MISSIONE 4
ISTRUZIONE
RICERCA

BRIEF

BIOROBOTICS

RESEARCH AND

INNOVATION

ENGINEERING FACILITIES

D.7.4 CROSS-FIELD REGULATORY ANALYSIS II

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani
PIANO NAZIONALE DI RIPRESA E RESILIENZA

Quadro riassuntivo rilascio documento

Data	*Stato documento*	*Realizzato da*	*Note*	*Supervisione*
01.02.2024	Draft	*Denise Amram*	Table of Contents	*NA*
12.04.2024	Draft	*Pelin Turan*	Updates on IP issues	*Caterina Sganga*
28.04.2024	Draft	*Arianna Rossi*	Updates on AI – related issues	*Denise Amram*
06.05.2024	Draft	*Francesca Gennari*	Updates on MDR and Machinery Products – related issues	*Denise Amram*
06.05.2024	Draft	*Denise Amram*	Revisions	*NA*
16.05.2024	Draft	*Arianna Rossi Francesca Gennari Andrea Blatti*	Updates and case-scenarios	*Denise Amram*
29.05.2024	Final	Arianna Rossi Denise Amram	Feedback from workshop and formatting	*NA*

DISCLAIMER

This project has received funding by the Ministero dell'Università e della Ricerca (MUR), Direzione generale dell'internazionalizzazione e della comunicazione within the framework of the National Recovery and Resilience Plan (NRRP) within the call for proposals framework REFORMS AND INVESTMENTS UNDER THE RECOVERY AND RESILIENCE PLAN – Next Generation EU , Intervention field 6: Investment in digital capacities and deployment of advanced technologies DESI dimension 4: Integration of digital technologies + ad hoc data collections 055 - Other types of ICT infrastructure (including large-scale computer resources/equipment, data centres, sensors and other wireless equipment). Mission 4 – "Education and Research" Component 2: from research to business Investment 3.1: "Fund for the realisation of an integrated system of research and innovation infrastructures Action 3.1.1 "Creation of new research infrastructures strengthening of existing ones and their networking for Scientific Excellence under Horizon Europe.

TABLE OF CONTENTS

ABBREVIATIONS

List of abbreviations
AI: Artificial Intelligence
CDSMD: Copyright in the Digital Single Market Directive
CHIs: Cultural Heritage Institutions
CTR: Clinical Trials Regulation
DA: Data Act
DGA: Data Governance Act
DMA: Digital Markets Act
DRM: Digital Rights Management
DSA: Digital Services Act
EDS: European Data Strategy
EHDS: European Health Data Space
E&Ls: Exceptions and Limitations
EUIPO: European Union Intellectual Property Office
EU: European Union
GDPR: General Data Protection Regulation
ICC: Italian Civil Code
InfoSoc Directive: Information Society Directive
IP: Intellectual Property
IPRED: Intellectual Property Rights Enforcement Directive
IPRs: Intellectual Property Rights
MDD: Medical Devices Directive
MDR: Medical Devices Regulation
ML: Machine Learning
MR: Machinery Regulation
MS: Member State(s)
NB: Notified Body/ies
PLD: Product Liability Directive
PLDU: Product Liability Directive Update
R&D&I: Research & Development & Innovation
ROs: Research Organisations
SEPs: Standard Essential Patents
TDM: Text and Data Mining
TPMs: Technological Protection Measures
OHIM: Office for the Harmonization in the Internal Market

INTRODUCTION

This Deliverable builds on D7.3 to illustrate the applicable legal framework impacting on BRIEF activities, providing a unique crossed-field analysis aiming at developing useful policies and recommendations for stakeholders and researchers. Contents are developed considering the results of the survey launched under the Deliverable D.7.2. on the engagement strategy as well as the evolution of the applicable legal framework, emerging from the multitude of legislative initiatives launched by the EU dealing with data-driven solutions and new technologies.

The report focuses on the mapping of the existing laws developing the ethical legal framework for the BRIEF ecosystem and its scientific community. In addition, it will pay tailored attention to the current legislative initiatives (not yet approved or entered into force) and their interpretative impact on Research & Development & Innovation sectors (hereinafter R&D&I). In fact, either EU Directives or EU Regulations shall be implemented / adapted to the existing sectorial national regulatory framework with different degrees of effectiveness in the Member States (hereinafter MS). Once applicable, EU Regulations, in fact, are directly effective in MS, but some provisions may find national implementations and interpretations. While EU Directives provides principles that need to be mandatory implemented in a national law of each MS. In addition to such legislative scheme, the EU identified new principles and obligations may directly impact on national (and even local) procedures of compliance even if the legislative initiative has not entered into force yet. In fact, in case of normative lacks, the interpretations provided in the working progress of the EU institutions may constitute a parameter to address decision-making processes and policies. This is the case of the so-called *ethical legal compliance by design and by default*[1], a principle that is mentioned in several legislative strategies impacting on research and innovation and finds new content thanks to sectorial interpretations.

Therefore, a cross-field analysis of the existing normative constrains allows to identify interpretative gaps and enablers in tailored and concrete scenarios useful to develop practical policies and recommendations to solve common interpretative issues for BioRobotic-related activities. Together with this report, in fact, further 8 *Policy Briefs* (no. 9 to 16) are released to provide a more user-friendly perspective of the applicable legal framework (plus an update on the previously published policy brief no. 4). A panel has also been organised to better raise awareness on these matters and receive feedback from the BRIEF community of stakeholders and beyond.

To this end, this report constitutes a living document, including a preliminary analysis the application of specific principles into concrete scenarios relevant for the BRIEF RI and its stakeholders. It builds on D7.3, new sections are in purple, and will be further developed into D7.5.

[1] https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ethics-by-design-and-ethics-of-use-approaches-for-artificial-intelligence_he_en.pdf.

2. METHODOLOGY

2.1. Cross-field regulatory analysis workflow

To design and create cutting-edge innovative solutions compliant with the complex system of enforcing regulations, it is important to precisely identify what the legal requirements are and how to deal with the ones that are about to be implemented, considering the evolution of the relevant framework impacting on R&D&I sectors. It was therefore important to draw up a first map of the theoretically relevant legal acts and then have a survey filled under D.7.2. to verify whether:

- the selected legal initiatives are relevant and, in case of gaps, the interpretative principles to address them;
- the regulatory and legal blocks affect innovation and to which extent;
- the EU legislative initiatives that are not into force may already perform as a useful interpretative parameter of the public health and data strategies.

The applicable legal framework is not only consisting of the legal requirements established by EU/national/local statutory law, but also of the complex ethical values transposed into either general or sectorial administrative procedures. The latter are establishing obligations and duties in order to accomplish with recognised standards applicable to a given scenario for certain purposes (*e.g.* ethical committees ones) as well as to a general principle of accountability (useful to avoid sanctions).

The aim of this deliverable is to finally delve into the fields of analysis selected under D.7.2., in order to build up a more clear and understandable state of the art of ethical legal framework applicable to the BRIEF ecosystem, aiming to design cutting edge BioRobotic devices, solutions, and allied technologies.

As anticipated, considering this cross-field analysis as a preliminary one, the current workflow arises from the combination of current compliance requirements, developed legal standards, and regulatory insights.

Thus, this report builds on the first analysis developed in D7.3 comprising the legal framework shaping the EU strategy on data and public health in order to highlight the interpretative issues emerging in concrete scenarios in R&D&I sectors, due to gaps and inconsistencies. Following the co-creation approach, the first version of this report (D7.3) has been presented in the first Awareness Panel on 20.07.2023 titled "*Tecnologie BioRobotiche e abilitanti: il quadro giuridico di riferimento. Scenari operativi*" to the consortium and stakeholders to receive preliminary feedback, highlighting the importance to not only establishing, but also maintaining a continuous dialogue with institutional and private stakeholders for the following versions (such as this report D.7.4. *and the following iteration D7.5*).

In this report, we take the chance to illustrate the recently approved text on European regulation on artificial intelligence (AI Act) that is not into force yet, but it had already become an essential frame of references for current analyses in for AI deployers and developers. In addition, we introduce relevant issues emerging within the Intellectual Property Rights domain. The content of D7.4 has been presented to the consortium's members on 20th May 2024 workshop, titled "BioRobotic and allied technologies: the legal framework. Operational scenarios II" as well. It allowed the audience to address the ethical legal issues emerging from the cross-field regulatory

initiatives like the Intellectual Property Rights, Artificial Intelligence, and Medical Devices legislations.

During both events, the structure and methodologies adopted in WP7 have been considered useful and well placed to achieve the project objectives. Received feedback have been embedded in the final draft of the report.

2.2. Compliance, standardisation, and regulation

The described workflow shall be interpreted as a consequence of a general methodology, developed within the research line ETHOS EThics and law witH and fOr reSearch (www.lider-lab.it) at LIDER Lab, DIRPOLIS Institute, Scuola Superiore Sant'Anna, that is remarkably applicable to the BRIEF RI activities.

In fact, in order to understand the societal impact of R&D&I nowadays, it is extremely useful to adopt a bottom-up approach, that starts from the roles and responsibilities allocation and compliance obligations analysis in order to verify whether or not existing standardisation mechanisms are applicable to the specific scenario or if further efforts shall be addressed to develop common practise and solutions.

In fact, if we consider that the multitude of the initiatives developed by the EU Commission on digitalisation, datafication, and innovation have the purpose to shape an inclusive digital society, all the services and products of the EU data economy cannot be avoided neither by the ethical-legal framework nor from the market. In addition, EU strategy on public health is increasingly aligning with the challenges launched by the data science and technological progress, thus establishing common procedures to perform clinical trials and develop medical devices in a digitalised healthcare system aiming to pursuing objectives of predictive, personalised, participative, precision, and preventive medicine, paying attention to AI-based applications and the establishment of common spaces of electronic health data.

Common principles shared among the different initiatives are crucial to interpret the possible overlapping and inconsistencies as well as to cover gaps in concrete scenarios. For example, the principle of accountability ensures that in each sector where a technology is introduced a human-centric perspective has been not only addressed, but also enhanced and empowered in all the life-cycle of a given study, service, product. This is true either for the general right to dignity or for its epiphanies, including privacy and data protection, autonomy, health, etc.

Therefore, this report provides a cross-field analysis including legal issues arising from human participation in clinical and non-clinical studies, personal and non-personal data governance, and protection in big and "small" data flows, human oversight, and empowerment before technology.

According to the first models developed to understand human behaviour before technology the grounds of usability, acceptability, and feasibility are the ones generally tested to ensure a concrete success of the solution in the market. Currently, to take an accountable behaviour in R&D&I sectors is essential not only to avoid sanctions within a rigid system of duties and obligations, but also to understand the regulatory challenges aiming to protect and promote fundamental rights.

The analysis of the existing interplay between compliance activities, identification of common practices and legal standards, as well as contribution to the regulatory debate helps to develop methodologies that – together with the technical activities – are promoting human dignity and the other EU values for a more inclusive society. Therefore, policy and recommendations that are completing this report aim to drive researchers and innovators both in the digital transition of traditional services and products development life-cycles and in advancing frontiers in biorobotics by adopting a responsible and accountable approach *by design* and *by default.*

Considering the role of BRIEF RI in the scientific research community, several opportunities to test the efficacy of the proposed approach towards ethical and legal compliance could not only improve and tailor specific procedures but also providing a unique opportunity to harmonise practices and act as – at least – national standard of compliance for provisions already into force and upcoming ones.

2.3. Comparative law approach contribution

Many legal studies are recently dealing with the challenges launched by the technological innovation. The added value provided to this report refers to the comparative law methodology that has been adopted to undertake the cross-fields analysis.

In fact, the analysis compares the hard law (mainly EU regulations and directives, and Italian laws) with the provisions that are included in ongoing proposals, and the law in action, therefore the current interpretations emerging from concrete scenarios.

Such a check of the coherence of the various provisions introduced or about to be introduced in the mentioned strategies at EU level provides the unique opportunity to assess whether the operational rules are concretely compatible both with the theoretical propositions and the practical needs emerging from the R&D&I life-cycles.

As a consequence, it would be easier to develop guidelines and recommendations able to promote systematic interpretations to be addressed for policy and law-making purposes, and – at the same time - to drive the R&D&I players towards more responsible approaches in shaping innovative methodologies coherent with the applicable values.

3. MAPPING OF THE RELEVANT LEGAL FRAMEWORKS

The following mapping of the legislative initiatives is developed following the current European Commission Strategies on Data, Public Health, Artificial Intelligence (AI), and Intellectual Property (IP) related ones as the four main fields in which the development of BioRobotic solutions may be framed.

In particular, data-driven research activities are daily dealing both with personal and non-personal data governance, facing also the challenges of openness, to provide replicable and reproducible studies, that may also include human volunteers. To this end, the interplay between public health interventions and the data strategy shall be addressed both to preserve individual rights of engaged volunteers in the given case, and the category of vulnerable groups.

In addition, data flows are functional to the development of innovative methodologies of data analysis, also based on algorithms, Machine Learning (ML) and other AI-based techniques. Thus, to address the values and the assessments already identified in the forthcoming regulation on AI, even if it doesn't constitute a binding obligation yet, can be a relevant standard to be followed in order to place into the market a product aligned with the EU values and requirements. At the same time, it is the opportunity to develop procedures in order to start implementing the conformity checks in the life-cycle/supply chain, anticipating the effects of the AI packages compliance activities (*ie* anticipating also costs and efforts allocation) in the current transition due to the new conditions established under the Medical Device Regulation and Clinical Trials Regulation and their national implementations.

The IP framework is also of pivotal importance both for the BRIEF activities and the BioRobotic field. Indeed, the IP framework informs and governs the various phases of R&D&I activities in the field, including those necessitate accessing information and technology on the state of the art in the field, conducting research activities by employing text and data mining (TDM) methods, training AI models with large datasets of various types of data, 3D-printing of robotic parts and the like. These examples are far from being exhaustive and can be easily multiplied – yet they are sufficient to justify the crucial role that IP plays in scientific research.

In this regard, the interplay of IP law with the BRIEF activities and the biorobotic fields is two-folded. On the one hand, the earlier stages of the R&D&I lifecycle require defining the state of the art, hence having access to, analysis, and use of the existing knowledge and technology in order to identify the current trends and gaps as well as to develop novel solutions to the unresolved problems in the field. Successful operationalisation of this endeavour, however, requires the analysis of and building on the existing scientific content, often, protected by conventional forms of intellectual property rights (IPRs), such as copyright, patent, trade secrets, and industrial design. On the other hand, the latter stages of such R&D&I activities are expected to result in scientific output eligible for IPRs-protection, such as scientific publications and inventions of the researchers and research organisations (ROs) included within the BRIEF network. Therefore, it is essential to lay a solid groundwork for the BRIEF consortium and activities to help clarify the ways in which the BRIEF network can tackle third-party IPRs in the context of scientific research and exploit the prospective scientific output of such research endeavours by utilising their prospective IPRs. In terms of policy making, the following analysis will be functional to highlight how a RI could exploit the research data generated, fostering the openness principle and contributing to the common data spaces, including in the

medical domain the opportunities that the European Health Data Space proposal is launching for the researchers.

3.1. The European Data Strategy

The European Data Strategy is the policy and legal framework that sets the principles and objectives to which the different EU legislative initiatives that we are analysing refer. Its main goal is to "*make the EU leader in a data-driven society*"[2]. More specifically, this means to create a single market for data. The advantage of this operation is that to have clear rules on how to use data will also allow it to freely flow within the EU[3]. This will enable public and private stakeholders, as well as EU citizens to re-use data both personal and non-personal (and by respecting at the same time Intellectual Property Rights) and across economic sectors.

The data-sharing and data-reuse will favour the creation of new products and services, especially on secondary markets and will benefit society, thus including businesses, research institutions, and public administrations[4]. Furthermore, comparing, and contrasting data and metadata extracted by documents is also of capital importance for better policy making and to allow an upgrade in public services.

It is also important to clarify that the rules that are published at an EU level do not just allow data to freely flow across EU countries. There are also some legal and ethical counterbalances to this principle. In fact, free flow of data does not mean that it can happen without considering privacy and data protection aspects, especially when personal data is involved. Moreover, there is also the need to balance rules to access the market to provide anyone who wants to enter/join the EU Digital Single Market to do it in compliance with fair competition principles[5]. The rules on data sharing and data re-use, finally must be "*fair, practical and clear*"[6].

The EU data strategy's articulation is complex but can be simplified in some main themes and guidelines:

- *"setting clear and fair rules on access and re-use of data*
- *investing in next generation tools and infrastructures to store and process data*
- *joining forces in European cloud capacity*
- *pooling European data in key sectors, with common and interoperable data spaces*
- *giving users rights, tools and skills to stay in full control of their data*"[7]

The different initiatives included in the European Data Strategy will be illustrated as a parameter to analyse the existing and already into force provisions shaping the ethical legal boundaries for biorobotic solutions.

2 See more at: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en, accessed 03 July 2023.
3 Ibid.
4 Ibid.
5 Ibid.
6 Ibid.
7 Ibid.

3.1.1. The General Data Protection Regulation

Even though the General Data Protection Regulation is not formally part of the current European Data Strategy, it is important to cite it, as it is the initiative that influenced the creation of all the following acts and proposals concerning the building of the Digital Single Market. Hence, **the GDPR sets the rules to protect personal data**, but, at the same time, strives to outline the rules through which personal data can **also be safely used and shared across the EU** for several purposes, including medical research, archive, and statistical ones. It applies to personal data, namely **any kind of information, in any format making a person** (*i.e.* the data subject) **identified or identifiable**. Personal data might also reveal specific characteristics of the data subject, that may expose her as a vulnerable individual or belonging to a vulnerable group. This is the case of, for example, health-related data and biometrics ones that are expressly considered as "belonging to particular categories of data", and therefore a more restrictive regime is applicable for lawfully process them as identified by article 9 GDPR. In these cases, pseudonymisation and encryption are those technical and organisational measures that could be applied as soon as possible to data flows processed for research purposes.

3.1.2. The Free Flow of Non-Personal Data Regulation

The reciprocal initiative respect to the GDPR is the regulation concerning the **Free Flow of Non-Personal Data** (FFNP). This regulation was drafted with the aim to ensure, among other things

- "*Free movement of non-personal data across borders: every organisation should be able to store and process data anywhere in the EU.*
- *The availability of data for regulatory control: public authorities will retain access to data, even when it is located in another EU country or when it is stored or processed in the cloud.*
- *Easier switching between cloud service providers for professional users. The Commission has started facilitating self-regulation in this area, encouraging providers to develop codes of conduct regarding the conditions under which users can move data between cloud service providers and back into their own IT environments.*
- *Full consistency and synergies with the cybersecurity package, and clarification that any security requirements that already apply to businesses storing and processing data will continue to do so when they store or process data across borders in the EU or in the cloud*"[8].

The further evolutions stemming from the FFNP consisted in the Digital Governance Act (DGA) and also the Data Act (DA) which will be respectively described.

3.1.3. The Data Governance Act

[8] See more at: https://digital-strategy.ec.europa.eu/en/policies/non-personal-data#:~:text=The%20Regulation%20on%20the%20free,and%20IT%20systems%20in%20Europe. Accessed 11 July 2023.

The **DGA main aim is to set the rules to facilitate and safeguard data sharing and reuse across sectors and Member States, such as from the public sector to the private one** when the Open data directive does not apply such as when the data concern individuals (e.g., health data) or companies (e.g., financial information). Whenever public entities make available personal data, they will also need to be equipped with privacy-friendly and security-enhancing tools and mechanisms that ensure the confidentiality of the data they share. The DGA also strives to create new entities whose main function will be to act as **data intermediaries to create a functioning and regulated data economy**. Data intermediaries are meant to add a layer of trust between the entities that share data, as they will be "neutral" entities without any proper interest in the sharing of data and they will need to notify the competent public authority of their intention.

Moreover, the DGA enables people to voluntary share their data, such as their health data, for non-commercial use that benefits communities or society at large (*i.e.*, data altruism), such as for scientific research purposes. This could mean that a person might share the results of a certain medical examination for free with a State-approved data altruism authorised body which will equip organizations with the possibility to reuse that data.

Lastly, the DGA lays down the rules for the creation of common European data spaces that are going to be domain-specific (e.g., health, mobility, skills, finance, etc) and will enable the flow of data between private and public organizations. Data spaces will be composed of both a secure technological infrastructure and governance mechanisms for trustworthy and not expensive data exchange. Vertical legislation, such as the European Health Data Space Regulation (see below), will complement the DGA by providing domain-specific rules and requirements.

3.1.4. The Data Act

The EU Regulation 2023/2854 (the Data Act) **sets clear rules concerning how private subjects should access data** that are generally generated by Internet of Things (**IoT**) objects in order **to create new products and services on secondary markets**. Moreover, the Data Act establishes rules concerning fairness in data sharing contracts, interoperability, and switching between cloud providers. In addition, a part of the DA aims at governing the relationship between the EU institutions, the MS and the private parties to share data in emergency situations such as the case of a pandemic.

Many of the DA's provisions are meant to **facilitate scientific research activities**. First, the DA introduces rules regulating situations where businesses are obliged to share data but can ask for a "reasonable compensation" from the data recipient. However, if the data recipient is a non-profit research organisation (or a micro-enterprise or a SME), it **cannot be charged more than the costs incurred for making the data available**. Second, when there is an exceptional need for purposes of public interest (e.g., during a public emergency but also non-emergency situations) and under specific terms and conditions, public bodies are authorized to access the data held by private entities. **Public entities may also share the data with research-performing and research-funding organisations** when they cannot carry out scientific research activities or analytical activities themselves, provided that the purpose of use is compatible with the purpose for which the data was requested. Third, the DA lays down **essential requirements** (e.g., about data formats and shared formal vocabularies) **to allow data**

to flow within and between data spaces that are meant to bolster data exchange within data spaces, thereby preparing the ground for enhancing the interoperability of data processing services. The necessary harmonised standards and open interoperability specifications, as well as the requirements mentioned above, will foster research and innovation activities.

3.1.5. The European Health Data Space

Another essential part of the European Data Strategy is the creation of common **European Data Spaces** which should be **protected and interoperable data storage infrastructures** that serve the purpose of having data lakes in the EU that are characterised by a particular feature. For instance, in the European Data Strategy there is a proposal to create a IoT manufacturing safe data space and a health data space among others.

In particular, the European Health Data Space (EHDS) proposal includes "*rules, common standards, and practices*"[9] for the **safe and secure exchange of electronic health data**, which are considered special categories of personal data and thus undergo the safeguards provided by and has two main functions which interest health data, whose regime of processing is described by article 9 GDPR. The EHDS sets several ambitious goals.

First, the EHDS intends to **enable the exchange of data for the delivery of healthcare across EU Member States and facilitate individuals' control** over their own health data. This is referred to as **primary use of data,** as it concerns data directly generated by or collected from patients to assess, maintain or restore the state of health. The EHDS also requires all electronic health record systems to comply with the specifications of the European electronic health record exchange format, thereby going beyond national fragmentation and ensuring that they are interoperable at EU level. In this way, individuals will be enabled to access and control their electronic health data without the fear of losing their data, or not be able to "carry" their own health data with them should they change country or experience a health emergency in another EU country.

Second, the EHDS aims at **strengthening secondary use of data across organizations and national borders for research, innovation and public health purposes**. Secondary use occurs when the data are re-used for purposes that are different from the purpose for which the data was originally collected or produced, for example when data collected for medical treatment is then re-used for furthering scientific research. Thanks to **closed, secure processing environments**, organizations will be able to **more effectively and more conveniently access to health structured datasets for further reuse**, overcoming the barriers related to the lack of data and avoiding the duplication of data collection activities, while respecting data protection requirements. The secondary use of data is especially relevant for those **research projects that develop new tools that need health-related datasets for training and validation.** The EHDS will make available relevant data, such as medical images in a secure manner to e.g., optimize the performance of AI-based medical decision-support systems, among the others.[10]

[9] See more at: https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space_en, accessed 03 July 2023.
[10] See other examples at: https://ec.europa.eu/commission/presscorner/detail/en/QANDA_24_2251, accessed 30 April 2024.

