy Platform", European Commission (2020). https://ec.europa.eu/research/openscience/pdf/ec_rtd_ospp-final-report.pdf#view=fit&pagemode=none , last accessed on 12/5/2021

[18]. [ONLINE] "Guides for Researchers: How to comply with H2020 mandate – for research data", OpenAIRE (2020). https://www.openaire.eu/how-to-comply-to-h2020-mandates-for-data , last accessed on 12/5/2021
[19]. [ONLINE] Gemelli University Hospital IRCCS. "CODICE ETICO", available at https://www.policlinicogemelli.it/wp-content/uploads-shared/2019/05/codiceetico2017-policlinico-gemelli.pdf , last accessed on 12/5/2021
[20]. OECD. Good Practice Principles for Data Ethics in the Public Sector, available at https://www.oecd.org/gov/digital-government/good-practice-principles-for-data-ethics-in-the-public-sector.pdf , last accessed on 12/5/2021
[21]. European Academies Science Advisory Council. "International Sharing of Personal Health Data for Research", available at https://easac.eu/fileadmin/PDF_s/reports_statements/Health_Data/International_Health_Data_Transfer_2021_web.pdf , last accessed on 12/5/2021
[22]. How, J. P. (2018). Ethically aligned design [From the Editor]. IEEE Control Systems Magazine, 38(3), 3-4.
[23]. Tschider, C. A. (2018). Deus ex machina: Regulating cybersecurity and artificial intelligence for patients of the future. Savannah L. Rev., 5, 177.
[24]. [ONLINE] Datatilsynet report: Artificial intelligence and privacy, available at https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf , last accessed on 12/5/2021
[25]. HLEG, A. (2019). A definition of AI: main capabilities and disciplines. Brussels. https://ec. europa. eu/digital-single.
[26]. [ONLINE] European Commission, "Ethics guidelines for trustworthy AI", available at https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai , last accessed on 12/5/2021
[27]. Mitrou, L. (2018). Data Protection, Artificial Intelligence and Cognitive Services: Is the General Data Protection Regulation (GDPR)'Artificial Intelligence-Proof'?. Artificial Intelligence and Cognitive Services: Is the General Data Protection Regulation (GDPR)'Artificial Intelligence-Proof.
[28]. [ONLINE] European Commission, "Guidelines 4/2019 on Article 25 Data Protection by Design and by Default", available at https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en , last accessed on 12/5/2021
[29]. [ONLINE] CIPL. "CIPL Recommendations on Adopting a Risk-Based Approach to Regulating Artificial Intelligence in the EU", https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_risk-based_approach_to_regulating_ai__22_march_2021_.pdf , last accessed on 12/5/2021