In spring 2024, the European Parliament and the Council reached a political agreement on the Commission proposal for the EHDS. This agreement amends the original Commission's proposal in a number of elements, such as allowing Member States to apply stricter measures on certain types of sensitive data (e.g., genetic data) for research purposes and to establish trusted data holders that can securely process requests for access to health data.[11]

3.2. Public health

The second main EU framework to take into consideration while mapping the relevant applicable EU laws and proposals concerns public health. It focuses on mainly three instruments that have been modified recently and that are still being implemented at a national level because of their complexity. Those legislative acts are Regulation (EU) 2017/745 on Medical Devices[12] (hereinafter referred to as Medical Devices Regulation, MDR) and the Regulation (EU) 2017/746 on In Vitro Diagnostic Medical Devices[13]. Considering the stakeholder consultation undertaken in D.7.2. our analysis will only focus on the MDR as it is the legislative act that is mostly connected to the partners and stakeholder's businesses and interests. Thirdly, we will also deal with the Clinical Trial Regulation EU 536/2014 (hereinafter referred to as CTR)[14] which harmonised the sector by repealing the precedent Clinical Devices Directive since last 31 January 2023.

3.2.1. The Medical Devices Regulation (MDR)

The previous Medical Devices Directive (MDD)[15] has been repealed by the present MDR, maintaining some similarities. Firstly, they both share the principle of the division of the different medical devices in several categories according to the risk that they might cause to humans (classes I, IIA, IIB, III). Secondly, according to the level of risk for human health that the device could cause, there is a differentiation concerning the certification and audit procedures that the medical device has to go through before being put on the market.

Thirdly, it is specialised audit and certification bodies registered with the EU Commission, the Notified Bodies, that do carry out certification compliance operations and they judge whether the medical device can obtain a CE marking. Only if the Notified Body considers that the device is compliant with a specific certification MDR procedure (that are set according to the device

[11] To learn more: https://www.consilium.europa.eu/en/press/press-releases/2024/03/15/european-health-data-space-council-and-parliament-strike-provisional-deal/, accessed 30 April 2024.

[12] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (Text with EEA relevance.) OJ L 117, 5.5.2017, p. 1–175.

[13] Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU (Text with EEA relevance.) OJ L 117, 5.5.2017, p. 176–332.

[14] Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC Text with EEA relevance OJ L 158, 27.5.2014, p. 1–76.

[15] Council Directive 93/42/EEC of 14 June 1993 concerning medical devices OJ L 169, 12.7.1993, p. 1–43.

level of risk) and that all the relevant EU rules about the respect of the best standards of quality and safety for this kind of product and the technological state of the art are respected, the Notified Body gives its authorisation for the device to circulate within the EU. However, a significant improvement of the MDR compared to the MDD was the introduction of post-market surveillance duties. In fact, previously, there was no way in which it was possible to monitor its functioning after it had been marketed. This necessity emerged after the defective breast-protheses case[16], which made it clear that the system needed to be updated and that also post-market surveillance duties needed to be implemented. Moreover, the previous MDD was drafted in a time when the development of technologies applied to health, including biorobotics, AI, IoT and allied technologies was still at the beginning. The MDR already considers software, at certain conditions, as a medical device[17], even though it does not explicitly mention neither AI nor biorobotic or other allied digital technologies.

One of the main differences between the previous system is that the MDR is a regulation, and, according to EU law it must be applied as is (unless there are explicit indications in the text on the basis of which some form of leeway is explicitly given to the Member States). Conversely, a directive is a harmonisation legislative tool which is binding just as far as the targets to meet, therefore MS do have a certain level of freedom while implementing them into national legislative initiatives. The directives allow for EU provision to better adapt to one MS legal tradition, but they risk increasing the legal fragmentation in the single market instead of reducing or harmonizing it. Given that the highest level of protection of human health was the main objective of the MDR and given that the previous medical device scandal had lowered the trust EU patients had towards the Notified Body system, the MDR is in fact a regulation and not a directive anymore.

Summing up, below follows the main objectives that the MDR aims to achieve are the following ones:

- "***stricter previous control for high-risk devices*** *via a new pre-market scrutiny mechanism with the involvement of a pool of experts at EU level*
- ***reinforcement of the criteria for designation and processes for oversight of notified bodies***
- ***inclusion of certain aesthetic devices*** *that present the same characteristics and risk profile as analogous medical devices under the scope of the regulations*

[16] The case involved the PIP manufacturer which specialised in breast implants, which were considered as medical devices and certified by a Notified Body (NB), TUV France, whose main legal seat was in Germany. PIP secretly altered the composition of the implants, and many women with PIP defective breast implants experienced pain, were hurt or were forced to have surgery again. However, the manufacturer had gone bankrupt in the meantime, and the affected women could not ask for compensation from it. Hence, a woman tried to get compensation by the NB, TUV, by relying on the rationale of the then Medical Devices Directive (MDD). The CJEU in the *Schmitt* judgment stated that the directive did not explicitly refer to the NB's liability but that it was up to the MS to set whether there could be a specific NB liability. If that was the case, that form of liability or remedy had to be necessary and proportionate with the EU legal order. See Judgment of the Court (First Chamber) of 16 February 2017. *Elisabeth Schmitt v TÜV Rheinland LGA Products GmbH*., Case C-219/15, ECLI:EU:C:2017:128

[17] Article 2(1) MDR.

- ***a new risk classification system for in vitro diagnostic medical devices*** *in line with international guidance*
- ***improved transparency*** *through a comprehensive EU database on medical devices and a device traceability system based on a unique device identification*
- ***introduction of an 'implant card'*** *for patients containing information about implanted medical devices*
- ***reinforcement of the rules on clinical evidence****, including an EU-wide coordinated procedure for authorising multi-centre clinical investigations*
- ***strengthening of post-market surveillance*** *requirements for manufacturers*
- ***improved coordination mechanisms*** *between EU countries in the fields of vigilance and market surveillance*"[18].

As of May 2021, the manufacturers have to comply with the several new obligations that are set in the MDR. However, because also of the COVID-19 pandemic, the MDR implementation was further delayed through a series of decisions and implementing acts[19].

3.2.1. Personalizing medicine: the case of custom-made medical devices.

According to the MDR a custom-made device is '*specifically made in accordance with a written prescription of any person authorised by national law by virtue of that person's professional qualifications which gives, under that person's responsibility, specific design characteristics, and is intended for the sole use of a particular patient exclusively to meet their individual conditions and needs.*'[20] For instance a teeth retainer or an orthopaedic corset or a limb prosthesis.
To have a custom-made device **a specific kind of prothesis** to be made, **then this is a custom-made device** if it is done according to the patient's characteristics and needs. However, '*mass-produced devices which need to be adapted to meet the specific requirements of any professional user and devices which are mass-produced by means of industrial manufacturing processes in accordance with the written prescriptions of any authorised person shall not be considered to be custom-made devices*'[21]. This means that a mass-produced pace-maker is not a custom-made device, but a soft and artificial organ designed for a specific person is.
The difference is relevant as custom-made device manufacturers have specific obligations, such as to draw up technical documentation[22] and will need to follow the procedure described at Annex XIII of the MDR. Here is a brief sum-up of the procedure explained.

Section 1: Contents and form of the official statement that the manufacturer or the authorized representative needs to draw up: e.g. name and address of the manufacturer, statement that the device needs to be used only by a particular patient.

Section 2: The manufacturer needs to make all the documentation concerning the custom-made devices for the Member State authority (The Ministry of Health in Italy) to allow the conformity

[18] See more at https://health.ec.europa.eu/medical-devices-new-regulations/overview_en accessed 03 July 2023.
[19] See more at https://health.ec.europa.eu/medical-devices-sector/new-regulations_en accessed 03 July 2023.
[20] Article 2(3) MDR
[21] Article 2(3) MDR
[22] Article 10(2) (4) MDR

assessment with the MDR requirements including the site where the custom-made devices are manufactured.

Section 3: The manufacturer must ensure that there is a correspondence between Section 2 requested documentation and the manufacturing process.

Section 4: the statement drew up according to section 1 must be kept for a period of **10 years**. If it is an implantable custom-made device **15 years**. The quality management procedure described in Annex IX Section 8 applies.

Section 5: The manufacturer will review and document its marketing experience after the product is manufactured and marketed by following the Post Market Clinical Follow-Up (PMCF) described at Annex XIV part B and '*implement appropriate means to apply any necessary corrective action'* [23]. This means that **there must be a plan, which shall be periodically revised in which there will be the specification of methods and procedures to proactively collect and evaluating clinical data to confirm the safety of the custom-made device and of identifying unknown side effects**[24]. This procedure aims to manage the risk that custom-made devices might have on an individual's health. Another important obligation is to report accidents to the competent authorities (the Italian Ministry of Health) according to the Article 87(1) MDR procedure.
BRIEF internal actors could fall under the definition of custom-made medical devices. Moreover, Italy has started implementing this part of the MDR with a specific decree (see Policy Brief no. 9).

[23] Annex XIII MDR Section 4
[24] Annex XIV MDR Section 6.1

PILLS OF MDR. CUSTOM-MADE DEVICES (ANNEX XIII MDR)
*Documents need to include the manufacturer's data as well as a **statement of the patient's needs***
*The **Italian National Ministry of Health** is the point of contact for the Italian custom-made medical devices' manufacturers to check the conformity of the device and the correctness of the technical documentation submitted*
*The manufacturer must ensure that there is a **correspondence** between section the requested documentation and the manufacturing process*
*The statement drew up according to point 1 of this table must be kept for a period of **10 years**. If it is an implantable custom-made device **15 years**. The quality management procedure described in Annex IX section 8 applies*
***Post Market Clinical Follow-Up (PMCF) duties for the manufacturer** described at Annex XIV part B and 'implement appropriate means to apply any necessary corrective action'* *Need to have a **plan**, which needs to be **periodically revised**, in which there will be the specification of methods and procedures to **proactively collect and evaluating clinical data** to confirm the safety of the custom-made device and of identifying unknown side effects* *Obligation to **report accidents** to the Italian National Ministry of Health*

Table 1 illustrates the key provisions concerning custom-made devices of the Medical Devices Regulation

3.2.1. When is Software a medical device?

Article 2 of the Medical Devices Regulation (MDR[25]) **expressly includes software as a medical device**. It is the same for the In Vitro Devices Regulation (IVDR[26]) at Article 2(1) IVDR. Although software must be considered a medical device **if it has a medical function** as explained in the same article 2 it is difficult to tell in practice whether software has a medical function or not.

The Medical Devices Coordination Group[27], which is an EU expert pool on medical devices, affirmed it in a policy document in 2019. The impact of this perspective is relevant for all BRIEF actors as they might develop software with a medical function and need to follow the MDR rules in order to put it into service in the EU market (see Policy Brief no. 10).

Consider that **when software is a medical device it will need to be certified** as such, following the rules on Software risk at Annex VIII MDR section 6.3. This can affect the marketing and sale of the medical device as such. Moreover, the guidance definition of software is very general

[25] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC *OJ L 117, 5.5.2017*, p. 1–175.

[26] Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU *OJ L 117, 5.5.2017, p. 176–332.*

[27] Medical Devices Coordination Group, '2019-11 Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR October 2019 '

and can include also the definition of AI systems. As a consequence, the AI Act provisions could be applicable also alongside the MDR procedures, once into force.

In order to better understand the decisional process because of which a manufacturer can understand whether it has created or not a software as medical device, it is better to look at the decision tree drafted by the MDCG and that is reproduced below.

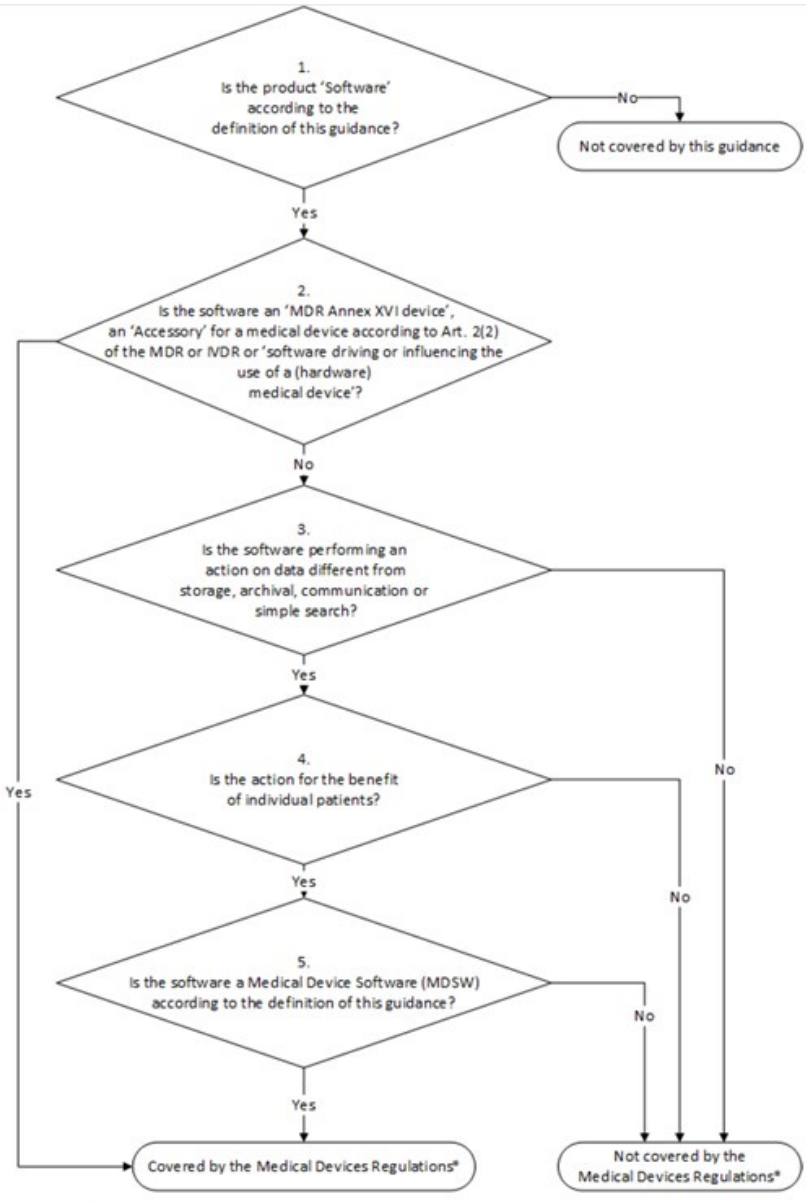

Figure 1. MDCG decision tree to qualify software as a medical device. Originally published in: Medical Devices Coordination Group, '2019-11 Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR October 2019, 9

3.2.2. The Clinical Trials Regulation (CTR)

The CTR long implementation process depended on the development of the Clinical Trial Information System (hereinafter CTIS), a unique EU clinical trials and portal database. The motivation underpinning the update of the previous directive was to create a truly harmonized system to carry out clinical trials around the EU.

The CTR main objective provides more transparency on clinical trials data. All information in the EU database will be publicly accessible in CTIS 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*

To support the transparency requirements of the Regulation, EMA has added 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*[28]"

In the table below, we listed the main compliance activities designed in the CTR.

Pills of CTR
The founding principle is that one must obtain a prior authorization for clinical trials after a scientific and ethical review is carried out from an Ethical Committee at a national level (Article 4 CTR).
In order to obtain this authorisation, the sponsor shall submit an application in the CTIS system and address it to the Member State where the clinical trial is going to take place (Article 5 CTR)
The evaluation of the proposal is divided in two parts. The first one mainly covers (Article 6 CTR): • The anticipated therapeutic and public health benefits of the clinical trial • The risks and the inconveniences for the subjects • Compliance with the requirements concerning the manufacturing and import of investigational medicinal products and auxiliary medicinal products
The second part instead mainly deals with (Article 7 CTR): • the compliance with the requirements for informed consent (chapter V CTR) • the compliance of the arrangements for rewarding or compensating subjects with the requirements set out in Chapter V (CTR)and investigators. • compliance of the arrangements for recruitment of subjects with the requirements set out in Chapter V (CTR) • compliance with Directive 95/46/EC

[28] See more at https://health.ec.europa.eu/medicinal-products/clinical-trials/clinical-trials-regulation-eu-no-5362014_en accessed 03 July 2023

• compliance with Article 49 CTR (Suitability of individuals involved in conducting the clinical trial) • compliance with article 50 CTR (Suitability of clinical trial sites) • compliance with article 76 CTR (Damage compensation) compliance with the applicable rules for the collection, storage and future use of biological samples of the subject

Table 2. An overview of the main provisions of the Clinical Trial Regulation

3.3. Internal Market, Industry, Entrepreneurship and SMEs

Within the framework of the EU Commission action concerning the internal market harmonization, and the relationships between the different kind of economic stakeholders, from big industries to small-medium enterprises (SMEs), it is important that Brief researchers are informed that the Machinery Regulation has been approved and this is going to impact their work. In fact, if one or more of the parts of their devices fall within article 2 MR (such as safety components, included software, chains, webbings and removable mechanical transmission devices) they will need to apply this text.

3.3.1Machinery regulation (MR)

In June 2023, the EU approved a regulation that is an update of the previous machinery directive (MD)[29] because of several reasons. One of the most important ones is the **emergence of AI systems that act as safety components in the interaction with machinery**. This updated document is the machinery regulation (**MR**)[30] and it sets harmonized minimum standards for health and safety requirements but also for the design and construction of complex machines as biorobotic products might be (e.g. co-bots, robotic industrial arms *et cetera*) [31].

Both in the MD and MR (but also the MDR) the manufacturer must comply with a set of requirements if they want to market their product or service in the EU Single Market. The manufacturer's objective is to **obtain the CE marking**, which certifies the conformity of the product or service with the EU standards for health and safety. The change from directive to regulation is relevant because the Member States will need to apply the new text without deciding autonomously how to implement it, as it is a regulation and not a directive anymore. This will lead to a higher level of harmonization across the machinery sector. This will also mean that BRIEF researchers can look at the regulation from now in order to understand how to comply with the new rules, except when the national ministries give further clarifications in more unclear passages of the regulation (see Policy Brief no. 16). Here follows a short preview.

PILLS OF MR
The MR has a **well-defined scope** and it applies to the list of Article 2(1) objects, **software as a safety component included**. The same article provides also a list of excluded objects such as weapons, and aeronautical products. The concept of machinery is an encompassing one and it is generally understood as 'an assembly, fitted with or intended to be fitted with a drive system other

[29] Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery and amending Directive 95/16/EC (recast) *OJ L 157, 9.6.2006, p. 24–86.*
[30] Regulation (EU) 2023/1230 of the European Parliament and of the Council of 14 June 2023 on machinery and repealing Directive 2006/42/EC of the European Parliament and of the Council and Council Directive 73/361/EEC PE/6/2023/REV/1 OJ L 165, 29.6.2023 (hereinafter MR).
[31] Article 1 MR.

than directly applied human or animal effort, consisting of linked parts or components, at least one of which moves, and which are joined together for a specific application' (Article 3(1) and following paragraphs)
All the ***actors*** involved in the machinery or related product's value chain have **duties and obligations.**
The objective is to obtain the **CE marking** through a **third-party conformity check**. Depending on the level of risk of the machinery, the conformity procedure will also vary.
The regulation sets a series of **essential health and safety requirements** that must be respected also not be liable under the **new product liability framework.** It is important because software as a safety component is considered also **for high-risk AI systems by Annex I and Article 6(1) of the AI Act.** This means that the two regulations (MR and AI Act) will need to be respected at the same time in this case, otherwise, there might be liability consequences (see *infra*).

Table 3. Overview of the key provisions of the Machinery Regulation

3.3. The EU Strategy on Artificial Intelligence

The third sectorial legal framework impacting on BRIEF activities is the so-called EU Artificial Intelligence (AI) Package, inspired to achieve excellence and trust, in order to boost research and industrial capacity while ensuring safety and fundamental rights.

3.3.1 The AI Act [32]

Finally approved by the European Parliament in 2024, the AI Act[33] is the world's first binding regulation that sets harmonized rules for the development and use of artificial intelligence (AI). The AI Act intends to ensure the safety of AI systems put into service or commercialized in the EU and uphold European fundamental rights, while boosting innovation in this field, leveraging the many benefits that can be envisioned, such as better healthcare. As part of the European approach to AI, this regulatory framework is accompanied by policies that support research and innovation such as the AI innovation package to support AI startups and SMEs[34] and the dedicated investment in Horizon Europe.[35]

To this end, the AI Act adopts a **risk-based approach** that lays down rules to determine whether an AI system is prohibited, high-risk or not high-risk – and the obligations for developers and deployers, regardless of whether they are based in the EU, that follow such a categorization. An AI system is defined as "[a] *machine-based system designed to operate with* ***varying levels of autonomy*** *and that may* ***exhibit adaptiveness*** *after deployment and that, for*

[32] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0206

[33] REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), https://data.consilium.europa.eu/doc/document/PE-24-2024-INIT/en/pdf

[34] https://digital-strategy.ec.europa.eu/en/news/commission-launches-ai-innovation-package-support-artificial-intelligence-startups-and-smes

[35] https://digital-strategy.ec.europa.eu/en/news/commission-invests-eu112-million-ai-and-quantum-research-and-innovation

explicit or implicit objectives, ***infers, from the input it receives, how to generate outputs*** *such as predictions, content, recommendations, or decisions that can influence physical or virtual environments*" (Article 3 §1).

3.3.1.1. Prohibited AI systems

Prohibited systems (Article 5) bear an unacceptable risk and encompass those that:

1) use **subliminal, manipulative or deceptive techniques** impairing informed decision-making and causing significant harm; this risk is particularly present when brain-machine interfaces are implemented or virtual reality is used since these technologies allow for great control over the stimuli presented to the person (Recital 29).
2) **exploit vulnerabilities** of individuals or groups (i.e., age, disability, socio-economic situation) to distort behaviour and thereby cause harm; for example, children are generally considered more vulnerable than adults and at risk of being more easily affected in digital settings because of their lack of experience and their lower ability to resist influence;[36] data-driven algorithms can target such vulnerability to external undue influences and exacerbate the harmful repercussions that people may experience.
3) resort to **social scoring** that results in detrimental or unfavourable treatment of certain people; social scoring refers to the classification or evaluation of individuals or groups based on data related to their social behaviour in certain contexts or to their personal or personality traits over a period of time; it becomes particularly problematic when it is used to disadvantage people in contexts that are unrelated to those where the data was gathered or to treat people in a disproportionate or unjustified detrimental manner (Recital 31), such as when it is used to restrict the freedom of movement or the access to certain services.
4) perform **risk assessments** based on profiling or personality traits to **predict the likelihood of committing a criminal offence**; such assessments are not based on the actual behaviour of a person, but rather on other traits that are not objective verifiable facts such as the place of residence or the level of debt (Recital 42).
5) compile **facial recognition databases from scraping** activities carried out on the internet or CCTV footage because this practice can violate fundamental rights such as the right to privacy (Recital 43).
6) **recognise emotions** in **educational institutions or the workplace**, for example when emotion-recognition systems are used to determine access to education and career progression; there are general concerns about the reliability of such technologies since they carry the risk of performing inaccurate analyses of facial expressions and providing mistaken conclusions about the inner state of individuals (Recital 44).
7) use **biometric categorisation systems that deduce sensitive attributes** from biometric data, such as the processing of people's face or fingerprints to deduce whether they belong to categories of race, political affiliation, religious or philosophical beliefs, sex life or sexual orientation.

[36] OECD, 'Consumer Vulnerability in the Digital Age' (2023) 355 <https://doi.org/10.1787/4d013cc5-en> accessed 2 May 2024.

8) use **real-time remote biometric classification systems in public spaces for law enforcement** unless the use is strictly necessary under specific conditions (e.g., searching for missing people, preventing terrorist attacks); such systems, such as those that enable facial recognition, may be experienced as surveillance tools and dissuade people from exercising their rights such as the freedom of assembly; the fact that they are used in real-time reduces or annihilates the potential for oversight and correction (Recital 32).

[9] *Key insights on Biometric Systems*
Biometric identification systems can uniquely identify a person through their face, voice, iris, or fingerprints. Biometric systems use as input biometric data, which is considered a special category of personal data under Article 9 of the GDPR, whose processing is prohibited, unless specific conditions apply (e.g., the explicit consent of the data subject). National data protection authorities have already prohibited biometric data processing when they are not used for law enforcement reasons (Recital 39).
The AI Act prohibits the use of biometric systems when they are employed to make deductions, and consequently categorize individuals, on sensitive attributes, such as race, sexual orientation and political affiliation. This prohibition does not apply to biometric datasets that are filtered, labelled or categorized in a lawful manner such as the sorting of images based on eye color.
When **AI systems are used for biometric categorization** that infers sensitive attributes from biometric data, but these cases are not covered by the prohibition, **they are classified as high-risk systems**.
Biometric systems are also growingly used **for the verification of digital identities** to provide users with access to certain services and to strengthen security measures, such as multi-factor authentication. **When used for verification purposes, including authentication, biometric systems are not considered as high-risk.**
Real-time remote biometric classification systems for the identification of people in public spaces for purposes of law enforcement are prohibited (see point 8 above). Such systems are often based on facial recognition, where they seek to match a face captured by a video camera in a public space with those that are present in a database, for example to identify people on a watchlist (large scale face matching), or where they track an individual's movements in a geographical zone (targeted face tracking). It is prohibited to use such systems to identify people in real-time, apart from specific cases with high public interest which outweighs the risk (such as searching for missing people or preventing terrorist attacks, among the others) (Recital 33). In these cases, **the use of real-time remote biometric classification system is authorized only if the relevant law enforcement authority has made a fundamental rights impact assessment and has registered the system in the relevant database** (Recital 34). When the same system is used for **remote identification but not in real-time, the system is classified as high-risk**.

Table 4. In-depth analysis of the classification of biometric systems as prohibited or high-risk AI systems in the AI Act

3.3.1.2. High-risk AI systems

AI systems are categorized as **high-risk** (Article 6) whenever they significantly affect safety or fundamental rights, in particular when:

(a) they are used **as safety components or a product and need a third-party conformity assessment**, thus fall under the EU's product safety legislation (see Annex II), such as toys, aviation, cars, **medical devices** and lifts; or

(b) they are used in the following domains (listed in Annex III):

1) systems for **remote biometric identification**, **biometric categorisation based on the inference of sensitive attributes** and **emotion recognition** (see examples above) that are permitted by the law;
2) management and operation of **critical digital infrastructure**, such as the supply of water, electricity or gas;
3) **education and vocational training** (e.g., admission, learning outcomes evaluation);
4) **employment, worker management and access to self-employment** (e.g., recruitment, termination of contract);
5) access to and enjoyment of **essential private services and essential public services and benefits** (e.g., eligibility for public assistance services, creditworthiness);
6) **law enforcement** (e.g., assessing the likelihood of offence);
7) **migration, asylum and border control** management (e.g., eligibility for asylum);
8) administration of **justice and democratic processes** (e.g., legal interpretation, dispute resolution).

Such systems would not be considered high-risk, when:

a) they perform a narrow procedural task
b) improve the results of a human activity
c) detects decision-making patterns or deviations from prior decision-making patterns but it does not replace or influence the human assessment without proper human review or
d) performs a preparatory task to an assessment relevant for the purpose of the use cases listed in Annex III.

If providers (i.e., developers) believe that their AI systems, even when included in the cases listed in Annex III, don't pose a significant risk of harm to health, safety, and fundamental rights, they must document such an assessment.

Systems that perform **profiling** are always considered high-risk.

3.3.1.3. Obligations for developers of high-risk AI systems

Various obligations are placed on the **providers** of high-risk systems, which refers to those who develop the systems and those who also place it on the market or put it into service under their own name or trademark (Article 3(3)). Developers can be identified as individuals (natural persons) or organizations (legal persons), such as enterprises. Article 9 imposes the creation, implementation, documentation, and maintenance of a **risk management system** that should be continuously and iteratively reviewed and updated, with particular consideration to whether the impacted people are minors or other vulnerable groups.

Such a system should

a) identify and analyse known and reasonably foreseeable risks to health, safety and fundamental rights when used for its intended purpose, as well as establish mitigation measures that should eliminate the risk or, when impossible, address it so that the relevant residual risk is deemed acceptable, plus provide information and training to deployers that are relevant for transparency purposes (Article 13);

b) estimate and evaluate risks that may emerge when the AI system is used for its intended purpose or when misused in foreseeable ways;

c) evaluate other risks that may emerge from post-market monitoring.

To identify appropriate risk management measures, the AI system shall be tested, including in real-world conditions (see below). At date, there exist many risk management methods for AI[37] that take into consideration different factors. We will provide more detailed guidance in the forthcoming best practices for researchers (D7.6 Report on Policy Design and Advice – second iteration).

To this end, providers can make use of the **regulatory sandboxes** that will be established at the national, or even local, level by the competent authorities (Article 57). Regulatory sandboxes are meant to offer a controlled environment that enables the development, training, testing and validation of innovative AI systems for a limited time before they are commercialized or put in use. Regulatory sandboxes enable the limited testing of innovative technologies in a real-world environment under regulatory supervision.[38] Provided that AI providers observe the agreed sandbox plan and the conditions for participation, no administrative fine will be imposed on them for violations of the AI Act and other regulations, if the competent authorities were involved in the supervision of the AI system testing. Since the goal is to **determine whether a certain innovative AI system is legally compliant,** such regulatory sandboxes can foster innovation and competitiveness, accelerate access to the EU market especially for SMEs and start-ups, and improve legal certainty for innovators. Competent authorities achieve this objective also thanks to the drafting of guidelines and sharing of best practices based on the results and lessons learnt from the experiences carried out within the sandboxes. Regulatory sandboxes are also meant to **identify risks upfront and devise mitigations measures**, on which competent authorities will provide guidance and support. Authorities will also produce a final report that can be used by AI providers to demonstrate compliance with the AI Act.

AI providers of systems listed in Annex III (see above) can also test their systems outside of regulatory sandboxes in "**real-world testing**" environments (Article 60) under specific conditions, such as the submission of a plan to the market surveillance authority that needs to authorize the testing; the registration of the testing under a unique identification number; a limited time period (no longer than 6 months); the informed consent of participants; effective oversight; and the possibility of reversing or disregarding the predictions, recommendations and decisions of the AI system.

Both regulatory sandboxes and real-world testing environments constitute relevant novelties for the AI systems developed within BRIEF, since they could offer safe environments where to test the AI systems and reach the market more rapidly, with enhanced legal certainty.

Data governance is another important requirement (Article 10) meant to ensure that the datasets used for training, validation and testing are relevant, representative, and, to the best extent possible, free of errors and complete through the application of measures throughout the whole data life-cycle concerning, among the others, bias detection and prevention. The requirement on data governance also impacts other requirements for high-risk AI systems, such

[37] For a recent overview, see e.g., Xia B and others, 'Towards Concrete and Connected AI Risk Assessment (C2AIRA): A Systematic Mapping Study', *2023 IEEE/ACM 2nd International Conference on AI Engineering – Software Engineering for AI (CAIN)* (2023)

[38] Thomas Buocz, Sebastian Pfotenhauer and Iris Eisenberger, 'Regulatory Sandboxes in the AI Act: Reconciling Innovation and Safety?' (2023) 15 Law, Innovation and Technology 357.

as the one on technical documentation, transparency, human oversight and risk management. We refer the reader to Policy brief no. 14 for more accurate information on data governance.

Providers of high-risk AI systems are also required to provide **technical documentation** to demonstrate compliance (Article 11). The documentation should include (see Annex IV) i) a general description of the system concerning e.g., the version of relevant software or firmware, the hardware and the user-interface provided to the deployers; ii) a detailed description of the system design covering elements such as expected outcomes, system architectures, training datasets, among many others; iii) a detailed description of the monitoring, functioning and control of the AI system, such as its capabilities and limitations in performance and the foreseeable unintended outcomes and sources of risks; a description of iv) the appropriateness of the performance metrics; of the v) risk management system; and of vi) relevant changes made during the lifecycle; vii) a list of the applied harmonised standards; viii) a copy of the EU declaration of conformity and xi) a description of the post-market surveillance system.

In addition, high-risk AI systems should technically allow for **record-keeping** of the systems' activities (Article 12) for traceability and monitoring purposes. Moreover, they are subject to **transparency** obligations so that deployers can interpret a system's output and use it appropriately (Article 13) – see also Policy brief no. 12 on transparency. In particular, information should be disclosed in a concise, complete, correct and clear manner about its functioning, such as i) the purpose, ii) the accuracy, robustness and cybersecurity; iii) circumstances that may lead to risks to the health and safety or fundamental rights; iv) the technical capabilities that are relevant to explain the output; v) when appropriate, its performance regarding specific persons or groups; vi) input data; vii) where applicable, information that can help deployers interpret the output and use it appropriately. In addition, the disclosure should regard human oversight and the computational and hardware resources needed, along other informational items.

The AI Act also establishes **human oversight** requirements (Article 14) to ensure the prevention or minimization of harm through the establishment of commensurate measures that can be developed by both the provider and the deployer. This means that human beings should be able to be meaningfully involved in the development and use of AI systems with the goal of detecting and addressing anomalies, being aware of automation bias, providing a correct interpretation of the system's output and the decision on whether to use it or not, as well as halting the system with a dedicated function when needed.

Furthermore, developers of high-risk AI systems should ensure an appropriate level of **accuracy, robustness, and cybersecurity** through technical and organizational measures (Article 15). Robustness measures minimize harmful or other undesirable behaviour by protecting the resilience of the system to any issue that may arise, such as errors, faults, inconsistencies, unexpected situations (Recital 75). Cybersecurity measures are meant to increase the resilience of the system towards malicious third parties' attempts that intend to alter its use, behaviour, performance or compromise its security properties (Recital 76). They should also put in place a **quality management** system to ensure compliance and document it (Article 17), should keep documentation for a period of 10 years after the system has been placed on the market or put into service (Article 18) and keep the logs of the record-keeping activity for an appropriate period (Article 19). If developers realize that their system is not in conformity, they should withdraw, disable or recall it, and inform distributors as well as other relevant actors. Providers should also cooperate with competent authorities (Article 21) and appoint an authorised representative established in the EU, when they are established in third countries (Article 22).

Targeted guidance for developers of AI systems will be provided in the form of best practices included in the next iteration of D7.6.

3.3.1.4. Obligations for deployers of high-risk AI systems

Deployers of AI systems are identified as those who use an AI system under their authority (Article 3(4)), which may have been developed by someone else or by themselves. In this last case, the same person or organization can play the role either of the **provider** or the **deployer** and be subject to the requirements that apply to both. Deployers are also subject to many obligations that concern the adoption of appropriate **technical and organisational measures to ensure proper use of the system**; the assignment of human oversight to people with the **necessary competence, training and authority** (see also Policy Brief no. 15 on AI literacy); the guarantee that **input data is relevant and representative**; **monitoring use and log keeping**, among the others (Article 26).

Deployers that are public bodies, private entities providing public services (in the areas of education, healthcare, social services, housing, administration of justice), entities performing creditworthiness assessment and risk assessment and pricing for health and life insurances must perform a **Fundamental Rights Impact Assessment** (hereinafter FRIA) for high-risk AI systems (Article 27), which is an evaluation of the risks that the AI system pose to fundamental rights of the individuals or groups of individuals likely to be affected (recital 96). Fundamental rights that may be impacted concern the presumption of innocence and right to an effective remedy and to a fair trial, the right to equality and non-discrimination, the right to freedom of expression and information, the right to privacy and data protection, among the others.[39] The FRIA consists in i) a description of the processes, period and frequency where the AI system will be used; ii) the affected people and the specific risks of harms; iii) a description of the implementation of measures of human oversight and measures against the identified risks. Deployers should then notify the market surveillance authority of the results.

Targeted guidance for deployers of AI systems will be provided in the form of best practices included in the next iteration of D7.6.

3.3.1.5. Requirements for general-purpose AI

General-purpose AI models (GPAI) are defined as an AI model **trained on a large amount of data that displays significant generality to be adapted to a wide range of downstream tasks**. They are also referred to as **foundation models** because they can be used as pre-trained models for more specialised AI systems. For example, large language models may be implemented into the developments of chatbots or automated translation services and can be thus considered as GPAIs.

Provisions in **Article 51 distinguish between general-purpose AI models with system risks and those that do not pose systemic risks**. This difference is based essentially on the model's size determined by its computing power (and the amount of data used for training). More

[39] For a concrete example of FRIA, see e.g., https://aligner-h2020.eu/fundamental-rights-impact-assessment-fria/

specifically, all providers of such GPAIs are subject to the obligation to provide the relevant technical documentation and information for downstream developers (Article 53). However, providers of GPAI whose FLOPs (floating point operations) is greater than 10^25 are considered as posing systemic risks, and thus subject to additional requirements, such as performing model evaluations, report serious accidents, and adopt cybersecurity measures (Article 55).

3.3.1.6. Scientific research

The AI Act strives to foster experimentation, innovation and international competitiveness, while ensuring safety and fundamental rights.[40] This is why, the provisions of the AI Act **do not apply** to AI systems and models that are "specifically developed and put into service for the **sole purpose of scientific research and development**" (Article 2(6)). This means that if AI systems are not developed to be commercialized or used outside of research settings, but are only developed for pure research purposes, the requirements of the AI Act do not apply. However, it is plausible that at least some, if not most, of the AI models developed within BRIEF may be later introduced on the market or used outside of research laboratory settings and therefore will need to comply with the requirements set forth by the AI Act and addressed to providers. Moreover, certain of these AI systems, such as those used as medical devices, are classified as high-risk systems in the AI Act and hence are subject to very stringent requirements, for both developers and deployers.

NB: any activity carried out by spin-offs, start-ups and enterprises, even if performed for research purposes, does not count as "sole purpose of scientific research and development". This means that the AI Act applies!

To comply with many of these requirements, **decisions taken at the development stage should be accurately documented** for later use, for example, to foster transparency and informed use and to enable the fulfillment of documentation requirements, data governance and human oversight of high-risk AI systems, as outlined earlier. This means that there is a long chain of accountability that relates the research activities developed in a laboratory to much later uses. Specific examples of how legal requirements should be already considered within research activities (*compliance by design*) are given in the scenario developed in 6.1. Scenario A) Reuse of health data. Furthermore, it is paramount to not forget that other regulations that are described in this report always apply, even to pure research activities, for instance about the **management of personal and non-personal data**.

Another relevant scenario for researchers concerns the regulatory sandboxes and other conditions of real-world testing described earlier. Most obligations of the AI Act do not apply "*to any research, testing and development activity regarding AI systems or models prior to being placed on the market or put into service*" (Article 2(8)). This does not mean that anything is permissible, since such activities should be nevertheless conducted in compliance with the requirements for sandboxes and real-world testing described above and should be carried out

[40] European Commission. Directorate General for Research and Innovation., *Successful and Timely Uptake of Artificial Intelligence in Science in the EU* (Publications Office 2024) <https://data.europa.eu/doi/10.2777/08845> accessed 18 April 2024

in accordance with the guidelines produced by the competent authority. Further, in real-world testing settings, scientists should be mindful of applicable Italian and European legislations.

Moreover, as we argue below, the **AI ethics framework** applies to any R&D activity. Overall, even when commercialization is not envisaged, scientists are held accountable for the decisions they take at any stage of the research. Thus, it is recommended to follow the ethical guidelines that the European Commission and other authoritative bodies publish, and respect the seven principles for the development of trustworthy AI reported below. Indeed, one of these cornerstones is accountability, accompanied by human agency and oversight, technical robustness and safety, privacy and data governance, transparency, diversity, non-discrimination and fairness, environmental and social well-being. As it can be noted, the requirements introduced by the AI Act build on such principles. More broadly, all researchers need to embed into their conduct the principles of reliability, honesty, respect and accountability of the European Code of Research Integrity. Whenever the AI systems may be foreseeably deployed on people, a good practice of scientific research conduct with human subjects[41] should be based on the following four tenets: i) respect for the autonomy, privacy and dignity; ii) scientific integrity; iii) social responsibility and iv) maximize benefits and minimize harms.

3.3.3 Ethical guidelines for AI development

In addition to the requirements laid down by the AI Act, the framework of reference remains the 2019's Ethics guidelines for trustworthy AI developed by the independent AI High-Level Expert Group appointed by the Commission. The framework is based on seven pillars that ensure that the **AI is trustworthy, human-centric and ethically sound.** The seven principles have also been further declined in the ALTAI checklist (see below) and are recommended by many research funding agencies, such as in the European Commission's guidelines on "Ethics By Design and Ethics of Use Approaches for Artificial Intelligence"[42] addressed at Horizon Europe's applicants and beneficiaries, to which we refer our readers for further information. As mentioned earlier, even though the AI Act excludes pure research activities from its scope, researchers nevertheless have accountability and other ethical duties. In the EU, several instruments have been produced to provide guidance to developers of AI and researchers that develop or somehow make use of AI, such as generative AI.

3.3.3.1. Assessment List for Trustworthy Artificial Intelligence (ALTAI)

The Assessment List for Trustworthy Artificial Intelligence (**ALTAI checklist**) developed in 2020 by the then High-Level Expert Group on Artificial Intelligence is a list that whoever develops new forms of technology (and, in particular, AI-based ones) is supposed to follow in order to check the compliance of their technology with EU values on technology. The checklist is not binding, it is a guideline shaping how a developer shall address the lawfulness, ethics,

[41] John Oates and others, 'BPS Code of Human Research Ethics' (The British Psychological Society 2021) <https://www.bps.org.uk/sites/bps.org.uk/files/Policy%20-%20Files/BPS%20Code%20of%20Human%20Research%20Ethics.pdf>.

[42] European Commission. Directorate General for Research and Innovation., 'Ethics By Design and Ethics of Use Approaches for Artificial Intelligence' (2021) <https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ethics-by-design-and-ethics-of-use-approaches-for-artificial-intelligence_he_en.pdf> accessed 18 April 2024.

and robustness of a given solution. It is divided in 7 chapters and 63 questions to address, aiming to assess different features:

- **Human agency and oversight:** it is important that no AI system is left completely unsupervised.
- **Technical robustness and safety**: it is necessary that the technology is sound also from a cybersecurity point of view.
- **Privacy and data governance**: it is mandatory to respect both data protection and privacy as fundamental rights under the GDPR obligations.
- **Transparency**: it is important to share with other researchers the results and also with the data subjects but there must be a counterbalance whenever relevant intellectual property is involved and data protection.
- **Diversity, non-discrimination and fairness:** it is important that data for algorithms training is selected and processed in a way that the highest variety of information is gathered and processed not to have biased results.
- **Environmental and social well-being**: it is necessary to think about durable and sustainable technology starting from the design of the solution as we are all witnessing a climate emergency.
- **Accountability:** this task is solved not only through the compliance with legal tasks, but also by being able to explain and justify each decision taken on ethical legal implications of the R&D&I.

3.3.3.2. Living guidelines on the responsible use of generative AI in research

In March 2024, the European Commission published guidelines on the **responsible use of generative AI in research addressed to various stakeholders,** within the ERA Forum, including universities, research organisations, funders and publishers: "*Living guidelines on the responsible use of generative AI in research*".[43] They build on the main principles of research integrity and on existing frameworks regarding the use of AI, such as the ALTAI checklist and the European Code of Conduct for Research Integrity.[44]

In particular, the guidelines are promoting a responsible use of generative AI, providing recommendations for organisations and researchers, inspired to the following 4 key principles of EU research conduct:

1) **Reliability**: strongly connected to the quality of research, it concerns the verification and reproduction of AI-generated content, with an eye on potential inequalities and discrimination issues as well as the falsification or manipulation of data; this also means to be aware of the limitations of generative AI, such as the risk of hallucinations, bias and inaccuracies.

[43] European Commission. Directorate General for Research and Innovation., 'Living Guidelines on the Responsible Use of Generative AI in Research' (2024) <https://research-and-innovation.ec.europa.eu/document/2b6cf7e5-36ac-41cb-aab5-0d32050143dc_en> accessed 18 April 2024

[44] ALLEA, *The European Code of Conduct for Research Integrity - Revised Edition 2023* (ALLEA - All European Academies 2023) <https://doi.org/10.26356/ECoC> accessed 18 April 2024

2) **Honesty**: applied to all stages of research, it also means disclosing whether generative IA has been used, for instance in interpreting data analysis, carrying out a literature review, identifying research gaps, formulating research aims, developing hypotheses and drafting articles.
3) **Respect**: towards collaborators, research participants, society and environment at large, responsible use of generative AI should also account for its limitations, its environmental impact and its societal effects concerning fairness, non-discrimination, prevention of harm, privacy, confidentiality and intellectual property rights; for example, researchers do not upload unpublished or confidential work, since it could be used for further training; they do not feed the tool with others' personal data unless they have gathered the consent of those people and unless they have a clear goal for doing so; they also need to be mindful about how and where the tool uses personal data and by whom it is managed.
4) **Accountability:** from the research idea to publication, but also beyond (societal impact), researchers are responsible for any output of the research (see also reliability), which should be sustained by human agency and oversight; this also means that researchers respect applicable laws (e.g., on the protection of personal data and of intellectual property).

3.3.2. The AI Liability Directive proposal[45]

The purpose of the AI liability directive proposal is to improve the functioning of the internal market by laying down **uniform requirements for non-contractual civil liability for damage caused with the involvement of AI systems**. The overall objective of the proposal is to promote the rollout of trustworthy AI, to harvest its full benefits for the internal market by ensuring victims of damage caused by obtain **equivalent protection to victims of damage caused by products** in general. The proposal also aims to **reduce legal uncertainty** for businesses developing or using AI regarding their possible exposure to liability and prevent the emergence of fragmented AI-specific adaptations of national civil liability rules.

The AI Liability Proposal (AILP) revolves around two main articles, Article 3 which sets some rules concerning the **disclosure of evidence procedural rule.** In sum, the claimant can ask the judge to compel the AI provider to show how the AI system works if it is not easily understandable for the claimant. During this procedure IP rights should be safeguarded. If the AI provider refuses to comply with the court order, the judge can presume a causal link between the damage sustained by the claimant and the AI system way of working.

Article 4 instead gives a set of detailed rules on **how the claimant can build their case in order for the judge to presume the presence of a causal link**. The article is divided into two parts: Article 4(1) concerns all the AI systems that are not high risk, for which the claimant needs to prove all of the following conditions: *"*

(a) the claimant has demonstrated or the court has presumed pursuant to Article 3(5), the fault of the defendant, or of a person for whose behaviour the defendant is responsible, consisting in the non-compliance with a duty of care laid down in Union or national law directly intended to protect against the damage that occurred;

[45] Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive), https://commission.europa.eu/system/files/2022-09/1_1_197605_prop_dir_ai_en.pdf

(b) it can be considered reasonably likely, based on the circumstances of the case, that the fault has influenced the output produced by the AI system or the failure of the AI system to produce an output;

(c) the claimant has demonstrated that the output produced by the AI system or the failure of the AI system to produce an output gave rise to the damage."

The second part, Article 4(2) set a series of examples that helped the claimant prove the condition set in Article 4(1)(a) if they managed to demonstrate that the AI provider did not follow the duties of care set in the AI act for high-risk systems.

However, this proposal is quite dependent on the AI Act first official proposal which is different from the latest text approved. That is why it is believed that it will go through extensive modifications in order to add rules concerning the General Purpose AI systems (GPAIs).

Still it is relevant for the BRIEF researchers as they will be more careful to respect the compliance duties of the AI Act as their **non-compliance with these duties can be used to presume the causal link between the damage endured by the claimant and the AI system's way of working and pay compensation.**

3.4. Intellectual Property Rights (IPRs)

The fourth and last pillar of the regulatory framework that concerns BRIEF activities is the set of EU Directives and Regulations aimed at establishing the copyright-, patent-, industrial design-, and trade secrets-related rules at the Union level and harmonising the national IP laws of the EU Member States. In line with the interplay of BRIEF activities with the conventional forms of IPRs, the EU legislation to be analysed herein can be categorised and enlisted as follows:

- **For copyright:** the Software Directive,[46] the Database Directive,[47] the Information Society Directive (InfoSoc Directive),[48] the Copyright in the Digital Single Market Directive (CDSMD),[49] and the Term Directive.[50]
- **For patents:** the Unitary Patent Protection Regulation,[51] Intellectual Property Rights Enforcement Directive (IPRED),[52] the Directive on the Legal Protection of

[46] Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs (Codified version) (Text with EEA relevance), OJ L 111, 05.05.2009, p. 16-22.
[47] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, OJ L 77, 27.03.1996, p. 20-28.
[48] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, OJ L 167, 22.06.2001, p. 10-19.
[49] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (Text with EEA relevance), OJ L 130, 17.05.2019, p. 92-125.
[50] Directive 2006/116/EC of the European Parliament and of the Council of 12 December 2006 on the term of protection of copyright and certain related rights (Codified version), OJ L 372, 27.12.2006, p. 12-18.
[51] Regulation (EU) No 1257/2012 of the European Parliament and of the Council of 17 December 2012 implementing enhanced cooperation in the area of the creation of unitary patent protection, OJ L 361, 31.12.2012.
[52] Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights (Text with EEA relevance), OJ L 157, 30.04.2004, p.45-86.

Biotechnological Inventions,[53] and the Proposed Regulation on Standard Essential Patents.[54]

- **For trade secrets:** the Trade Secrets Directive.[55]
- **For industrial design:** the Design Directive,[56] and the Community Design Regulation.[57]

3.4.1. Copyright

In broad terms, copyright refers to a bundle of economic and moral rights granted to the author or the creator of an original intellectual creation, which is often required to be fixed on a tangible or an intangible medium.[58] Such an intellectual creation could be in literary, scientific and artistic domains. Regardless of the domain, mode or form of expression, the quality or content thereof, an intellectual creation would, in principle, be eligible for copyright protection if it is the outcome of the author's/creator's own intellectual creativity[59].

Copyright subsists in literary works – including software, artistic works, cinematographic works, musical works, architectural works, and original databases. Nevertheless, it is essential to emphasise that copyright protects merely the expression of an idea rather than the idea itself[60].

The economic rights encompassed within copyright consist of the rights to reproduction, communication to the public, making available to the public, and distribution (including lending and rental)[61]. Complementary to these rights of an economic nature are moral rights, which, generally, comprise the rights to claim authorship, and to object to certain modifications and other derogatory actions[62].

In the EU and the Member States, the existence, enjoyment and enforcement of copyright do not require any formalities, such as the registration of the work to a registry held by a public authority. Thus, copyright exists automatically once the original intellectual creation is created.

The author/creator of a work is, in principle, the first copyright owner of the work. Whereas the moral rights comprised in copyright remain with the author/creator, the economic rights thereof can be transferred or licensed to third parties. The transfer of copyright results in the change of

[53] Directive 98/44/EC of the European Parliament and of the Council of 6 July 1998 on the legal protection of biotechnological inventions, OJ L 213, 30.07.1998, p. 13-21.
[54] Proposal for a Regulation of the European Parliament and of the Council on standard essential patents and amending Regulation (EU) 2017/1001 (Text with EEA relevance), 27.04.2023, COM(2023) 232 final.
[55] Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful, use and disclosure (Text with EEA relevance), OJ L 157, 15.06.2016, p. 1-18.
[56] Directive 98/71/EC of the European Parliament and of the Council of 13 October 1998 on the legal protection of designs, OJ L 289, 28.10.1998, p. 28-35.
[57] Council Regulation (EC) No 6/2002 of 12 December 2001 on Community designs, OJ L 3, 05.01.2002, p. 1-24.
[58] WIPO Intellectual Property Handbook, World Intellectual Property Organization, Geneva-Switzerland, 2004.
[59] Ibid. Also see: Directive 96/9/EC, Art. 3(1); Directive 2009/24/EC, Art. 1(3); Directive (EU) 2019/790, Art. 14.
[60] Agreement on the Trade-Related Aspects of Intellectual Property Rights as Amended by the 2005 Protocol Amending the TRIPs Agreement, Art. 9(2). Also see: Directive 2009/24/EC, Art. 1(2).
[61] Berne Convention for the Protection of Literary and Artistic Works, Art. 5.
[62] Ibid, Art. 6bis.

the copyright owner; however, copyright licenses enable certain uses of a copyright-protected work without creating changes in the copyright owner's title.

The use of copyright-protected work, however, is not restricted to the transfer of copyright or the voluntary licensing of copyright by the copyright owner. The EU copyright acquis and the national copyright legislations of the EU Member States consist of several exceptions and limitations (E&Ls) to copyright, which facilitate the use of copyright-protected works in certain special cases (e.g. for research purposes) without the authorization of and, often, remuneration of the copyright owner.[63] Additionally, the EU and national legislative frameworks have other mechanisms to achieve the same result, such as compulsory licenses tailored for certain uses of copyright-protected works. Last but not last, copyright does not confer eternal economic rights to its holder. As a general rule, copyright lasts during the lifetime of the author and at least an additional fifty-year post-mortem.[64] Once this term of protection is over, the work in question falls into the public domain and can be freely used by anyone.

This report concentrates on copyright for two major reasons: First, the R&D&I activities in the biorobotic field, in tandem with the general principles of research, inaugurate with the study of scholarly literature; access to, use and analysis of software; and access to and use of databases – all of which constitute IP that is, in principle, eligible for copyright protection. Furthermore, with the emergence of AI technology and the implementation of generative AI models in the R&D&I activities, copyright becomes more relevant as the datasets used to train AI models are often protected by copyright or sui generis database rights whilst also consisting of copyright-protected content. Second, the scientific results of the BRIEF project as well as of the. researchers and ROs within the Consortium are expected to be incorporated in scholarly publications, edited volumes, or to lead to the production of databases and software – all of which might entitle their authors with copyright over their intellectual creations as such. Therefore, this report centralises the needs and expectations of the BRIEF researchers and ROs, and it elaborates on the legal framework that governs access to and use of software, databases, and literary and artistic works.

3.4.1.1. Software Directive

Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs, or the so-called Software Directive, was adopted on 14 May 1991 in order to ensure the protection of software by copyright in all the EU Member States. The Directive was expected to be transposed to the national laws of the Member States by 1 January 1993.[65] The Directive had retrospective effect, without prejudice to any acts concluded and rights acquired before this date[66].

[63] For the full mapping of the E&Ls to copyright, see: Caterina Sganga, Péter Mezei, Magali Contardi, Pelin Turan, István Harkai, Giorgia Bucaria, and Camilla Signoretta. "D2.3 Copyright Flexibilities: Mapping and Comparative Assessment of EU and National Sources". Zenodo, January 16, 2023. https://doi.org/10.5281/zenodo.7540511.
[64] Berne Convention for the Protection of Literary and Artistic Works, Art. 7.
[65] Directive 91/250/EEC, Art. 10(1).
[66] Ibid, Art. 9(2).

The Software Directive of 1991 was later codified by Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs, which entered into force on 25 May 2009[67].

As revised, the Software Directive applies to computer programs "in any form, including those which are incorporated into hardware"[68] as well as the "preparatory design work leading to the development of a computer program"[69]. In line with the general principles of copyright law, the Software Directive provides legal protection to the expression of a computer program. For the same reason, "the ideas and principles which underlie any element of a program, including those which underlie its interfaces"[70] – hence, the logic, algorithms and programming languages – are neither eligible for nor protected by copyright under the Software Directive[71].

Contouring its scope as such, the Software Directive regulates the authorship of software, including the exercise of rights stemming from authorship in the case of the development of software under an employment contract, the exclusive rights (copyright) of software developers, the exceptions and limitations (E&Ls) to copyright over software, and the special measures of protection envisioned for tackling the infringement of copyright over software. The first two aspects (authorship and the scope of copyright protection) are essential for the software to be developed in the context of BRIEF and R&D&I activities, given that these rules shed light upon the EU standards concerning the rightsholders of copyright-protected software. The E&Ls to copyright are of pivotal importance due to providing researchers with the opportunity to use the software in certain cases without having to seek a license from the copyright owner.

3.4.1.2. Database Directive

Directive 96/9/EC of 11 March 1996 on the legal protection of databases entered into force on 16 April 1996, and the Member States were required to transpose the Directive to their national laws by 1 January 1998.[72]. The Directive was amended by the CDSMD in 2019.

As amended, the Database Directive defines a database as "a collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means"[73]. Broadly articulated as such, this definition encompasses databases available in any form, including online and offline databases[74]. However, computer programs involved in the making or operation of such databases are excluded from the scope of the Database Directive[75].

The Database Directive regulates the legal protection of databases by copyright or by sui generis rights, with respect to their defining characteristics. Databases that are original in their structure

[67] Directive 2009/24/EC, Art. 10(2).
[68] Ibid, Recital 7.
[69] Ibid.
[70] Ibid, Art. 1(2).
[71] Ibid, Recital 10.
[72] Directive 96/9/EC, Art. 16(1).
[73] Ibid, Art. 1(2).
[74] Ibid, Art. 1(1).
[75] Ibid, Art. 1(3).

and arrangement are protected by copyright,[76] whereas databases that required qualitatively or quantitatively substantial investments in the collection, verification and organization of their materials are protected by sui generis rights[77]. Copyright protection entails the bundle of economic and moral rights indicated above; whereas the sui generis protection comprises the rights for extraction and re-utilization, which respectively refer to "the permanent or temporary transfer of all or a substantial part of the contents of a database to another medium by any means or in any form"[78] and "making available to the public all or a substantial part of the contents of a database by the distribution of copies, by renting, by on-line or other forms of transmission"[79]. Copyright protection applies to databases created before 1 January 1998,[80] while the sui generis protection extends to databases completed from 1 January 1983[81].

As emphasized by the Database Directive, the copyright and sui generis protection envisaged for databases do not extend to works and other subject-matter (such as personal and non-personal data, public sector information, open data and the like) contained in the databases.[82] The works and other subject-matter compiled under the copyright-protected or sui generis-protected databases might be subject to disparate and multiple legal regimes (such as GDPR, Open Data Directive as well as copyright, patent, trade secrets, industrial design rights, and legal norms on unfair competition).

The Database Directive, therefore, regulates the database author's and maker's rights, the term of sui generis protection envisioned for databases, and the E&Ls to copyright and sui generis over databases which help lawful users to access to and use copyright-protected and sui generis-protected databases without the authorization and compensation of the rightsholders.

3.4.1.3. Information Society Directive (InfoSoc Directive)

Directive 2001/29/EC of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, or the so-called InfoSoc Directive, is the cornerstone of the EU copyright framework, as it represents the most comprehensive harmonization intervention on EU copyright law. Due to this, the InfoSoc Directive encompasses a wide spectrum of copyright-related matters, including the technological protection measures (TPMs) and digital rights management (DRM) systems, while also containing the largest set of copyright flexibilities introduced in the EU copyright acquis so far. In this regard, the InfoSoc Directive is essential for the BRIEF activities since it is the main - or the prominent - EU instrument that helped the EU and its Member States to adapt their copyright regimes to the particularities of the digital era and the technological advancements. In fact, the mandatory E&L to facilitate temporary reproduction, enshrined in Article 5(1) of the InfoSoc Directive, still constitutes the lynchpin of researchers' and ROs' time- and cost-efficient endeavours to train AI models by using copyright-protected works.

[76] Ibid, Art. 3(1).
[77] Ibid, Art. 7(1).
[78] Ibid, Art. 7(2)(a).
[79] Ibid, Art. 7(2)(b).
[80] Ibid, Art. 14(1).
[81] Ibid, Art. 14(3).
[82] Ibid, Artt. 1(3), 3(2).

The InfoSoc Directive entered into force on 22 June 2001,[83] with a deadline set for 22 December 2002 for the Member States' implementation of the Directive into their national laws.[84] The operational text of the Directive was modified first, in 2017, by the Marrakesh Directive, and then, in 2019, by the CDSMD. As amended, the Directive applies to works and other subject-matter protected by copyright or related rights,[85] yet without prejudice to acts concluded and rights acquired before this date[86].

3.4.1.4. Copyright in the Digital Single Market Directive (CDSMD)

Directive (EU) 2019/790 of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (CDSMD) entered into force on 7 June 2019. The Member States were given time to transpose the Directive into their national laws by 7 June 2021[87]. Despite the significant delays in the process, the transposition of the CDSMD was finalized in 2023.

Comprising the most recent addition to the EU copyright framework, the CDSMD was aimed to improve the functioning of the Single Market by adapting certain key E&Ls to copyright to the particularities of the digital and cross-border environment and to improve the licensing practices to enhance the accessibility of out-of-commerce works across the EU. In this regard, this Directive is crucial for the BRIEF activities due to being the only copyright instrument to introduce mandatory E&Ls to copyright and related rights for TDM.

3.4.1.5. Term Directive

Directive 2006/116/EC of 12 December 2006 on the term of protection of copyright and certain related rights (Term Directive) is also worth noting in the context of the BRIEF activities, given that this Directive is aimed at harmonizing the duration of the legal protection granted upon copyright-protected works as well as the duration of the legal protection provided for other subject-matter (first fixations of films, phonograms, broadcasts, performances) protected by related rights (rights of film producers, phonogram producers, broadcasting organisations, and performers).

The Term Directive is of particular importance for two main reasons. First, it contours the borders of the public domain, which, in its broadest terms, refers to the sum of works and other subject-matter that are not protected by copyright or related rights or materials as such whose copyright protection has lapsed. Therefore, the public domain is a generic term to collectively refer to the materials that can be used, in theory, without authorization and payment of royalties/fees. Second, the Directive crystallizes the rules regarding the duration of the economic and moral rights of the authors and creators of original works. Therefore, this Directive is essential for researchers and research organisations involved in the BRIEF network to contemplate the term of their copyright over their prospective scientific output.

[83] Directive 2001/29/EC, Art. 14(1).
[84] Ibid, Art. 13.
[85] Ibid, Art. 10(1).
[86] Ibid, Art. 10(2).
[87] Directive (EU) 2019/790, Art. 29.

3.4.2. Patent

Patent, also in its broadest terms, is a document issued, upon application, by the competent authority (often an industrial property office) which, on the one hand, consists of the detailed description of an invention and, on the other hand, provides a legal monopoly in favour of the applicant, as the patent owner, to prevent the unauthorized commercial exploitation of the patented invention.[88] The term "invention", in this context, refers to "a solution to a specific problem in the field of technology"[89], which may relate either to a product or a process.

To be eligible for legal protection originating from a patent, an invention shall meet certain criteria. These criteria comprise **(1)** the existence of a patentable subject-matter, **(2)** the industrial applicability of the subject-matter, **(3)** the novelty of the subject-matter, **(4)** the existence of a sufficient inventive step, also known as the "non-obviousness" of the subject-matter, and **(5)** the disclosure of the invention in the patent application.[90]

It shall be noted that, just like copyright and other IPRs, the legal protection entitled by a patent is limited in time in order to balance the private interests of the patent owner with the public interest. The term of legal protection conferred to the patent owner is, often, limited to 20 years. During the term of legal protection, the patent owner has the exclusive right to commercially exploit the invention through the sale, manufacturing, and import of the patented invention or by concluding exclusive or non-exclusive licenses to enable the use of the patented invention by third parties in return of royalties, which are also known as "voluntary licenses".

It shall be noted, however, that the abovementioned exclusive rights of the patent holder are not unlimited or eternal. On the one hand, as opposed to the voluntary licenses granted by the patent owner, the compulsory licenses introduced by the national legislative frameworks would enable the use of the patented invention without the authorization of the patent owner, however, in certain special cases and provided that certain conditions are respected. On the other hand, after the lapse of the term of protection, the patented invention falls into the public domain and thus can be freely used by anyone.

The information provided herein provides merely a snapshot of the patents, whereas the patent-related aspects of the BRIEF activities will be analysed in the next iteration (D7.5) of this deliverable.

3.4.3. Trade secrets

Trade secrets, also known as know-how or undisclosed information, are broadly articulated by the EU legislator as "valuable know-how and business information that is undisclosed and intended to remain confidential"[91]. Therefore, trade secrets differ from the other forms of IPRs due to their holders' interest in preventing them from becoming available to the public, whereas IPRs such as patent and design rights require registration of the invention and the design to

[88] WIPO Intellectual Property Handbook.
[89] Ibid.
[90] WIPO Intellectual Propery Handbook.
[91] Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use or disclosure [2016] OJ L 157/1, Recital 1.

secure a legal monopoly to appropriate them for a limited period of time. In this regard, the legal protection envisaged for trade secrets constitutes an alternative to patent and design rights whilst enabling the appropriation of the results of research and innovation. Due to this, trade secrets are acknowledged by the EU legislator as "the currency of the knowledge economy"[92] given the economic value and the competitive advantage they provide to their holders, especially in innovative industries and fields.

3.4.3.1. Trade Secrets Directive

Directive (EU) 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (Trade Secrets Directive) entered into force on 5 July 2016[93]. The EU Member States were required to transpose it to their national laws by 9 June 2018[94].

The Trade Secrets Directive aimed at eliminating the differences between the national laws of the Member States concerning the definition of "trade secrets" and the other essential terminology such as "unlawful acquisition", "use" and "disclosure" of trade secrets by third parties. Furthermore, it harmonises the scope of legal protection granted to the trade secrets holder, as well as the legal consequences of and remedies for infringement of the rights of the trade secret holder, while also regulating the consequences of reverse engineering of a product to acquire information falling under the trade secret of an enterprise. In this regard, the Directive sets the European standards for the legal framework on trade secrets, hence approximating the laws of the Member States on the matter.

The Trade Secrets Directive is yet another legal instrument that is crucial for BRIEF activities as not only business enterprises but also ROs, including the ones without any commercial interest, invest in "acquiring, developing and applying know-how and information" that would provide competitive and innovation-based advantage to the holders of such knowledge. Therefore, not only the ways in which to access and use third-party trade secrets in the context of R&D&I endeavours but also the optimal ways to keep confidential the know-how to be developed by the BRIEF researchers and ROs are of pivotal importance to the BRIEF project.

3.4.4. Industrial design

Industrial design is yet another conventional form of IPR which protects the ornamental and non-functional features of an article or product.[95] In other words, it is not the article or the product, but the design embodied in such article or product that is protected by industrial design rights.[96] The design that is subject to the industrial design rights may be two-dimensional as well as three-dimensional, including those generated with the aid of 3D-printing technology. Nevertheless, not every design is eligible for legal protection. In principle, "designs dictated essentially by technical or functional considerations"[97] are carved out of the scope of legal

[92] Ibid.
[93] Directive (EU) 2016/943, Art. 20.
[94] Ibid, Art. 19(1).
[95] WIPO Intellectual Property Handbook.
[96] Ibid.
[97] Agreement on the Trade-Related Aspects of Intellectual Property Rights, Art. 25(1).

protection envisaged for industrial designs. Additionally, designs that do not meet the novelty threshold set by the applicable law would also not be entitled to legal protection.[98]

In the EU, the acquisition of design rights, in principle, requires the registration of the design to the competent intellectual/industrial property office of the State in which legal protection is sought. However, the Community Design Regulation also acknowledges legal protection, with a more restricted term of protection, to unregistered designs. Indeed, the Union's IP framework envisions a five-year legal protection, renewable up to 25 years,[99] for registered designs and three-year protection unregistered ones.[100]

During the term of legal protection, the rightsholder holds the exclusive right to use and prevent third parties from using the design in question.[101] Whereas the design rightsholder will be the only one to use, also to commercially exploit, the design through the sale, import, or export of products bearing the design or by licensing or transferring the design rights, with the lapse of the term of legal protection the design will become part of the public domain to be freely used by anyone.

3.4.4.1. Design Directive

Directive 98/71/EC on the legal protection of designs (Design Directive) is one of the two EU legislations that set the legal framework for industrial designs at the Union level. Entered into force on 17 November 1998[102] and had to be implemented in the national laws of the Member States by 28 October 2001,[103] the Design Directive harmonises the design protection legislation of the Member States by setting the Union standards. To do so, it provides a unitary definition for the term "industrial design", clarifies the legal consequences of the registration of industrial designs, approximates the eligibility criteria to grant legal protection to industrial designs and sets the scope and term of such legal protection as well as the limitations to the exclusive rights of the industrial design holder to enable the use of registered designs in certain special cases.

In this respect, the Design Directive constitutes one of the building blocks of the IP framework that informs and governs the R&D&I activities of the BRIEF network as it would apply to the products to be developed through the R&D&I activities in the BRIEF context as well as the products protected by third-party design rights in order to develop such. Hence, the Design Directive is key to comprehending the prospective rights of the BRIEF consortium and how to acquire such rights, as well as the ways in which the BRIEF researchers and ROs can use the legally protected state-of-the-art products for research purposes.

3.4.4.2. Community Design Regulation

[98] Ibid, Art. 25(1); Directive 98/71/EC, Art. 4.
[99] Council Regulation (EC) No 6/2002, Art. 12.
[100] Ibid, Art. 11.
[101] Agreement on the Trade-Related Aspects of Intellectual Property Rights, Art. 26(1).
[102] Directive 98/71/EC, Art. 20.
[103] Ibid, Art. 19.

Last but not least, Council Regulation (EC) No 6/2002 on Community designs (Community Design Regulation), which entered into force on 6 March 2002,[104] shall be briefly mentioned herein for it sets the rules concerning the registration of an industrial design to the European Union Intellectual Property Office (EUIPO) (previously known as the Office for Harmonization in the Internal Market (OHIM)) in order to secure legal protection within the borders of the EU. The Regulation tackles the procedural aspects of the legal framework revolving around industrial designs as it regulates the steps to register a design to the EUIPO and the legal consequences of the acceptance or rejection of such an application. Additionally, it sets the Union rules on the legal protection provided to unregistered industrial designs.

In this regard, the Regulation, mainly, provides the procedural details for EU-wide legal protection which co-exists with the national legal protection that stems from the registration of the design to a national intellectual/industrial property office. Whereas the legal protection envisioned in the latter case remains within the borders of the State in which the design is registered, registration of the design to the EUIPO secures the protection and enforcement of the rights of the industrial design holder across the EU.

Thus, the practical importance of the Regulation stems from the fact that it provides EU-wide legal protection, aside the national legal protection, resulting in the same set of legal rights and responsibilities across the EU, by submitting a single application to the EUIPO. Whereas the details of this Regulation will not be further explored in this report, it is worth highlighting the Community Design Regulation as it offers a cost- and time-efficient way to secure legal protection for industrial designs across the EU.

4. CROSS-FIELD ANALYSIS

In the previous section, the main goals of the legislative initiatives impacting on the EU Data Strategy, Public Health, AI, and IPRs are shortly described in order to define a redline across the different sectors in order to justify the selection provided in our analysis.

In this section, we illustrate the results of the first step of the cross-field analysis aiming to extract for each legislative initiative the main features and the ethical-legal principles that are relevant in the R&D&I sectors, especially for data-driven research infrastructures based on robotics applications, like BRIEF RI is.

EU/national legal framework	*Main principles applicable to BRIEF RI*
GDPR *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on*	The GDPR is important as it sets for the first time some guiding principles in respecting the data protection and privacy fundamental rights such as: • Accountability; • Lawfulness; • Fairness; • Transparency; • Data minimisation; • Accuracy; • Storage limitation;

[104] Council Regulation (EC) No 6/2002, Art. 111(1).

the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) *OJ L 119, 4.5.2016*	• Integrity and confidentiality • Privacy-by-design and by-default
Italian Code of Privacy D. lgs 193/2003 updated with D.lgs. 101/2018, as amended by L.D. 37/2024 Italian Data Protection Authority provisions implementing and /or clarifying some aspects of the GDPR	Italian Code of Privacy: at articles 100, 110 and 110*bis* the Italian Privacy Code sets the main rules to process personal data for the medical biomedical and epidemiological research and further data-sharing for these activities. Article 100 states that public entities such as universities can communicate and share data concerning studies and research activities even to private parties and through electronic means. As far as Articles 110 and 110*bis*, they respectively concern the medical, biomedical and epidemiologic research and the reuse of data for scientific research or for statistical purposes. In the first case, the data processing can be carried out when the conditions of Article 9 (2)j of the GDPR apply (which means that it needs to be carried out for reasons of public interest) and a DPIA has been carried out. Moreover, consent is not required when it implies a disproportionate effort or risks to make the whole research be unsuccessful: in this case the data controller shall submit the research project to the competent ethics committee for approval. Finally, the Data Protection Authority will indicate deontological guarantees to respect according to article 106, paragraph 2, letter d of this code. By decision n. 298 issued on 9.5.2024, the Italian Data Protection Authority adopted new safeguards under Article 110 of the Italian Code of Privacy, pending the implementation of new ethics rules according to Articles 2-*quarter* and 106 of the Italian Code of Privacy. Pursuant to the new safeguards, data controllers shall: a. Obtain positive opinion from the competent ethical committee. b. Motivate and document the presence of ethical or organisational reasons (explained hereafter) according to which 1) data subjects are not contactable anymore; 2) trying to obtain data subjects' consent would lead to a disproportionate effort (in this case data controllers shall document the reasonable efforts made); 3) trying to obtain data subjects' would entail a significant prejudice for the objectives of the research. c. If these conditions are met, data controllers shall conduct a data protection impact assessment according to Article 35 GDPR. Ethical reasons that make it impossible to obtain data subjects' consent occur when the needed information would inform data subjects about research that may cause material or psychological damages to them.

	Organisational reasons occur when the impossibility of processing data related to non-contactable data subjects would lead to significant problems for the quality of the research. In order to ascertain a quality diminution deriving from the impossibility of processing some data, data controllers shall take into account the inclusion criteria of the research, the recruitment procedures, the statistical numerosity of the sample, and the time passed from the moment since personal data were obtained. Article 110*bis* of the Italian Privacy Code, instead, states that the national Data Protection Authorities can authorise the reuse for scientific or statistical research when: I) it is not possible to inform the data subject. The Italian Data Protection Authority requires the research institutions to try to reach the patients at least three times[101] or II) the delay risks to bring prejudice to the outcome of the research. It adopts its decision within 45 days. The further treatment of personal data by third parties can be authorised by the national authority through general provisions. Data protection authority provision on 5.6.2019 concerns specific categories of data. In particular, one of the joint documents concerning data processing is about data that are used scientific research (Aut gen. 9/2016) [105]. In this document it is explained that what could already be deduced from the Articles 5 and 89 of the GDPR: it allows derogations for scientific research especially to collect the data subjects' consent for the processing of their health data whenever there are: 1) ethical reasons concerning the data subjects' ignorance about their health condition 2) organization insurmountable problems which could affect the final results (for instance they are either dead or not reachable) 3) serious health concerns (and in that case the research should have a specific result the objective to make the data subjects' health better). In any case, the data controller is always bound to put in place the technical and organizational measures apt to safeguard the data subjects' right to data protection according to the principle of minimization. *Deontological rules on processing for scientific research*[106] There is a specific part, added to the main document, which specifies the deontological rules to follow when processing personal data for scientific medical, biomedical and epidemiologic research. One of the most important ones is to state that this is done in compliance with Helsinki Convention and that the data subject must express their intention to be informed about possible health-related issues that they might not have been aware about. Moreover, it is then made it explicit that the universities and research institutes carrying out medical research must ensure the respect of these deontological rules.

[105] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9124510 accessed 03 July 2023.
[106] https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9069637 accessed 03 July 2023.

	Rules on the use of consent to re-use data concerning health Opinion of 30 June 2022, n. 9791886[107] The Italian DPA explained that for medical research it is possible to use consent to process data. However, the initial consent clause must not be ultra-general, but it is required that consent must be obtained and must be specific for each kind of processing that will be carried out starting from the health data that the patient had provided the controller originally.
Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (Text with EEA relevance) PE/85/2021/REV/1 OJ L 152, 3.6.2022, p. 1–44 (DGA)	The DGA aims to effectively create a data governance system among public institutions, companies and business stakeholders and citizens, promoting mechanisms of data sharing and reuse, including the "data altruism". In particular, it sets: • conditions for re-use of certain categories of data held by public sector bodies • a notification and supervisory framework for the provision of data intermediation services • a framework for voluntary registration of entities which collect, and process data made available for altruistic purposes; and • a framework for the establishment of a European Data Innovation Board
Clinical Trials regulation (and its implementation in Italy): Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC Text with EEA relevance OJ L 158, 27.5.2014 (CTR)	The CTR harmonises and digitalises procedures for clinical trials, stating in particular that: • Each clinical trial must be subjected to both a scientific and ethical review • The ethical review shall be performed by an ethics committee in accordance with the law of the Member State concerned. The review by the ethics committee may encompass aspects addressed in Part I of the assessment report for the authorisation of a clinical trial as referred to in Article 6 and in Part II of that assessment report as referred to in Article 7 as appropriate for each Member State concerned. • The procedure will be unified through a common EU portal where all the documents must be submitted (CTIS) and the authorisation procedure is led by one MS and there will also be a common data base
National implementation of Clinical Trials Regulation into the Italian discipline: 26, 27, 30 January 2023 decrees	The Italian framework concerning the re-organisation of the clinical trials revolves around the re-organization and rationalization of the discipline of the Ethical Committees. Here follows a synthesis of the main points of the three decrees. **Decree Jan 26, 2023**: selection of the Ethical Committees per region (40); **Decree Jan 27, 2023**: field of application (substantial amendments of clinical trials proposals) and postponement of the application of the CTR until 31 January 2025. However, one can already start using the new EU portal, Clinical Trial Information System (CTIS); presentation of Clinical Trials (CT) proposal; Evaluation of proposals into 2 parts. The first part concerns (see Article 6 CTR).

[107] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9791886 accessed 03 July 2023.

	• the nature of the CT (e.g. low-intervention clinical trial); • the therapeutic and public health benefits of the proposed CT; • the risks for the subject; • the compliance with marketing and labelling requirements and • the adequateness of the presented material The second part instead concerns (Article 7 CTR): • the compliance with the requirements for informed consent (chapter V CTR) • the compliance of the arrangements for rewarding or compensating subjects with the requirements set out in Chapter V (CTR)and investigators. • compliance of the arrangements for recruitment of subjects with the requirements set out in Chapter V (CTR) • compliance with Directive 95/46/EC; • compliance with Article 49 CTR (Suitability of individuals involved in conducting the clinical trial) • compliance with article 50 CTR (Suitability of clinical trial sites) • compliance with article 76 CTR (Damage compensation) • compliance with the applicable rules for the collection, storage and future use of biological samples of the subject. **Decree Jan 30, 2023**: definition of the Local Ethical Committees (Comitati Etici Territoriali) and National Ethical Committees (Comitati Etici Nazionali); respective subject and territorial competences; composition criteria; independence of the members requirement; methods of financing (national system of fees).
Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (Text with EEA relevance) OJ L 117, 5.5.2017, Medical Devices Regulation (MDR)	MDR sets all the compliance duties a manufacturer must follow to commercialise medical devices in the single EU market. In particular, it is useful to highlight as follows. • According to the MDR, software can also be considered as a medical device under certain circumstances; • A series of certification procedures that vary according to the level of risk of the device; • Its deadline for national implementation is 26 May 2024 therefore it is extremely important that medical devices producers comply with these rules.
Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the	It develops a market surveillance system, including conformity obligations as follows. • Creation of conformity assessment bodies • Creation of market surveillance system • Each MS will appoint an accreditation body • Set-up of a community market surveillance framework • Set-up of a Community Rapid Information System

marketing of products and repealing Regulation (EEC) No 339/93 (Text with EEA relevance) OJ L 218, 13.8.2008, p. 30–47 (CE Marking Regulation)	
National Implementation of the MDR D.lgs 137/2022 and decrees 12 April 2023. GU 13 June 2023 n.136 Concerning respectively: A) Administrative procedures of national relevance for the submission of communications relating to clinical investigations for devices bearing the CE marking used in the context of their intended use referred to in Article 16(3) of Decree No 137 of 2022. B) Administrative procedures of national relevance for the submission of the application for clinical investigation for medical devices not bearing the CE marking referred to in Article 16, paragraph 2 of Legislative Decree No. 137 of 2022. (G.U. General Series, no. 136 of 13/06/2023)	A) CE marking: it concerns: • official communication for products bearing the CE marking until the EUDAMED database is fully operational (communications are officially addressed at the Italian Health Ministry). • The documentation sent must be compliant with the MDR requirements. • The official communication to the Health Ministry must happen after an Ethical Committee approval (local, CET, or national CEN) • Communication of the trials beginning within 30 days to the competent authority B) no CE marking: it concerns: • official communication for products not bearing the CE marking until the EUDAMED database is fully operational (communications are officially addressed at the Italian Health Ministry) • legal entities/subjects habilitated to officially communicate information to the Italian Health Ministry is the sponsor • official communication for products bearing the CE marking until the EUDAMED database is fully operational (communications are officially addressed at the Italian Health Ministry) • The request for the start of clinical trials are done after having acquired a favourable opinion of an Ethical Committee (local, CET, or national CEN) • The sponsor communicates the beginning of the trial promptly to the competent authority.
AI Act Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (**Artificial Intelligence Act**)	The AI Act is the world's first binding law on artificial intelligence that establishes the European framework for the development and deployment of artificial intelligence systems whenever they are put into service or commercialized within the European Union. It is a complex piece of legislation that includes provisions on: • AI systems definition as software (primarily); • Risk classification of AI systems, encompassing prohibited, high-risk and low-risk AI systems; • Prohibited systems such as systems that use manipulative, deceptive and subliminal techniques, that exploit vulnerabilities, that implement emotion recognition and biometric categorization, social scoring and predictive policing; • General-purpose AI systems have general transparency obligations, combined with additional requirements e.g., on risk assessment and mitigation whenever they pose systemic risks;

	• Compliance requirements for high-risk AI systems such as risk assessment, transparency, accuracy, data governance, human oversight • Derogations for scientific research.
Data Act (rules on access and re-use of personal and non-personal data from IoT, 2023/2854), DA	The Data Acy is the most general (horizontal in EU parlance) regulation on connected products and related services. It has several thematic blocks of rules concerning: • data access contractual and business relationships involving a user, a data holder and (optionally) also a data recipient; • the obligations for data-holders to make data available + dispute settlement provisions; • the unfair contractual terms related to data access and uses between enterprises (if a clause is unfair according to Article 13 DA then it is null and void); • making data available to public sector bodies and union institutions, agencies or bodies based on exceptional need (e.g. pandemic); • switching between data processing services; • the safeguards for non- personal data in international context; • interoperability rules. In theory it will be applicable for all IoT object (see the definition of product in the DA) also for e-health purposes.
Regulation (EU) 2023/1230 of the European Parliament and of the Council of 14 June 2023 on machinery and repealing Directive 2006/42/EC of the European Parliament and of the Council and Council Directive 73/361/EEC PE/6/2023/REV/1 OJ L 165, 29.6.2023 (hereinafter MR).	The MR is important for the BRIEF project because • It can apply to parts of the devices built if they fall in its field of application (such as motor transmission parts or security software) • It creates a set of rules and procedures to follow based on a risk-assessment rationale in order to obtain the CE marking • It is important as it sets in its Annex II essential health and safety requirements which, if not respective, might trigger a product liability claim • The fact that it also applies to security software makes it possible that, as far as software is concerned, the AI Act regime for high-risk AI system will need to be applied at the same time with the MR requirements
Regulation (EU) 2024/903 of the European Parliament and of the Council of 13 March 2024 laying down measures for a high level of public sector interoperability across the Union (Interoperable Europe Act) PE/73/2023/REV/1 OJ L, 2024/903, 22.3.2024	Particularly noticeable are: • The obligation for the public infrastructure to have an interoperability assessment • The obligation for a Union or public sector body to share its own interoperability measures so that other Union or national public sector bodies can re-use them • The Commission's obligation to share its interoperable Europe solutions on a dedicated portal

Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs (Codified version) (Text with EEA relevance), OJ L 111, 05.05.2009, p. 16-22.	The Software Directive, whilst harmonising the EU Member States' national copyright laws, clarifies the scope of copyright protection for software, the authorship of software, the exclusive rights conferred to the copyright owner of the software, the E&Ls introduced to the exclusive rights of the copyright owner of the software, and the special measures of protection envisioned for the software. Within this framework, it is worth highlighting the following selected element of the Software Directive: • Any computer program comprising its author's intellectual creation is considered an original literary work and entitled to copyright protection. The copyright protection envisioned for software extends to the "preparatory design material" thereof. • Copyright protects merely the expression of a computer program, whereas the ideas and principles underlying its elements and interfaces are not copyright-protected. • The author, hence the first copyright owner, of a software can be either an individual or a group of natural persons or a legal entity. • If the software is created in the context of an employment relationship or by following the instructions of the employer, then the economic rights over software belong, in principle, to the employer. However, the employer and employee can agree otherwise via the employment contract or any other contract. • According to **Article 4** of the Directive, the exclusive rights of the rightsholder of software are as follows: o the permanent or temporary reproduction of a computer program by any means and in any form, in part or in whole; in so far as loading, displaying, running, transmission or storage of the computer program necessitate such reproduction, such acts shall be subject to authorisation by the rightsholder; o the translation, adaptation, arrangement and any other alteration of a computer program and the reproduction of the results thereof, o distribution to the public, including the rental, of the original computer program or of copies thereof. • **Articles 5 and 6** of the Directive provide **the lawful acquirer of software** to perform certain acts that fall under the exclusive rights of the rightsholder, without necessarily seeking the authorization of the rightsholder, for certain specified purposes. These E&Ls to the copyright are as follows: o (1) The permanent or temporary reproduction of a computer program by any means and in any form, in part or in whole; in so far as loading, displaying, running, transmission or storage of the computer program necessitate such reproduction, such acts shall be subject to authorisation by the rightholder; (2) the translation, adaptation, arrangement and any

	other alteration of a computer program and the reproduction of the results thereof, without prejudice to the rights of the person who alters the program. These acts can be performed if the rightsholder of the software has not prohibit such uses by any contractual terms, and only if these acts are necessary for the intended use of the software. o To make a back-up copy of the software. o To observe, study or test the functioning of the program in order to determine the ideas and principles which underlie any element of the program. However, these acts shall be performed with respect to the acts of loading, displaying, running, transmitting or storing the program – as long as the lawful acquirer is entitled to do so. o To reproduce the code and to translate the form of the code of the software (decompilation) in order to obtain the information necessary to achieve the interoperability of software with others only if such information has not previously been readily available and the acts necessary to achieve interoperability are confined to the relevant parts of the original software. The information obtained to achieve interoperability shall not be used for the goals other than maintaining interoperability, or given to others, or used for the development, production or marketing of a software that is substantially similar to the original one.
Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, OJ L 77, 27.03.1996, p. 20-28.	The Database Directive was essential to harmonise the discrepancies in the national copyright laws of the Member States, especially with regard to the (originality) criteria required to grant legal protection to databases and the scope of the rights conferred upon the database authors/makers. Therefore, the Database Directive, by reconciling the various levels of originality sought by different Member States, introduces legal protection to the distinct characteristics of databases: copyright protection for databases which "by reason of the selection or arrangement of their contents, constitute the author's own intellectual creation" (Article 3(1)), and legal protection by sui generis rights to databases "which shows that there has been qualitatively and/or quantitatively a substantial investment in either the obtaining, verification or presentation of the contents" (Article 7(1)). In so doing, the Database Directive sets the Union standards on the authorship of databases, the exclusive rights over databases and the E&Ls to such rights, as well as the term of protection for the sui generis rights. The following can be presented as the highlights of the Database Directive, which are also of crucial importance for the BRIEF activities: • The author of a database can be a natural person or a group of natural persons. In the latter case, the exclusive rights

	deriving from database authorship shall be jointly exercised by the members of the group. • In the Member States whose legislative framework permits, a legal entity may, as well, be designated as the author hence the rightsholder of the database • According to **Article 5** of the Database Directive, the author of a copyright-protected database would have the following exclusive rights: o temporary or permanent reproduction by any means and in any form, in whole or in part; o translation, adaptation, arrangement and any other alteration; and the reproduction, distribution, communication to the public, display or performance to the public of the results of the aforementioned acts; o distribution to the public of the database or of copies thereof, o any communication, display or performance to the public. • **Article 6(1)** of the Directive introduces a mandatory exception or limitation (E/L) to the copyright of the database author in favour of **lawful users** of a database or of a copy thereof. This provision allows the performance of any of the acts covered by the above-mentioned exclusive rights of the database author, without seeking authorization, however only for the purposes of access to and normal use of the contents of the database. When the lawful user is authorized to use only part of the database, the provision applies only to that part. • Additionally, **Article 6(2)(b)** of the Directive introduces another E/L to copyright, specifically, for research purposes. Indeed, this provision holds that the Member States can adopt laws to permit "the use of databases for the sole purpose of illustration for teaching or scientific research, as long as the source is indicated and to the extent justified by the non-commercial purpose to be achieved". • As to the scope of sui generis rights, **Article 7** of the Directive refers to two rights: extraction, which refers to "the permanent or temporary transfer of all or a substantial part of the contents of a database to another medium by any means or in any form", and re-utilisation which stands for "any form of making available to the public all or a substantial part of the contents of a database by the distribution of copies, by renting, by on-line or other forms of transmission". • **Article 8** of the Directive provides an E/L to sui generis rights in favor of the lawful user of such a database. It permits the lawful user of the database to extract and/or re-utilize insubstantial parts of its contents, evaluated

	qualitatively and/or quantitatively, for any purposes. Where the lawful user is authorized to extract and/or re-utilize only part of the database, these actions can be performed only to that part. • Additionally, **Article 9(b)** of the Directive introduces an optional E/L to sui generis rights. It allows the lawful user to extract a substantial part of the contents of a database, without the authorization of the database maker, for the purposes of illustration for teaching or scientific research. However, such practices shall be accompanied by the indication of the sources of the database, and they shall be performed for non-commercial purposes. • It shall be underlined that the copyright or sui generis protection envisioned for the databases does not extend to the contents of the database. Indeed, the contents of the database might be subject to different sets of norms, including but not limited to IPRs and data protection. • The term of legal protection for copyright-protected databases is subject to the general rules encompassed within the Term Directive, whereas the legal protection for sui generis is regulated in detail in **Article 10** of the Database Directive. Setting the main rule, **Article 10(1)** of the Directive grants 15 years of legal protection to such databases. This term shall be calculated from the 1st of January of the year that follows the date of the completion of the making of the database. • **Article 10(3)** of the Directive includes a provision that can be an incentive for database makers, given that it acknowledges that any substantial change executed on the contents of the database might lead to a new database eligible for sui generis protection if such alteration is considered to be a substantial new investment.
Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, OJ L 167, 22.06.2001, p. 10-19.	The InfoSoc Directive is one of the building blocks of the EU copyright legislation due to constituting the EU's first comprehensive attempt to harmonize the key economic rights of copyright holders whilst introducing a set of mandatory and optional E&Ls to these exclusive rights. In this context, **Article 5(1)** of the InfoSoc Directive, which comprises the only mandatory E/L to copyright within the Directive, is of significant importance to research activities that involve AI technologies as this provision is deemed to facilitate training AI models with copyright-protected works and other legally protected subject-matter without any infringement and without having to seek authorization from the rightsholders. • Indeed, Article 5(1) of the Directive obliges the Member States to adopt an E/L which would restrict the exclusive

	right to reproduction of authors, performers, phonogram producers, film producers, and broadcasting organisations. • The provision permits temporary acts of reproduction, which are transient or incidental, and which are an integral and essential part of a technological process, for the sole purpose of enabling transmission in a network between third parties by an intermediary or for the lawful use of a work or other-subject matter. • The temporary reproduction of a work, fixation of a performance, phonogram, cinematographic work, or the fixation of a broadcast can be made by any means and in any form, in whole or in part, and it shall not have any independent economic significance. Additionally, the InfoSoc Directive introduces Union standards to prevent the harmful effects of technology on copyright and related rights, by taking into account the ways in which technology has eased the infringement of copyright and complicated the enforcement of such. Thus, it allocates **Article 6** to the so-called technological protection measures (TPMs), which is articulated as "any technology, device or component that, in the normal course of its operation, is designed to prevent or restrict acts, in respect of works or other subject-matter, which are not authorised by the rightholder of any copyright or any right related to copyright as provided for by law or the sui generis right provided for in [the Database Directive]" (Article 6(3)). Thus, while promoting the adoption of measures by the Member States to prevent the circumvention of TPMs, **Article 6(4)** of the Directive also requires the adoption of measures to enable the enjoyment of the E&Ls to copyright and related rights in order to secure the use of such content despite the TPMs. Also in this context, the InfoSoc Directive dedicates **Article 7** to tackle the digital rights management (DRM) system. For the purposes of the Directive, rights-management information refers to "any information provided by rightsholder which identifies the work or other subject-matter (...), the author or any other rightsholder, or information about the terms and conditions of use of the work or other subject-matter, and any numbers or codes that represent such information" (Article 7(2)). Considering the facilitation of the removal or circumvention of DRM measures vis-a-vis the technological advancements, the Directive requires the EU Member States to adopt measures to prevent such actions as well as the distribution, importation, broadcasting, communication or making available to the public of content whose DRM information has been removed or altered.

Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (Text with EEA relevance), OJ L 130, 17.05.2019, p. 92-125.	Constituting the most recent legislative attempt of the EU legislature to adapt the EU copyright framework to the necessities of the digital era, the CDSMD provides key provisions for research activities, including the E/L it introduced for text and data mining (TDM) purposes. The E&Ls to enable TDM, which are introduced to the EU copyright law by the CDSMD, contours the ways in which the data analytics tools can be used over legally protected works and other subject-matter without leading to infringement of IPRs. For the purposes of the CDSMD, TDM is defined as "any automated analytical technique aimed at analysing text and data in digital form to generate information including but not limited to patterns, trends, and correlations." The CDSMD contains two legal provisions addressed to this purpose: Articles 3 and 4. The focus of this report will be on Article 3 of the CDSMD as it introduces an E&L, specifically, for the purposes of scientific research, without necessarily elaborating on what "scientific research" refers to. However, Recital 12 CDSMD leaves no doubt that the scientific research herein encompasses both natural sciences and human sciences. Accordingly, this provision is addressed not only to ROs but also to cultural heritage institutions (CHIs). Article 3 CDSMD limits the exclusive rights of the author of a copyright-protected database, the sui generis right of the database maker, the right of reproduction under the InfoSoc Directive, and the exclusive rights of press publishers against reproductions and extractions made by ROs and CHIs. These beneficiaries are permitted to reproduce and extract works or other subject-matter to which they have lawful access in order to undertake TDM for scientific research. In light of Recital 14 of the CDSMD, the notion of "lawful access" within this provision shall be understood as having obtained access to content through open-access policies, contractual agreements including subscriptions, and other "lawful means", including the access to "content that is freely available online". Aside from using the works and other subject-matter for TDM purposes as such, beneficiaries are allowed to store copies of the reproductions or extractions of works made in the TDM process in so far as their storage is subject to an appropriate level of security. The Directive does not impose any temporal restrictions on the act of storage. The only requirement is that the retention of the mined results is justified by scientific research purposes, including verifying research results. Recital 15 of the CDSMD further stipulates that the copies may also be retained for scientific research applications beyond TDM, such as scientific peer-review and joint research, if such acts are covered by the E&L provided in Article 5(3)(a) of the InfoSoc Directive, again with no temporal limitation.

	The Directive envisions the possibility for rightsholders to take some measures to guarantee the security and integrity of networks and databases where their works and other subject-matter are hosted. As clarified by Recital 16 of the CDSMD, these measures should be adopted considering the potentially high number of access requests to and downloads of works and other subject-matter. Such measures may encompass, for instance, tools to ensure that only authorized beneficiaries with legal access can access their data, including IP address validation or user authentication. However, these measures must be strictly limited to achieving their intended objective. To this end, the Directive calls the Member States to facilitate the development of best practices mutually agreed upon by rightsholders and beneficiaries of the exception. As a last remark to Article 3 of the CDSMD, it shall be emphasized that Article 7(1) of the CDSMD prevents this exception from being overridable by contractual arrangements. The TDM exception envisioned in Article 3 CDSMD has been implemented in **Article 70-ter l.aut,** by adopting the letter of the EU provision almost verbatim. Still, it is important to note that the Italian legislature, also by adopting the letter of the EU provision, clarifies that ROs, for the purposes of Article 70-ter l.aut, refers to universities, including their libraries, research institutes or any other entity whose primary objective is to conduct scientific research or to carry out teaching activities that include scientific research, which alternatively: (a) operate on a non-profit basis or whose bylaws provide for the reinvestment of profits in scientific research activities, including in the form of public-private partnerships; (b) pursue an aim of public interest recognised by a Member State of the European Union. Also in this context, the Italian provision clarifies that the ROs on which business enterprises can exert a decisive influence, such as having preferential access to the results generated by scientific research activities, cannot benefit from this TDM E/L.
Directive 2006/116/EC of the European Parliament and of the Council of 12 December 2006 on the term of protection of copyright and certain related rights (Codified version), OJ L 372, 27.12.2006, p. 12-18.	The Term Directive harmonised the duration of legal protection envisioned for copyright-protected works, including software and databases, while also setting the standards concerning the calculation of the term of protection as such as well as the duration of legal protection envisioned for copyright-protected works originated in non-EU countries. Whereas it is neither possible nor desired to enlist the details of such calculation methods for each category of copyright-protected works, the following shall be included herein as the key points of the Term Directive: • In principle, the copyright protection envisioned for literary and artistic works, including "original" software and database, lasts during the lifetime of the author(s) and 70 years after the death of the (last surviving) author (Article 1). • As a general principle, **Article 8** of the Directive stipulates that the term of protection begins simultaneously in all EU

	Member States, and it is calculated from the 1st of January of the year following the event giving rise to it. • Last but not least, **Article 7** of the Term Directive stipulates that the works originated from non-EU countries and whose authors are not nationals of an EU Member State shall be protected in the EU as long as the legal protection continues in the country of origin. However, this term shall not exceed the term of protection envisioned in the EU copyright legislation for the same category of works.
Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (Text with EEA relevance), OJ L 157, 15.06.2016, p. 1-18.	The Trade Secrets Directive introduces the minimum standards for the legal protection to be provided for trade secrets by all the EU Member States, while also encouraging the Member States to adopt measures that go beyond the standards set thereby. In this context, the following constitute the key points of the Directive, which were instrumental to harmonising the legal protection of trade secrets across the EU: • **Article 2(1)** of the Directive articulates the term "trade secret" over three cumulative definitive criteria. o First, for any information to be considered a trade secret, it shall comprise information that is, "as a body or in the precise configuration and assembly of its components," not known among or readily accessible to persons "within the circles that normally deal with the kind of information in question". o Second, information as such shall have commercial value which stems from the fact that it has been kept as a secret. o Last, the person in control of such information should have taken "reasonable steps" to keep such information secret. • **Article 3** regulates the ways in which a trade secret can be legally acquired, used or disclosed. Whereas the national laws of the EU Member States other circumstances to justify the acquisition, use or disclosure of trade secrets, the Directive identifies the following as the lawful means to acquire a trade secret: o Independent discovery or creation of a trade secret. o Reverse engineering or in other words "observation, study, disassembly or testing of a product or object that has been made available to the public". o Through the exercise of workers' rights or workers' representatives' rights to information or consultation regulated within the Union or national laws. o Any other practice that is in conformity with honest commercial practices. • Aligned with the lawful acquisition, use or disclosure of trade secrets, **Article 4** of the Directive enlists the unlawful acquisition, use and disclosure of such confidential information.

	• According to **Article 4(2),** the following acts would be deemed unlawful acquisition of a trade secret: o "Unauthorised access to, appropriation of, or copying of any documents, objects, materials, substances or electronic files" which are under the control of the trade secret holder and which contain the trade secret or from which the trade secret can be deduced. o Performance of any other act that would be contrary to honest commercial practices. • Likewise, the following acts, enlisted in **Article 4(3)**, would be considered unlawful use or disclosure of a trade secret: o The use or disclosure of a trade secret that has been unlawfully acquired. o The use or disclosure of a trade secret carried out in a way that would breach a confidentiality agreement or any other duty not to disclose such information. o The use or disclosure of a trade secret carried out in a way that would breach a contractual or any other duty which limits the use of the trade secret. • Last but not least, **Article 5** of the Directive introduces certain limitations to the exclusive rights of trade secret holders. According to this provision, the acquisition, use or disclose of a trade secret would be exempted from the scope of unlawful practices if they are performed under the following circumstances: o For exercising the right to freedom of expression and information. o For revealing misconduct, wrongdoing or illegal activity if performed for protecting the greater public interest. o The communication between workers and their representatives as long as such communication is happening as part of the exercise of rights justified by the Union or national laws. o For protecting a legitimate interest recognised by the Union or national laws.
Directive 98/71/EC of the European Parliament and of the Council of 13 October 1998 on the legal protection of designs, OJ L 289, 28.10.1998, p. 28-35.	The Design Directive, while harmonising the national legislations of the Member States, creates a common ground for the legal protection of industrial designs by introducing precise definitions for the key terminology, clarifying the eligibility criteria for legal protection, the scope and term of the legal protection conferred upon designs, as well as the limitations to the exclusive rights of the registered design holder. The key take-aways of the Design Directive are, especially with respect to the BRIEF activities, as follows: • **Article 1** of the Directive defines the key terminology as follows: o The term "design" refers to "the appearance of the whole or a part of a product resulting from the features of, in particular, the lines, contours, colours,

	shape, texture and/or materials of the product itself or its ornamentation". o The term "product" which is essential to the definition of "design" is articulated as "any industrial or handicraft item, including inter alia parts intended to be assembled into a complex product, packaging, get-up, graphic symbols and typographic typefaces". Whereas computer programs are explicitly excluded from the scope of the definition of "product", the broadly articulated description of the term as such applies to 3D printed products or parts thereof. • **Articles 2** and **3(1)** of the Directive crystalize that the legal protection envisioned for industrial design requires the registration of the design at the competent intellectual/industrial property office in the country in which legal protection is sought. • **Article 3(2)** of the Directive sets the eligibility criteria for legal protection. According to this provision, a design would be protected by a design right only if it is new and has individual character. • In light of the regulation within **Article 4**, a design would be deemed new only if "no identical design has been made available to the public" before. As to the other criteria, **Article 5** holds that a design would be considered to have an individual character if "the overall impression it produces on the informed user differs from the overall impression produced on such a user by any design which has been made available to the public before (...)". • **Article 7** contours the eligibility criteria for legal protection by clarifying that designs that are dictated by the technical function of the product or by the standards to enable the compatibility of a product with others would not be deemed new or individual character. • Likewise, **Article 8** of the Directive excludes designs that are contrary to public policy or morality from the scope of the Directive. • A registered design, as per **Article 12** of the Directive, would entitle the rightsholder to the exclusive rights to use the design and to prevent third parties from using the design. The use of the design encompasses acts such as launching a product to the market which bears the design; and importing, exporting or stocking a product as such. • As regulated by **Article 10**, the term of legal protection conferred to the rightsholder starts from the date of the filing of the registration application and lasts for 5 years. The term of protection can be renewed for 5-year periods multiple times, however up to a maximum of 25 years. • **Article 13(1)** of the Directive provides a regulation that is of pivotal importance for BRIEF activities, as it identifies the limitations to the exclusive rights of the design rightsholder. According to this provision, the performance of the following acts does not conflict with the exclusive rights of the design rightsholder:

	○ Acts done in privately and for non-commercial purposes, ○ Acts done for experimental purposes, ○ Acts of reproduction for making citations or for teaching. However, these acts shall be compatible with fair-trade practices and shall not unduly prejudice the normal exploitation of the design. Additionally, these acts shall be accompanied by the indication of the source of the design in use.
Council Regulation (EC) No 6/2002 of 12 December 2001 on Community designs, OJ L 3, 05.01.2002, p. 1-24.	The Community Design Regulation sets the norms for the EU-wide protection of industrial designs. Therefore, the content of the Regulation is largely procedural as the vast majority of the legal provisions encompassed within the Regulation are concerned with the application to be submitted to the EUIPO for the registration of an industrial design, the examination of such an application, the possible consequences of the examination process, the establishment of the design courts to resolve legal disputes concerning Community designs and the like. Whereas the substantial provisions of the Regulation closely follow the letter of the Design Directive, the legal provisions on the protection of unregistered designs constitute a novel aspect of the Regulation, as this aspect has not been covered within the Design Directive. Therefore, it is worth briefly reflecting on the legal protection of unregistered designs. The Regulation adopts the same definitions for "design" and "product" as well as the eligibility criteria required for acquiring design rights. Nevertheless, the novelty and individual character criteria are slightly adapted to the features of unregistered designs, as it is no longer possible to take the date of application for the registration as a reference point. In this regard, **Article 5(1)(a)** of the Regulation holds that the benchmark for novelty and individual character would be determined by considering the designs that have existed before the design in question has been made available to the public. Similarly, **Article 11(1)** stipulates that the term of protection envisioned for unregistered designs would start from the date on which the design has been made available to the public for the first time within the EU. The design will be under legal protection for a three-year period starting from this date. As opposed to the term of protection envisaged for registered designs, the term of protection for registered designs is not subject to renewal. Finally, **Article 19(2)** introduces an important regulation which impacts the exclusive rights of the design rightsholder. According to this provision, the rightsholder of an unregistered design can prevent the use of the design by third parties only if such use "results from copying the protected design".

Proposals of EU legislation	*Main principles that will be applicable to BRIEF RI activities*
European Health Data Space (EHDS, secondary use of health Data for research, COM/2022/197 final), EDHS	EHDS proposal will give rise to a new EU harmonised framework which will eventually: • Support individuals to take control of their own health data • Support the use of health data for better healthcare delivery, better research, innovation and policy making • Safe and secure exchange, use and reuse of health data in centralized infrastructures designated by MS
Cyber resilience Act (proposal on cybersecurity requirements for products with digital elements, COM/2022/454 final)	This is a horizontal regulation which will serve as a "mold" for whichever more specific document will be applicable for the cybersecurity of e-health devices. At the moment, this proposal excludes E-health applications (medical devices) but it does include wearable devices which might also have E-health functions.
Product liability directive proposal (COM/2022/495 final) PLDU	This proposal will be crucial for all interconnected devices, such as the IoT and that can use as well AI systems either at the edge or in the cloud. Moreover, the product liability directive is the main liability regime that is applicable as a consequence of the non compliance with the MDR, MR and AI act duties whenever a connected object and software are involved. There are similarities with the AILP, but in the new text voted on 12 March 2024 by the EU parliament, the relationship between the two liability directives has been made implicit. What is noticeable is that, as well as in the AILP, there are two articles which deal with the disclosure of evidence and also with presumptions. In the PLD, these presumptions can concern the defectiveness of the product and the causal link between the defective product and the damage sustained by the claimant. Moreover, the specific mention of surrogation in the position who has been damaged makes it clear that to insurance contracts will become of even greater importance in goods with digital elements issues.
AI civil liability directive proposal (COM/2022/496 final)	It involves new rules (especially Articles 3 and 4) concerning the harmonization of tort liability rules whenever an AI system contributes or directly causes a damage. However, the AILP will most probably be modified at length as it was closely connected to the AI Act official proposal of 2021 when GPAIs where not yet present. It might take a long time before there will be an agreed text on this issue.

Table 5. First part of the cross-field analysis that identifies the main features and the ethical-legal principles of each regulation that are relevant in the R&D&I sectors, especially for data-driven research infrastructures based on robotics applications

The mapping also needs to be supplemented with areas of private law that are expressly regulated in the civil code or special laws in Italy (or in the given legal system).

In the technological and digital dimension, the known paradigms require in fact adaptations to EU regulations or practical applications to align the different legal institutions and develop common procedures applicable to the daily life-cycle of R&D&I.

Below some samples of cross-field legal areas that are impacting on the ethical legal framework shaped by the above illustrated legislations referred to the EU data strategy on R&D&I sectors.

Cross-field legal areas	*Paradigms and issues to be addressed*
Insurance issues	The insurances legal discipline in Italy is divided between the Italian civil code (general dispositions) and special laws. • The articles from **1882 to 1932** of the **Italian Civil Code** deal with the general aspects of insurance contracts. This discipline has not been modified since the publication of the Civil Code but the Court of Cassation has interpreted the general articles in order to admit, at certain conditions, the use of the so-called 'claims-made' clauses in 2016 and 2018. These insurance policy clauses were originally born in Common law countries but are becoming increasingly common also in the EU has they can also give relevance to the circumstances of the damage (claims made deeming clause) and have a period of validity beyond the end of the insurance policy (claims made sunset clause). • The specific discipline of private insurance instead can be found at L.D. 7 September 2005, n. 209, **Codice delle assicurazioni private** and subsequent modifications. It is a code of EU inspiration which sets rules on private insurance policies and sets also up the **IVASS** (Istituto per la Vigilanza sulle Assicurazioni) the body that must exercise checks on insurance policy intermediaries with the objective to protect the insured clients and to maintain a fairly competitive insurance market. At present, there are not specialised insurance policy contracts for new technologies, but insurances companies are researching and trying to understand how to draft these new contractual clauses while at the same time dealing with the digital transition, including the AI-based solutions, implementation in their daily work[108].
Liability issues	Both in extra-contractual and product liability cases, there are traditional notions of: • Unfulfillment of a contractual obligation • causality link, • fault/ presumption of fault The rules for both contractual and extra-contractual liability can be found in the ICC. The general rules concerning **obligations-duties of care** can be found from **Articles 1173 until 1320 of the Italian Civil Code**. Then from **Article 1321 and ff. of the Italian Civil Code,** one can find the rules on **contracts.** Finally, the rules on **tort/extracontractual liability** from can be found from **Articles 2043** until **2059 of the Italian Civil Code**. They partly share the rules on how to calculate **compensation** (articles from **1123-1229**). The main difference between these two forms of liability is that, in case of contractual liability, there is always a contractual relationship among the parties. Conversely, in the extra-contractual/tort liability a damage occurs between two or more parties who are not tied by a contractual relationship.

[108] Unipol "Quaderno Intelligenza Artificiale e Robotica" https://www.unipol.it/sites/corporate/files/document_attachments/quaderno_intelligenza-artificiale-e-robotica_2017.pdf

Intellectual property	Issues concerning intellectual property are of particular interest: • patents and standard essential patents, SEPS, proposal for a regulation. In Italian law, patents are dealt within the Code of Industrial Property, D.lgs. 30/2005 and partly by the Italian Civil Code (see art. **2585** and following). • trade-secrets (D.lgs. 11 May 2018 n. 63, implementing the Directive EU/2016/943 on the same theme). • technology transfers. At a national level there was the creation of ENEA Tech in 2022, a national foundation that is deemed to help Universities and Research Hubs to transfer IP from universities and research institutions to the industry. Moreover, it is important that the rules on block-exemption when interpreting Article 101(3) TFEU to research and development horizontal agreements have been recently modified and need to be implemented soon in Italy[109] concerning collusive agreements as they will become binding from 1st July 2023. These are actually some of the legal issues that have the higher chance to come across while designing, deploying and commercializing BioRobotic devices.
Contractual matters	The complex chains of production and the coexistence between hardware and software parts of a BioRobotic device could make it necessary to have contracts with companies which are specialised in the supply of software services or hardware production. The relationship with these other subjects is regulated by contracts, hence the relevance of this subject.
Health Law	This is a discipline which is now very diversified but relevant to the BRIEF project as many of its subparts (e.g., clinical trials, certification issues and insurance policies) will be needed for R&D&I. It is also a legal discipline that has become increasingly complex and needs to be explained and simplified for the operators of this sector, BioRobotic experts included. • Risk management and insurance • Healthcare services organisation • Medical malpractice

Table 6: second part of the cross-field analysis that identifies cross-field legal areas

5. GAPS AND ENABLERS IDENTIFICATION

The following step for providing a cross-field analysis is to identify from the interplay of the different legislative initiatives interpretative gaps and inconsistencies that may arise in the practical application of the illustrated principles and obligations, as well as the legal provisions acting as enablers for certain common purposes that could either help to define standards or policies and recommendations. In the following subparagraphs there will be a list of the more relevant gaps and enablers under the lenses of a BRIEF stakeholder.

[109] Regione Toscana " Antitrust la commissione UE ha adottato una revisione dei regolamenti orizzontali di esenzione per categoria sugli accordi di ricerca e sviluppo" https://www.regione.toscana.it/-/antitrust-la-commissione-ue-ha-adottato-una-revisione-dei-regolamenti-orizzontali-di-esenzione-per-categoria-sugli-accordi-di-ricerca-e-sviluppo-r-s-e-di-specializzazione accessed 03 July 2023

5.1 Gaps and enablers

As a preliminary step, it is important to clarify that in this deliverable, gaps are intended as, in general, legal and/or administrative factors (or the lack of) which can hamper innovation in any way. With specific reference to the BRIEF project, innovation corresponds to the scientific and practical output, being it in form of either new technologies, protocols, or scientific research articles. Conversely, enablers are all the factors of legal and/or administrative nature that can foster innovation, in general, and with specific reference for the BRIEF ecosystem.

As seen in the mapping, there are several proposals at the EU level that can be of interest to the BRIEF partners and stakeholders. Most of them are either in the middle or at the end of the EU legislative procedure, hence, most of them are not still binding yet from a legal point of view. However, the principles they refer to, which are set in the recital part of these proposals, oftentimes do have an ethical meaning and force which need to be known and implemented as well as the future operative rules. The presence of ethical rules is an opportunity for innovators as it allows planning for the design of new allied technologies even if the operating rules might be different or not into force, because they will respond to the same principles.

All the legislative proposals and acts that were previously outlined may contain both gaps and enablers. In the following sub-paragraphs, there will be an explanation of a possible classification, which will synthetise the main gaps and enablers emerging from this cross-field analysis.

From a methodological viewpoint, the identification of gaps and enablers is relevant to shape those interpretations that are functional to facilitate the compliance process. In fact, covering with good practices the administrative/legal gaps and taking advantage of the enablers, R&D&I activities will be facilitated.

Once set the practical need, it will be possible to compare the legislative initiatives shaping the legal framework and through the identification of gaps and enablers, law and policy making activities will be developed through operational rules etc. For instance, we will discuss how this process is particularly relevant for the common need to enable secondary use of data. In fact, it constitutes a precious opportunity to capitalize on research results, share and make it be useful not only for publication but also for the development of business ideas which might or might not benefit the health sector.

Considering that there are three main applications of the secondary use of data that may emerge in the context of BRIEF activities, we will identify gaps and enablers among the reconstructed legal mapping in order to achieve the purposes of data sharing, as listed below.

Secondary use of data	*Purposes*
Secondary use of data for research	It allows using good quality data in order to better substantiate research in terms of responsible innovation, as it is the premises for its replicability and reproducibility.
Secondary use health data for research	Healthcare sector will benefit from the data sharing and reuse in order to provide more personalised, predictive, precise, participatory, and preventive medicine.
Secondary use of data as an economic asset	It is important also to capitalize the economic value of data, an element that must be taken in consideration when developing products that will be commercialized such as new technologies and theoretical and applied research.

Table 7: Secondary uses for data. A list.

5.2. General gaps and enablers emerging from the cross-fields analysis

Some gaps are related to notions and definitions that are not completely overlapping between different initiatives. Other ones refer to procedural inconsistencies that could require to identify in the practical scenario a harmonised solution able to comply with different sets of obligations. In other cases, again, gaps may just be referred to lack of a provision establishing a specific term or condition that instead would have solved interpretative issues related to a given step of the R&D&I life-cycle.

As stated, gaps and enablers might emerge both from a theoretical comparison of the sources of law and from their practical application.

In this regard, looking at the most impacting regulations like the AI Act and Data Act, we may immediately remark an interpretive issue arising from the related fields of application.

In the AI act, thus, the categorisation of AI systems into high and low risk may not be straightforward in practice. Moreover, what the research exemption excludes is also of difficult interpretation, when it comes to settings that are not "pure" research settings, since many AI systems developed within research laboratories may be later commercialized or put into use. Similarly, the Data Act can be applied in theory to several IoT objects, no specifications are reserved for those impacting on the healthcare sector/market. The main problem with these endeavours, however laudable, is the effective time that they will need to be effectively implemented: we can take as a wake-up call the implementation of the CTR. It was officially approved in 2014 but even in 2024 the CTR is not yet fully operational. This could be potentially the near future concerning proposals such as the EHDS and for some part for the Cyber-resilience Act.

A first methodological approach to avoid these negative implications - due to the fact that legislative progress has a slower evolution than the technological one is - to address the ethical-legal principles in a responsible and accountable way, fostering the compliance by design and by default also with the common principles emerging from the discussed proposals regardless of the effective time of their approval or their implementation. From this perspective, the reference to a trustworthy approach stands for overcoming the formal barriers in order to achieve a higher level of compliance with the EU values. If it shall be translated into providing an impact assessment for new AI-based technologies impacting to fundamental rights protection (like dignity, healthcare, private life, data protection, employment, etc), this could be an interpretative solution to be boosted in terms of legal enabler.

There is another group of legal acts that are currently being implemented, meaning the MDR and the CTR which are also the first serious efforts concerning harmonization in public health. More specifically, the gaps that can be found in the CTR is that despite its effort to make the clinical trials discipline thoroughly harmonized, there are still many differences in the ways the ethical committees are being implemented and reorganized into national (and even local) law. As far as the MDR is concerned, it is not yet fully operational and it is not yet clear what is to be the relationship between manufacturers, insurance companies, and product liability rules (See Article 10.16 MDR).

The last group of gaps concerns more closely IoT products and liability rules. The more a technological device is complex, effective but also expensive, the more likely it will become object of specific insurance policies. In the absence of a generalised EU law policy on high-risk technologies and of medical devices it is important to try to understand how insurance law will evolve. Moreover, depending on the high or low risk of the AI system embedded in the given device, there will be the application of either the Product Liability Directive Update or the AI civil liability directive (and therefore the national implementation according to specific territoriality criteria). The new PLDU is not quite clearly connected to the MDR, unlike the actual one and the AI civil liability directive risks creating fragmentation problems given that *de facto* parts of the civil procedure and civil substantial law will be changed according to the directive indications but leaving the MS a relative amount of freedom on how to implement it.

In this uncertain legal framework, the experience of over 5 years of GDPR application could help to identify common interpretations to be followed as *precedent* to justify a given choice under the principle of accountability. Nevertheless, there are still interpretative doubts also arising from the GDPR and its application especially in the research and development domain.

More concretely, the attribution of the roles of controller and processor for devices and technologies for connected environments is allocated case-by-case: in fact, the role of controller or processor is of capital importance as most of the compliance duties fall on the controller and the EDPB[110] to have a more substantial approach when deciding who the controller is. This means that even if an organisation is appointed as the data processor but *de facto* has controller tasks or just disregards the tasks assigned to them and adds new ones, then it will be considered a controller. This approach could affect the burden of the proof also in terms of liability either for data breach related damage compensation or for other losses that may occur to a data subject / user of a given solution/device.

Finally, as a general gap, there is **a lack of harmonization and coordination** concerning the implementation of EU legal acts at national level. These risks undermine the creation of a Digital Single Market because among the different Member States implementations that increase the fragmented approach, introducing legal barriers – especially for cross-border scenarios.

The table below refers more in detail the lacks and gaps emerging from the interplay of the legislative initiatives insisting on the fields of EU Data Strategy, Public Health, and Artificial Intelligence package that might require a systematic interpretation in order to not constitute a barrier to the innovation.

Legislative act	*Gaps and lacks to be interpreted*
GDPR	The allocation of roles between players as (joint) controllers, processors, third parties and recipients might become extremely multilayered considering the complexity of the supply and value chains. Its translation into a data sharing agreement could be difficult to be standardised. Also the lack of pre-determined technical and organisational measures to be applied in case of pseudonymised and anonymised data may constitute a barrier, as the result of a data protection impact assessment could be perceived as different levels of risks for similar data processing activities. National implementations introducing different safeguards as additive conditions to process sensitive data under article 9 and – especially for scientific research and

[110] EDPB, "Guidelines 07/2020 on the concepts of controller and processor in the GDPR," https://edpb.europa.eu/our-work-tools/documents/public-consultations/2020/guidelines-072020-concepts-controller-and_en accessed 13 July 2023.

	statistics purposes – could constitute a barrier for data sharing. For example, in Italy, the consent of the data subject is required also in cases where the GDPR seems to promote another legal basis for data processing, like in the case of use and reuse of health-related data for scientific purposes (see policy briefs n.1, 2, 3,4).
MDR	According to the new framework all the medical devices producers have to comply with the new and numerous duties (which involve also post-market surveillance) in addition with the process involving conformity certification by Notified Bodies. This complex system requires the implementation of a general strategy of compliance (see policy briefs n. 6, 7, 8).
Clinical Trials Regulation (CTR) and implementation	The legislative decree concerning the implementation of the clinical trials regulation was voted some years ago but the more centralised paradigm for carrying out clinical studies at the EU level had to be reconciled with the disciplines of the Italian Ethical Committees which used to be several in most of regions. Now this aspect has been dealt with by the last decrees of January and June 2023, but it is still uncertain whether the implementation of the national law will be sufficient and/or efficient given that there is still the possibility to adhere to the old regime. In fact, it is true that the EU CTR wants to promote a more unified and harmonized take on clinical trials, in theory. In practice, implementing the unified Clinical Trials portal (CTIS) and database EUDAMED took years and in 2023 the CTR is not fully applied/operational. Moreover, there are many differences and discrepancies in how the EU countries implemented these rules. This makes it difficult to find EU partnerships for more effective and cross-national clinical trials (see policy briefs 5,8).
AI Act (AIA)	Some forms of AI are forbidden, such as the ones that discriminate against a person or certain groups and those that use subliminal techniques to manipulate decision-making (which could be a risk of certain human-brain interfaces). Among the forms of AI systems that are admissible there is a main division between high-risk and not high-risk AI systems. If the system is considered high-risk through the combination of the definition at Article 6 AIA and Annex I-III, there are many compliance obligations concerning the design and the implementation of the AI system (e.g., risk assessment, transparency, documentation, etc), which places an additional burden on researchers throughout the entire lifecycle when the systems are meant to be commercialized or put in use (and thereby go beyond mere research settings). Moreover, the sectorial and national implementations could represent a barrier to innovation.
Data Act (DA)	The aim of the DA is to set a general regulation for **any kind of IoT object**. This proposal's wide range of application makes it difficult to foresee how its implementation will unfold. More specifically, the DA spans from cloud providers switching capabilities to data-sharing in 'emergencies' to the access to one's own IoT data to develop another product (read IoT object) or a service on a secondary market. The obligations of all the parties involved (mainly the user, the recipient and data holder) and how the contracts among them should be regulated are explained at Articles 3-13 of the proposal. Moreover, at this stage, the DA does not make any difference between IoT with consumer/professional functions and e-health IoTs. This also makes it more complicated to **coordinate** this proposal with all the EU e-health law block of legislation as data concerning health needs more protection in general than 'less sensitive' categories of personal data.

Table 8: Legislative acts gaps and interpretative barriers

Proposal	*Gaps*

EDHS proposal	The EDHS proposal sets the groundwork for the creation of a new system to share health record data and to take advantage of the secondary use of the health data. However, in order to operate efficiently, it requires quite some work in terms of **standardisation** and **interoperability** among the systems of the different EU Member States (MS) and the proposal in itself does not give much practical guidance on this aspect.
Cyber-resilience Act proposal	This proposal fulfils the important function to lay down horizontal rules -meaning quite general ones- which could allow better interoperability and incentivise the creation of new shared IT standards to overturn the present low level of cybersecurity standards of products with digital elements. The proposal is quite clear in creating an administrative system based on **notified bodies** that should make the operators involved more accountable. However, it is now difficult to foresee whether there would not be any confusion among this proposal's connections **with other EU proposals or EU legislative acts and area of application**. In particular, see the more general safety regulation and the machinery regulation and as well as with the newly approved NIS 2 directive.
Machinery Regulation (MR)	While in the MR proposal there was an explicit reference to the AI act, the same cannot be said in the text of the approved MR regulation. Still in the approved AI act in Annex III there is still the reference to the machinery regulation in the description of high-risk AI systems in connection with Article 6 but also in the definition part, when the meaning[111] 'safety component' is described. Software is included in the definition of safety components[112] and can be a (high-risk) AI system if it is '*fully or partially self-evolving using machine learning approaches ensuring safety functions*'[113]. Nevertheless, in the MR software is important also for other things such as to access technical documents necessary for the correct use and conformity of the machinery[114]. For the safety component AI software, one has to look in Annex III concerning essential health and safety requirements. In Part B of the mentioned Annex III. it is explained that it is important to protect from corruption or hazardous intentions the software and data that "*are critical for the compliance of the machinery or related product with the relevant essential health and safety requirements*" [115] . Further on among the different requirements of the control system it is mentioned that "*the tracing log of the data generated in relation to an intervention and of the versions of safety software uploaded after the machinery or related product has been placed on the market or put into service is enabled for five years after such upload, exclusively to demonstrate the conformity of the machinery or related product with this Annex further to a reasoned request from a competent national authority*"[116]. The fact that the connection with the AI act is not clear anymore from the text of the MR is a gap in the sense that there is no clear definition on how to harmonize the conformity procedures, meaning the one concerning a high-risk AI system and the one concerning software as a security component. The introduction of AI for safety components is also an enabler as it allows machine manufacturers to be more informed about AI and its risks as decided by Article 4 b of the AI act on AI literacy.

[111] 3(14) AIA.
[112] Article 3(3) MR.
[113] Recital 19 MR.
[114] Article 10 MR
[115] MR, Annex III, Part B, 1.1.9
[116] MR, Annex III, Part B, 1.2.1 (f)

	The MR proposal's aim is to **update the current machinery directive discipline** which could not be entirely applied to new devices and items that are influenced by technological developments such as the ones in the BioRobotic field. The MR includes in its **ANNEX I** (which gives a list of high-risk machinery devices) also **software ensuring safety functions, including AI systems** and **Machinery embedding AI systems ensuring safety functions** (n. 24 and 25). However, its connection with the risk assessment for fundamental rights that is foreseen in the AI Act proposal is not clearly explained in the following annexes.
Product Liability Directive Update (PLDU) proposal	The product liability directive update apparently has a well-defined field of application. However, it is not clear how it will relate to the update of the Medical Devices Regulation (MDR) and to the AI civil liability directive proposal as far as AI low and high-risk systems are concerned. In fact, the MDR refers to the actual PLD by stating that the manufacturer must have enough funds (including insurance) to cover for product liability costs (Article 10.16 MDR). This reference to the MDR is not present in the new text of the proposal. That makes it clear that it will depend on the evaluation about whether the AI system powering the object is either high or low risk that the PLDU or the AI civil liability would be applicable. This new division changes the rules on how to prove damage, fault and the causality link. In fact, the PLDU tries to achieve a balance between the instances of the consumers and of the manufacturers, but it is slightly more tilted towards the consumers' side (see articles 4, 6, 7,8,9). Moreover, formally, the PLDU also can guarantee (at certain conditions) **compensation for data damage**, which is considered a product, a good, even when it is not used for professional purposes. However, the PLDU application is formally separated by the rules concerning personal data, and in particular, Article 82 GDPR which explains how data protection rules damage should be compensated. The criteria about compensation according to Article 82 have also been explained in a recent judgment by the EU Court of Justice (C-300/21)[117].
AI civil liability proposal	The most relevant changes this proposed directive is going to bring forward are rules concerning civil procedure of the Member States. In particular, the rules concerning the difficulty in proving the connection (causal link) between the damage and the fault caused by the AI system. In particular, Article 3- **disclosure of evidence** and rebuttable presumption of noncompliance- and Article 4 of the proposal – **rebuttable presumption of a causal link in the case of fault**-provide principles according to which the MS civil procedural laws will need to conform. Being it not explicit about the maximum or minimum character of the proposal, it might be implied that the Member States have sufficient leeway in implementing these rules amend to make them more harmonised with their legal tradition. The problem is that they might implement them in a very different way from each other. This last element risks to limit the collaboration between the internal partners and external stakeholders that could be in other MS.

Table 9: EU proposals gaps and interpretative barriers.

Conversely, even if the previously described EU legal acts and proposals unveil unclear parts and their respective coordination seems uncertain, it is important to highlight that **they do contain important reference to EU values and general principles** that could be used as enablers to solve any interpretative issue or gap.

First of all, the risk-based approach that has been developed in the GDPR drives all the mentioned initiatives. Therefore, once that the main player (data holder, data controller, manufacturer, sponsor etc) is identified, an assessment under the relevant ethical legal framework shall be formally / informally undertaken, possibly with support of domain experts.

[117] Judgment of the Court (Third Chamber) of 4 May 2023. *UI v Österreichische Post AG.*, C-300/21, ECLI:EU:C:2023 :370.

This would be useful to identify for each step of the given data processing activity (methodology / solution development) not only binding obligations, but also soft law safeguards that could be required in the short and medium term during the life-cycle of the R&D&I.

The table below illustrates for each legal initiative how the combination of enablers respect to the purposes and objective of a given legislative initiative may find specific barriers in their practical implementation that need to be addressed through a methodological approach inspired to general principles of accountability aiming to develop structured ethical-legal assessments by design and by default.

Proposal/ Legal Act	*Enablers*	*Barriers*	*Methodological solution*
GDPR	Risk based approach including self-assessment activities for the data controller. *Favor* for the reuse of personal data for scientific research and statistics purposes. *Favor* for self-regulatory mechanisms for similar data processing activities (codes of conducts). Collaborative tools between data controllers and data protection authorities. Data Protection Officer to drive compliance activities.	Room for national safeguards for data processing activities for research and statistics purposes that might identify further constrains for cross-border data processing (e.g. the role of consent for the reuse of health-related data for research purposes). Unclear differences between private and public nature of the data controllers, as well as between research and Research & Development & Innovation purposes.	Any action shall be justified under the general principles. Data protection impact assessment is a part of the ethical legal compliance by design and by default in any case there is a personal data processing concerning health data and their reuse for research and innovation purposes.
DGA	Intermediation services as safeguards for data subjects' rights. *Favor* for bottom-up mechanisms of data sharing through data altruism bodies. Collective control, oversight and exercise of the rights of the data	Complexity to set up intermediation services. Level of awareness for data subjects is still low in terms of opportunities provided by data altruism mechanisms. Different nature and structure of cooperatives in Member States.	Development of common guidelines for consent collection and management through services of intermediation. Development of common terms and conditions for platforms offering data.

	subjects through data cooperatives pursuing mutualistic scope.		
MDR	Risk based approach tailored to the medical device classification. Introduction of EUDAMED the common MD database; There should be a person which is in charge of the MDR compliance. There is a standardisation not only of certification procedures per se but also of manufacturers' obligations and of whoever is involved in the process, and of post-market surveillance obligations.	Long period for the EUDAMED portal implementation Medical devices manufacturers are undergoing several procedures to have their devices certified again. Compliance with the new rules must be proved and one must expect also post-market surveillance of the product	To develop a risk-based strategy, including compliance with conformity assessment procedure for managing modifications to the devices; appoint a person responsible for regulatory compliance and its monitoring. Prepare and keep up to date all the technical documentation for each device.
CTR	There will be a functioning unified portal (CTIS) and it will rationalise and harmonise at the least the beginning of the procedure. The ethical committees are in charge of the procedures evaluation, but the sponsor and the investigator(s) are the roles leading the creation of the relevant documentation and the implementation of the clinical trial.	Long period of implementation Ethical committee discipline depends on Member States and often by local practises.	Principle of the highest level of protection of human health and accountability allow to take the proper balance between different needs, rights, or interests.
Cyber resilience act	Ensuring the highest possible level of cybersecurity, that is combined with the	Might take a long time to have an approved and coherent set of common and interoperable standards.	Refer to standards and safeguards developed by ENISA in order to carry out a *by design* assessment

	robustness pillar under AI Act.		under the cybersecurity ground of analysis.
EDHS	Safe environment to share electronic health data for their reuse. Centralisation of health data flows with common safeguards and procedures of access and sharing. Possibility to request the health data access body to elaborate data and provide an aggregate result. Incidental findings communicated through the health data access body.	Complex structure to guarantee the interoperability of Member States health records but also to allow the secondary use of data. The level of awareness and training on the matter is still low.	It will be important to follow-up any relevant standard concerning health, as well as interoperability of data formats. Privacy information shall include the possibility that today a given data flow stored for secondary use purposes could then converge into an EDHS once established.
PLDU	Data are considered as products that can be damaged; the EU consumer must always have an EU-based legal subject to whom they can ask for compensation. New rules on how to prove defectiveness and the causality link in objects with digital elements	Adaptation of the products/good legal concept to data which had always been considered as part of software; complex to implement the procedural inputs that have been put in the proposal.	Need to be updated with important national cybersecurity agency updates on what are the risks of malfunctioning; it will be necessary to better design the product (generally an IoT object) in advance.
AI Civil Liability Dir. (proposal)	Presumption of liability for the manufacturer. Obligation of providing technical information on the AI system in case a damage occurred.	Complex rules concerning the proof of causation and fault whenever the AI system is high risk according to the AI act. National implementations are required as it is a directive.	Need to focus on the design of the AI system and try to make it as explainable as possible.
Machinery Products Reg. (proposal)	Protection of human health and risk management	Rules that will partly interconnect with the AI act because of the mention in the Annex I.	Necessity to follow up on the connection between AI high risk systems.
AI Act	All of the above principles plus a general	The classification in high and low risk AI system will often depend also on the concrete features of the AI	Guidelines are already available to perform the ethical legal assessment (see ALTAI checklist) and

	principle of protection of fundamental rights	system and its functions. Thus it is challenging to provide general recommendations. The exemption for scientific research does not apply to start-ups and SMEs, thus it may be challenging in the BRIEF R&D ecosystem to understand which responsibilities apply to whom, since some AI systems may be developed within academic settings but then commercialized within spin-offs. Moreover, transparency, documentation, data governance and human oversight requirements for high-risk systems need to rely on information produced throughout the entire life-cycle, thus also during initial phases of research. This places an additional burden on researchers. Even when the legal provisions do not apply because the AI system is only developed for pure scientific purposes, researchers still need to respect research ethics safeguards.	for ethical conduct in computer science and engineering research. Following ethical guidelines early-on may help researchers proactively predispose their AI systems for later commercialization.

Table 10: Enablers Barriers and Practical Consequences

6. INTERPRETATIVE ISSUES EMERGING IN CONCRETE SCENARIOS

To test and validate the undertaken cross-field analysis, it is useful to develop practical scenarios where the application of some provisions included in the illustrated legislative frameworks may arise controversial interpretations. In fact, it is quite common that in order to proceed in the life-cycle of the R&D&I activities, specific decisions shall be undertaken either to cover a legislative gap, or to properly solve an overlapping between different provisions, or fostering an enabler in order to better exploit a situation / protect given rights.

6.1. Scenario A) Reuse of health data

Development of a study where data previously collected by clinical centres for healthcare purposes are processed by a team of engineers to train a robotic platform aiming to develop some tasks to support clinical diagnosis.

The first issue concerns the identification of conditions and requirements to reuse data processed for healthcare purposes. The second one refers to whether it is mandatory to recontact patient or not for consent and / or to receive an ethical committee approval.

In order to solve this practical case, it is important to illustrate the position of the Italian DPA, which spans from the EDPB approach[118].

As far as the reuse of data for statistics and scientific research is concerned, article 89 GDPR and article 5 GDPR are relevant. In particular, Article 89 GDPR titled "*Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes*", states that the MS while processing personal data for archiving purposes in the public interest, and among other things, for research must ensure that the personal data processing is subjected to appropriate safeguards. More specifically, those safeguards can consist of organizational or technical measures which must be focussed to obtain the enactment of the data minimization principle, which is protected by Article 5(1) GDPR. As an example, pseudonymization is explicitly mentioned. In the second paragraph, however, MS are granted a certain leeway, meaning that they can provide for derogations from the applications of Articles 15 (right of access by the data subject) 16 (right to rectification by the data subject) 18 (right to restriction of processing), 21 (right to object) and to some conditions of the first paragraph of the same Article 89 GDPR, provided that "*such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes".* As in all EU law, exceptions and derogations must be interpreted in a strict way.

To sum up, even though processing for research and scientific purpose is possible, it must be done in a way that complies with the GDPR main principles. That is, on the one hand, to ensure the respect of the fundamental right to data protection, and, on the other hand, to allow personal data circulation by taking into account a risk management approach. This means that the data controller must enact all the technical and organizational measures that are deemed essential to ensure the rights of the data subjects. Derogations are allowed but just for some specific articles and only when the GDPR obligations seriously make the achievement of one of the listed purposes, such as the scientific research one, impossible, which is rarely an occurrence, hence this paragraph must be applied rarely and only when truly necessary. On the basis of these reasoning the analysis of the practical case can be developed.

In this regard, data concerning health belongs to the series of personal data that is protected by Article 9(1) GDPR and that, according to 9(2) could only be processed where some of the conditions listed are actually met. In an opinion of 2019 [119], the Italian Data Protection Authority considers the main bases to process data concerning health are the following:

- Reasons of public interest on the basis of Union or Member States law (Article 9(2)(g) GDPR).

[118] Source cited in Table 1.
[119] Garante per la Protezione dei Dati Personali "Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario – 7 marzo 2019 [9091942]" https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9091942.

- Reasons of public interest in the public health sector (Article 9(2)(i) GDPR).
- Reasons concerning preventive medicine, diagnosis, assistance, health or social therapy or management of health and social services (Article 9(2)(h) GDPR).

However, these legal bases do not exclude the other options that are provided by the same Article 9(2) whenever they fit best for the purpose of the treatment. This is for instance the case of consent at Article 9(2)(a).

To this set of considerations, it must be kept in mind that the Italian Data Protection Authority with its opinion of 2022[120] also introduced the concept of "*consenso a fasi progressive*" (progressive consent) concerning health data. This means that whenever consent is the legal basis on which the processing (according to Articles 6(1) and 9(2)(a) GDPR) it must be **the most specific possible**. Whenever a kind of processing was not specifically mentioned in the privacy policy /data protection document, the controller -the hospital where the data are collected, in this case- must also specify that data could be processed by processors or third parties as it appears to be in this case for research purposes (see policy brief n. 4).

This means that patients should be contacted again in case the initial consent form was not clear enough (also by giving examples in the privacy policy) that patients' personal data could be used for medical research also from the third parties, such as the researchers in this case.

The best-case scenario would be to modify the privacy policy accordingly if this processing case is not explicitly considered by the hospital policy document. However, sometimes, to wait for the modification of the privacy policy to enter into force could require time to the disadvantage of the research. That is why it is indeed possible to recontact the patients but there is a further distinction to consider and that depends whether the hospital where the research data is collected is either a private or a public structure.

If it is a private legal entity, it can recontact the patients on the basis of its legitimate interest (Article 6(1)(f) combined with Article 6(4) GDPR) and let the patients know that they can always refuse this further processing of their personal data. If it is a public structure, it can use the reason of public interest in the health sector.

In this complex framework of checks and balances, other procedure shall be taken into consideration in order to maintain an accountable behaviour. For example, if the data are used for a clinical trial or study by a clinical centre, the submission of the protocol to the competent ethical committee is mandatory for enabling the health-related data flows under the Italian Data Protection Authority authorisation of June 5th 2019, as well as under the Ethics rules on data processing for scientific research and statistics for research activities carried out by a university/research centre.

The second issue may concern how to establish the data governance (roles and responsibilities), ownership and access rights to the new dataset.

As far as the data governance is concerned, the data flows from the hospital to the research centre shall be governed under an agreement of joint-controllership, if the two centres are both deciding means and purposes of the re-use of the data previously collected for healthcare purposes by the hospital; or through an appointment of data processor if it is the hospital

[120] Garante per la Protezione dei Dati Personali "Parere ai sensi dell'art.110 del Codice e dell'art.36 del Regolamento- 30 giugno 2022 [9791886]" https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9791886

outsourcing the research in order then to use the results of the platform; or through a data sharing agreement in which the research centre will then process data as an autonomous data controller.

Considering that the research group is carrying out a kind of processing (namely aiming to develop a new diagnosis system) that in the end produces an outcome which could benefit the hospital even though not directly. In this sense, more than processor or third party, the research group could be considered – for this specific purpose- autonomous, therefore a kind of controller. This line of interpretation is actually the one proposed by the EDPB[121]. Once the platform has been developed and used to create research results data, then, the new dataset could:

i) belong to both (the hospital and the research centre) and be either private or public;
ii) belong to only one of the two centres and be either private or public;
iii) belong to a third party and be either private or public.

An agreement between the two centres shall state the governance, ownership, and access rights. This would allow to better solve the issues concerning accountability, but also to better allocate risks and liability. This is because the initial data set officially belongs to the hospital and the data subjects, but the outcome is of the research group. As a part of this strategy, it is suggested to elaborate a data management plan to clearly know:

- which kind of data the parties own
- the quantity of data they specifically have on site.
- which purpose and which kind of processing they want to carry out
- what their cybersecurity strategy is
- what the communication strategy with the patients is in case of a data breach and the drafting of a Data Protection Impact Assessment (DPIA)

ALTAI checklist and other ethical duties on algorithms trained on the data

From an ethical point of view, it is indeed helpful to use the ALTAI checklist for the part of data processing undertaken by algorithms, in order to make the AI-based solution (in the example the platform) ethically compliant even before the entry into force of the AI act.

The checklist addresses the 7 grounds of analysis through 63 open questions that could drive the compliance activities by design and by default. If the requests of the check-list cases are met, the AI system shall be considered compliant.

Academic researchers have an ethical duty under the principles of reliability, honesty, respect and accountability of the European Code of Research Integrity. For example, reliability concerns the verification of the produced content and avoiding equality and non-discrimination issues. This means that scientists need to address potential sources of bias in their training datasets and the outputs that their models produce. Honesty may mean disclosing whether certain tools of AI, including generative AI, have been used for supporting the analysis of data. Respect is related not only to research participants, but also to society and environment at large. Researchers need to consider the limitations, environmental impacts, and societal effects of the AI model they develop, with an eye on privacy, confidentiality and intellectual property. This

[121] EDPB, " Guidelines 07/2020 on the concepts of controller and processor in the GDPR", https://edpb.europa.eu/our-work-tools/documents/public-consultations/2020/guidelines-072020-concepts-controller-and_en accessed 03 July 2023

means, among the others, that the lawful and fair use of personal and non-personal data is always paramount. Accountability refers to the responsibility of researchers who must be able to justify their conduct from idea to publication, as well as provide means to other parties to oversee their conduct and assess the possible risks and misuse of the AI models they create (see also Policy Brief 1 on Accountability).

Will the AI Act apply?

If the algorithm trained on the health data is developed for pure research purposes, a superficial analysis could conclude that the AI Act does not apply (see Article 2(6)). However, it is not entirely the case, especially when the algorithm leaves the research settings to be employed in the real-world and can be classified as a medical device (hence: a high-risk AI system). This means that researchers need to carefully reflect on the foreseeable uses of the AI systems that they develop, because most obligations that apply to AI systems have far-reaching repercussions and request that are considered early on.

For example, the transparency requirements of Article 13 impose that developers of high-risk AI systems disclose information on the intended purpose, technical capabilities, input data, performance of the system on certain groups or persons. Moreover, information that can help its users to interpret the output and deploy the system correctly as well as the accuracy of the model should also be disclosed as to avoid misuse (see **Policy Brief no 12**). In addition, appropriate documentation should be provided to demonstrate compliance with the AI Act's provisions of Article 11 and should contain, among others, details about the expected outcomes, the system architectures, the employed datasets, the monitoring, functioning and control of the AI system, such as its capabilities and limitations in performance and the foreseeable unintended outcomes and sources of risks. It should also contain information about the training data sets used (thereby partially overlapping data governance): about their provenance, scope and main characteristics; how the data was obtained and selected; labelling procedures (e.g. for supervised learning), and data cleaning methodologies (e.g. outliers detection) (see Article 11 and Annex IV). Especially when there is the risk of bias and unlawful discrimination, relevant information about data governance is also useful to determine and maintain the risk management system (Article 9) and to enable human oversight (Article 14) to prevent or minimize harm. In conclusion, there are many requirements on the use of data for training and validation that are imposed by the AI Act and that need to be considered and addressed early on to ensure compliance by design and by default. Ignoring this recommendation implies that it is going to be impossible to commercialize or use the system outside of research settings.

Once developed issues addressed by design, which steps to put it on the market? And in the healthcare system?

Once the design part is completed, it would be interesting to discuss which following steps there could be in terms of a commercialisation of the future robotic platform. Regardless of the final user's type (private or public), if the robotic platform has a medical function, the route to take is the certification according to the MDR. The length of this process depends also by the level of risk that that it will be assigned to the medical device. Moreover, there should be checks concerning the compatibility with the requirements set forth by the AI Act, especially how to categorise the AI systems (high *v.* low risk) that could be used by the platform. If the device/platform is finally marketed, it will probably be very expensive and maybe not really necessary for private use. Therefore, the envisaged location should be the one of either a private or a public hospital. Some more elements to think about are connected to the concretisation of risks theme. There is the possibility that AI algorithms might cause a damage to a person, either

of material or immaterial nature. In this case, the distinction between high and low risk AI systems is crucial: if the AI system is considered high-risk then the AI civil liability directive will be applicable (whenever it is approved). If, instead, the AI system used is considered a low-risk system the new Product Liability Directive Update (PLDU) proposal could be applicable. Moreover, at Article 5 PLDU, the possibility of insurance companies to surrogate themselves instead of the patient and for a person to bring a collective action against a producer is now expressly mentioned in the draft text. At the moment, this is also allowed under the current regime as the MDR makes direct reference to the product liability directive and mandates the producer to have sufficient means (e.g. insurance) through which it could face product liability and also class action claims.

6.2. Scenario B) Research on children

Consider the following scenario: the objective is the development of a survey aiming to analyse the level of usability and acceptability of a wearable prototype for children.

How to address children's vulnerability? How do parents get involved? Who is going to answer? Parents?

As a preliminary remark before providing suggestions to solve this scenario, there is the necessity to explain if, how, and when, minors can actually express consent to data processing at Article 8 GDPR and to participate to a study providing an informed consent.

As known, children are considered vulnerable categories of subjects and vulnerable data subjects *par excellence,* however, according to their maturity and age their vulnerability shall be balanced with their right to express their own opinion. For example, in proceedings concerning children of 12 years old, it is required to ensure their right to be heard. From a practical point of view, the issue is related to the fact that the data controller shall introduce technical and organisational measures aiming to collect consent from the entitled user: the legal representative or directly from the child. The same practical issue (with different factors that shall be assessed by the researcher) shall be addressed in case of children engagement in a study, where beyond the formal information related to the age threshold, also the maturity and self-confidence shall be assessed case-by-case, determining a different role of the parent/legal representative for the informed consent purposes.

From a data protection perspective, Article 8 GDPR sets at 16 years old the age from which the minor could validly express their consent for services of the information society. However, this disposition leaves leeway to the Member States to set a lower age threshold which, in any case, cannot go below 13 years. In Italy, article 2 *quinquies* of the Italian Privacy Code refers to 14 years old. In any case, it is the controller, who sets the means and purposes of the data processing (Articles 4(7) and 24 GDPR), must make sure that, "*in those cases, the consent is given or authorised by the holder of the parental responsibility over the child,* ***taking into consideration available technology***[122]" (Article 8 GDPR). This means that it does not always need to be the perfect *ad hoc* technology to make sure the parents are informed, but the best combination of means available that can ultimately protect the child.

The main legal bases to process data in the context of a survey to assess the usability and acceptability of a prototype are:

[122] Emphasis added.

- Contract relationship Article 6(1)(b) GDPR: if the trial of the prototype is included in a contractual relationship between the developer and the user. It seems unlikely in our scenario including children.
- Legitimate interest Article 6(1)(f) GDPR: especially, if the structure offering to fill in the survey is private. Otherwise, if the survey is developed by a public research centre/university article 89 GDPR is applicable.
- Vital interest of the subject 6(1)(d) GDPR: in extreme hypothesis, if the prototype is applied in a clinical trial and the user is also patient.
- Consent (but keeping in mind to distinguish the consent to fill the survey that could be express with undertaking the survey and the consent to process data). In case, no other legal basis is applicable, consent could be required (with double thick on the survey and on the privacy information). It is also necessary to consider: i) that whenever there is a new purpose a new consent must be obtained and, ii) age limits to express consent, otherwise the legal representative one is required) Article 6(1)(a) GDPR.

Even if the parents of the children who are minors can legally provide consent to data processing, as requested by Article 8 GDPR, from an ethical point of view the situation is more nuanced.

In fact, if one considers also the Charter of Fundamental Rights of the EU, Article 24 considers that they have a right to "*express their views freely. Such views shall be taken into consideration on matters which concern them in accordance with their age and maturity*"[123]. That is why, despite the Italian implementation of the GDPR sets at 14 the age through which a minor can express their consent to data processing, in this case, because of the clinical or non-clinical research implications it is important to follow a precise check list as far as the methodology in obtaining the parents' consent but also to let the child understand the procedure they will actually have to go through.

Considering these premises, the methodology to solve the case-scenario could be the following one.

The survey shall be designed in a way that it also respects the principle of data minimization set at article 5(1) GDPR. Therefore, all personal data collected shall be justified in terms of necessity and proportionality. To this end, it is preferable to ask for range of information in order to receive aggregate answers.

Then, it could be recommended (or even mandatory according to internal procedures, namely institutional protocols for engaging children in research activities) to draft an ethical protocol for the involvement of children in research activities which could be submitted to relevant ethical committees for approval[124]. It has to be structured in a way to describe all the possible situations that the research facility could have the need to require minors to participate in research and to detail whether there is privacy or bodily invasive or non-invasive practices and always to opt for the least invasive ones. Briefly, this document must i) identify the current risks; ii) list the organizational and technical measures to avoid or limit the risks from

[123] As cited in the Scuola Sant'Anna document titled "CHILDREN'S PROTECTION IN RESEARCH ACTIVITIES" approved by the Academic Senate with Decision n.267 of 10/12/2020, https://www.santannapisa.it/en/node/55403, accessed 13 July 2023, 3.
[124] One can take inspiration from the one drafted by Scuola Superiore Sant'Anna.

happening; iii) to outline in a clear way who has taken on roles and responsibilities and iv) to describe how accountability will be taken if anything happens.

The second thing is to draft an information privacy for legal representatives and for children. As above-mentioned, there are techniques of legal design which could help in drafting the data protection documents for informed consent in a way that even a child could understand.

Finally, the research group needs to get the informed consent of the legal representative informed consent for children including legal representative's authorisation.

For the informed consent purposes three different cases may arise:

I) Minors below or 13 years old (14 in Italy): need for their parents to answer the survey for them. However, the children's opinion is legally relevant from 12 years old (or lower in case of particular maturity of the child): a balance shall be undertaken. Information sheet, privacy policy, and informed consent shall be signed by the legal representatives. Additional information sheet shall be provided in a child-friendly language for the child.
II) Between 13 (14 in Italy) and 17 years old: the minors can fill in the survey but there must be a data protection/privacy document that is written in a child-friendly way: through simple language, including icons in a way to have a clear outline of the privacy risks and consequences for them. Specific legal design techniques are applicable. Information sheet, privacy policy, and informed consent shall be signed by the child and the parents shall provide an authorisation to proceed.

From 18 onwards (so for the legal representatives) there should be in any case a privacy policy that is easily understandable for all adults, even the ones who are not used to data protection rules.

6.3. Scenario C) Monitoring of accessible public areas with drones

Consider the following scenario: the municipality asks you to conduct an experiment aimed at enhancing the city's security. In particular, you are required to provide technical expertise through the design of drones equipped with cameras and microphones able to capture videos and detect particular sounds (like screams or help requests) in accessible public areas (such as squares or streets). Successively, these data will be processed in order to detect useful patterns for future alarm systems.

6.3.1. The first issue concerns how to conduct a correct data protection impact assessment in such scenarios.

In cases such as the one described below, you will be considered "data processors" under Article 4 of the GDPR and the obligations enshrined in Article 28 shall be observed. In particular, among all the obligations, the data processor assists "*the controller in ensuring compliance with the obligations pursuant to Article 32 to 36 taking into account the nature of processing and the information available to the processor*".
The cited provisions concern security measures, data breaches and the data protection impact assessment (DPIA). The latter will be explained hereafter.

Under article 35 paragraph 1 "*where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data*". According to article 35 paragraph 3, the DPIA is surely required when "*a systematic monitoring of a publicly accessible area on a large scale*" occurs, and this is the case described here.
As data processor, you will be asked to assist the data controller (the municipality in this scenario) during the preparation of the DPIA.
In particular, combining Article 35 GDPR and the opinion of the Article 29 Data Protection Working Party (01/2015) on Privacy and Data Protection Issues relating to the Utilisation of drones, you shall assess the impact by providing:

- A) "a systematic description of the envisaged processing operations and the purposes of the processing…";
- B) "an assessment of the necessity and proportionality of the processing operations in relation to the purposes" is due;
- C) "an assessment of the risks to the rights and freedoms of data subjects" and an explanation concerning "the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned".

Starting from letter A), you are required to indicate what kind of data you are processing (personal, non-personal and particular categories of data, the so-called sensitive data). The Italian Data Protection Authority stated that in data processing such as the one discussed here, the DPIA shall contain an explanation on the impossibility of conducting the research without processing particular categories of data like conversations; then, it shall be indicated who are the data subjects (you will need to specify to who is oriented your data processing) and the data retention period (in months or years). Moreover, you will need to specify the means of processing (hardware, software, persons, nets etc.). The Italian Data Protection Authority requires a detailed description of the means used, such as the specific datasets, software etc.
Moving to letter B), Article 35 requires an explanation of the necessity and proportionality of the processing. Thus, you will need to specify the legal basis for the processing (in this scenario, the monitoring of accessible public areas) according to Article 6; the specific purposes of this data processing (in this case the research project aimed to enhance the city's security); the legitimacy of the purpose given that only some public authorities, in certain cases, can monitor accessible public areas. So you will need to be appointed by these authorities and provide proof of it. Recently, the Italian Data Protection Authority specified the duty to prove the need to conduct such monitoring activities in real areas while possible also in simulated scenarios, so it will be important to provide solid reasons for this specific data processing in public areas; you will be also asked to explain why the data you are processing are adequate, pertinent ad limited only to those necessary according to article 5; also, you shall indicate the retention period under article 5.
To fulfil the obligations described under C), you shall describe the origin, the nature, the peculiarities and severity of the potential risks related to the specific processing (unauthorised access, loss of data, risks associated with the perception of mass surveillance by the inhabitants etc.).

In order to assess these factors, it is important to identify the incidents likely to occur, the sources of risks, the likelihood and the severity, the measures appointed to prevent them and the consequences of these risks materializing on fundamental rights of the inhabitants (considering in particular the combination of severity and likelihood). As an example: what is the potential impact (in terms of likelihood and severity) of the loss of data related to religious beliefs of minorities?
The Italian Data Protection Authority recalls Article 35 paragraph 9 stating that in scenarios like this, data controllers and data processors shall involve the potential stakeholders (the inhabitants) and collect feedback from them.

6.3.2. The second issue concerns the implementation of proper anonymisation techniques according to the GDPR.

As data processors, as long as you process personal data, you will be asked to implement appropriate technical and organisational measures to ensure level of security according to Article 28 GDPR.
On the other hand, according to recital 26 GDPR, if data processed are not classifiable as personal data, you will be not obliged to respect the GDPR provisions. Given that, if the original processing involves personal data, the only way to convert them in non-personal data is the anonymisation.
The Article 29 Working Party, in the opinion 05/2014 on anonymisation techniques, clarified as the anonymisation of personal data is *per se* a personal data processing. Only after it, GDPR will not apply; before it, it will apply. Recently, the Italian Data Protection Authority affirmed that also temporary collecting of personal data, such as the people's faces before the anonymisation, constitutes data processing, therefore all the measures prescribed by Article 32 shall be respected before the anonymisation.
Still, the Italian Data Protection Authority explained how to make anonymisation techniques adequate to the scenario here described. In particular, the Authority stated that personal data collected by microphones are not adequately anonymised if the technique consists in the substitution of the inhabitants' voices with a fake voice, keeping unaltered the characteristics of the audio signal, including the content of the conversation. The Authority highlighted that the voice substitution was not adequate because from the conversation's content personal information related to the speaker and to third persons may be derived. So, this specific technique will not be considered proper anonymisation. The microphones will need to be designed in order to keep conversations not audible for data controllers and data processors, especially if the intended purpose of the microphone is to detect just loud sounds, otherwise it would be possible to identify the data subjects.
Concerning the visual contents recorded by drones, the Italian Data Protection Authority stated that a proper anonymisation technique cannot be limited to the obfuscation of faces or vehicle number plates. In facts, data subjects are still identifiable through other characteristics such as the body type, clothing, place of the recording etc. Moreover, this information may be combined with data collected by the microphones and with other data collected by thirds, so resulting in personal data after the combination.
Furthermore, the fact the video resolution is not high is not enough to prove a correct anonymisation, even more if video data are combined with audio data.

To conclude, the anonymisation must guarantee the result of the impossible identification of the data subjects.

6.4. Scenario D) Development and placement on the market of a posture support for work-time, aimed to decrease physical fatigue during desk work, equipped with an AI system as a safety component able to detect system's failures.

6.4.1 How to assess the conformity of the AI-equipped posture support?

In case of the development and placement on the market of a posture support for work-time equipped with an AI system as a safety component, there are two relevant pieces of legislation: the Machinery Regulation (MR) and the Artificial Intelligence Act (AIA). The reason why the Medical Device Regulation (MDR) is not involved is because the described posture support does not fulfil the requirements set by the MDR to classify it as a medical device[125]. In facts, it is not intended to cure the worker, but just to enhance his/her work conditions.
If the manufacturer aims to place the product on the market, specific procedures must be followed. Once these are observed, the manufacturer will obtain the CE marking, which certifies the conformity of the support with the EU standards for health and safety. Both MR and AIA procedures must be followed (AIA works as a horizontal regulation, thus its rules will be added to the MR ones).
In this case, the manufacturer of the support is also the developer of the AI system.

6.4.2. Conformity under Machinery Regulation.

Firstly, the manufacturer shall identify the correct conformity assessment module provided by the MR. It lays down four different modules[126]. When artificial intelligence (referred to by the regulation as fully or partially self-evolving behaviour using machine learning approaches

[125] «medical device' means any instrument, apparatus, appliance, software, implant, reagent, material or other article intended by the manufacturer to be used, alone or in combination, for human beings for one or more of the following specific medical purposes:
— diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease,
— diagnosis, monitoring, treatment, alleviation of, or compensation for, an injury or disability,
— investigation, replacement or modification of the anatomy or of a physiological or pathological process or state,
— providing information by means of in vitro examination of specimens derived from the human body, including organ, blood and tissue donations, and which does not achieve its principal intended action by pharmacological, immunological or metabolic means, in or on the human body, but which may be assisted in its function by such means. The following products shall also be deemed to be medical devices:
— devices for the control or support of conception;
— products specifically intended for the cleaning, disinfection or sterilisation».

[126] The modules applicable when AI systems are involved are described in Annex VII, VIII, IX,X.

ensuring safety functions) is involved, according to annex I[127], the manufacturer shall undergo the conformity assessment indicated by Article 25 paragraph 2. In case of AI, the latter prescribes, alternatively, 3 types of procedures on manufacturer's choice: 1) EU type-examination (module B), followed by conformity to type based on internal production control (module C); 2) conformity based on full quality assurance (module H); 3) conformity based on unit verification (module G).
Once the module is selected, then several obligations are set.
The combination of modules B and C requires the manufacturer to undergo two different assessments. Firstly, module B describes the EU-type examination, which entails an EU-notified body examination; if at its end the support is compliant with the regulation, the examination will result in a certificate of conformity. This procedure must be combined with the one described under module C (conformity to type based on internal production control), which requires the manufacturer to ensure that the support is compliant with the type described in the EU type-examination certificate. Later, the regulation prescribes the affixation of the CE marking on the support in conformity with the type described in the EU type-examination certificate. The procedure ends once the manufacturer draws up an EU declaration of conformity for the support and keeps it at the disposal of the national authorities for at least 10 years after the support has been placed on the market or put into service.
Moving forward, module H (conformity based on full quality assurance) prescribes the manufacturer to operate an approved quality system for design, manufacture and final product inspection and testing.
The manufacturer shall apply for an assessment of its quality system to the notified body of its choice. The quality system shall ensure compliance of the support with the requirements of this Regulation. All the elements, requirements and provisions adopted by the manufacturer shall be documented in a systematic and orderly manner in the form of written policies, procedures, and instructions.
The notified body shall assess the quality system to determine whether it satisfies the prescribed requirements. The notified body's decision shall contain the conclusions of the audit and the reasoned assessment decision. Once received the decision, the manufacturer shall undertake to fulfil the obligations arising out of the quality system as approved and to maintain it so that it remains adequate and efficient.
Still, the manufacturer shall keep the notified body that has approved the quality system informed of any intended change to the quality system and the latter shall evaluate any proposed changes. Successively, the manufacturer shall affix the required CE marking and draw up a written EU declaration of conformity for the support and keep it at the disposal of the national authorities for at least 10 years.
The last possible choice is the module G (conformity based on unit verification). Under it, the manufacturer will make available proper technical documentation, to let the notified body be able to assess the support's conformity with the relevant essential health and safety requirements set out in Annex III and shall include an adequate analysis and assessment of the risks.
A notified body chosen by the manufacturer shall carry out appropriate examinations and tests, to check the conformity of the support with the applicable essential health and safety requirements set out in Annex III or have them carried out. The notified body shall issue a

[127] Annex I, part A, pargraph 1, number 5-6.

certificate in respect of the examinations and tests carried out. The manufacturer shall keep the certificates at the disposal of the national authorities for at least 10 years after the support has been placed on the market.
The manufacturer shall affix the required CE marking as seen before.
Finally, shall draw up a written EU declaration of conformity and keep it at the disposal of the national authorities for at least 10 years after the support has been placed on the market or put into service.

6.4.3. Conformity under Artificial Intelligence Act.

The previously explained framework applies to support with AI safety components. These types of supports are regulated also by the Artificial Intelligence Act, once into force. According to article 6 AIA, all the systems covered by the legislation indicated in Annex I are considered high-risk systems under the AIA, therefore several obligations are mandated upon the manufacturer. Annex I explicitly refers to the Machinery Regulation, thus, AI systems working as safety component in machineries (as described by Article 3 MR) are considered high-risk systems under the AIA.
Manufacturers of such high-risk AI systems shall run a conformity assessment procedure before their products can be sold and used in the EU. They will need to comply with a range of requirements including testing, data training and cybersecurity.
The risk management obligations (art 9 AIA) first require identification of the reasonably foreseeable risks that the support can pose to health, safety or fundamental rights when it is used in accordance with its intended purpose. Consequently, it is prescribed the adoption of appropriate and targeted risk management measures designed to eliminate or reduce the risks identified. The measures shall be such that the relevant residual risk associated with each hazard, as well as the overall residual risk of the high-risk AI systems, is judged to be acceptable.
Moreover, high-risk AI systems which make use of techniques involving the training of AI models with data shall be developed on the basis of training, validation and testing data sets that meet the quality criteria provided by Article 10 AIA. Training, validation and testing data sets shall be relevant, sufficiently representative, and to the best extent possible, free of errors and complete in view of the intended purpose. They shall have the appropriate statistical properties, including, where applicable, as regards the persons or groups of persons in relation to whom the high-risk AI system is intended to be used.
Moreover, according to Article 13, the support shall be designed and developed in such a way as to ensure that their operation is sufficiently transparent to enable deployers to interpret a system's output and use it appropriately.
Among the several duties set for, some of them may overlap with the ones provided by the machinery regulation. For example, there is no clear definition of how to harmonise the conformity procedures set for by the MR and the AIA. Or, the log recording is prescribed both by AIA (art. 12) and MR (Annex III, part B, 1.2.1, f). Technical documentation described by article 11 AIA may overlap with the one set for by module G, Annex I, MR.
Furthermore, AIA and MR lack harmonised standards. It is still possible to apply the ones designed under the machinery directive (EN ISO 14121-1 – Safety of machinery – Risk assessment – Part 1: Principles), still in force until 2027, but they should be updated to face AI challenges.

7. MAIN PRINCIPLES

As a result of the preliminary cross-fields analysis above-introduced and the possible applications we illustrated in the previous paragraph, we provided a series of methodological remarks and suggestions that may be considered to identify some principles inspiring systematic interpretations of the different matters. We will focus here on the principles of accountability, transparency and fairness as they are the most general underpinning all the previously cited legal acts.

Firstly, the principle of **accountability** refers to the possibility, for both controllers and processors, of always being able to justify their data processing activities. Accountability is the motor of data protection governance: we find it explicitly stated in general terms in article 5(2) GDPR[128], but then it is in the chapter devoted to the duties and obligations of both the processors and the controller that one can find concrete examples of it (chapter IV of the GDPR). For instance, the obligation of keeping a record of the processing activities (article 30 GDPR) or the drafting of a DPIA (article 35 GDPR) as well as being in charge of the security of the processing (article 32 GDPR) are concrete examples of accountability. Moreover, the principle of accountability is also connected to the principle of privacy by design and by default of article 25 GDPR. Being accountable and responsible for the data processing that happens because of a product, service or methodology that we develop means also to design it in a way that is the most data protection and privacy protective. Furthermore, it is important that all the choices taken by whoever wants to process data can be explained and, if possible, that there is a (preferably written) record of the motivations underpinning technological, organizational and economical choices. In this way to have a data management plan is already very important in order to be accountable. However, to be accountable not only means to just complete the tasks that are assigned by the GDPR but it coincides also with a more pro-active attitude: the controller must always think in ways that even the data processing is made better and is less invasive of data subjects' fundamental rights. This also brings on a radical shift in the way of thinking about data-protection and privacy also while carrying out scientific research: being accountable by respecting legal and ethical duties and obligation might actually turn out to be fruitful and improve scientific research[129].

The principle of **transparency** refers to the obligation the controller has to inform the data subjects (e.g. patients, or more generally users) about the ways in which their data is being processed[130]. In order to inform the data subjects of how their data is being used, and if there are any changes to the original forms and ways of processing, the **language used must be clear and comprehensible** (article 12 GDPR). This means also to employ techniques of legal design such as icons, or other graphic techniques that make privacy policies easily understandable.

---

[128] Paul de Hert and Guillermo Lazcoz, "When GDPR-Principles Blind Each Other: Accountability, Not Transparency at the Heart of Algorithmic Governance," *European Data Protection Law Review* 1(2022): 31-39.
[129] Denise Amram, "Building up the "Accountable Ulysses" model. The impact of GDPR and national implementations, ethics, and health-data research: Comparative remarks," *Computer Law and Security Review* 37(2020): https://doi.org/10.1016/j.clsr.2020.105413.
[130] Council of Europe and EU Fundamental Rights Agency (FRA), *Handbook on European data protection law* (Luxembourg: 2018), 119-122.

The principle of **fairness** is included between lawfulness and transparency, but it has not always been easy to define, as it clearly interacts with those above-mentioned principles that we can read at article 5(1)(a) GDPR[131]. It can be interpreted, in accordance with the context, as not only being strongly entwined with lawfulness and transparency but also with "*non-discrimination, fair balancing, procedural fairness, bona fide*"[132]. It will depend on the specific context to understand whether a certain procedure allows for a balance - such as, for instance, an updated privacy policy and a dynamic way of filling in a survey to make the data subject more aware- or, instead, if it is the case for non-discriminating certain groups of people who might constitute a minority quantitatively, but could be important for the accuracy of data processing results.

The table below shows how the interpretations developed in light of each mentioned principles under the GDPR could be useful to solve some practical issues emerging in the research life-cycle concerning R&D&I sectors from the interplay with other normative requirements and conditions.

Principle	*Practical need*	*Interpretative solution*
Accountability	To define time to pseudonymise data collected in a clinical or non-clinical trial	According to the principle of minimisation, pseudonymisation techniques shall be implemented to the dataset as soon as possible, for example, as long as the dataset has been validated, before the analysis.
Transparency		The information on the applied criterion shall be included in the privacy policy.
Fairness		Once pseudonymised no attempts of individuals reidentification shall be undertaken.
Accountability	To define information to be selected in a survey regarding the profiling of participants	Instead of asking the volunteer age, address, nationality, it is better to provide range of information, eg. age: 18-30,31-45, etc; in Milan municipality, Tuscany Region, Spain, EU / non-EU etc., EU – non-EU. Choices shall take into account the number and quality of data.
Transparency		The level of aggregation of the collected information shall be included in the privacy policy.
Fairness		Profiling activities shall be explainable.

[131] Gianclaudio Malgieri, "The concept of Fairness in the GDPR: A linguistic and contextual explanation," Proceedings of FAT* '20, January 27–30, 2020. ACM, New York, NY, USA, 14 pages. DOI: https://doi.org/10.1145/3351095.3372868.
[132] Ibid.

Accountability	To define roles and responsibilities in the clinical protocol and for the data governance purposes	Roles and responsibilities shall be allocated considering the concrete activities and life-cycle of the research more than possible formal constrains.
Transparency		The information sheet and the privacy policy shall include details on the governance of the study and on the data governance, especially to facilitate the exercise of participants' rights.
Fairness		The roles and responsibilities allocation shall avoid any discriminatory conditions.

Table 11: Main guiding principles of the GDPR

8. PRELIMINARY POLICIES AND RECOMMENDATIONS

This first cross-field analysis allows to develop a series of policy and recommendations aiming to shape a responsible – and at the same time effective - approach towards the development of biorobotic devices and allied technologies from an ethical-legal perspective.

To this end, we address the following policies and recommendations impacting on two different aspects of the life-cycle of the research.

The first one refers to a checklist for developers, innovators, and researchers aiming to address the main pillars of the ethical-legal compliance during the different steps of the life-cycle of the research.

Preparatory activities	*Comments*
Develop an ethical-legal compliance strategy	If you are unfamiliar with the concepts of impact assessment, accountability, pseudonymisation, data management plan, open data, open science, take time to extend your skills and competence.
Check whether the development you your idea implies either personal data processing, or non-personal data processing, or volunteers' engagement, or algorithms and their training, etc.	Calls for funding may include tailored templates for self-assessing these profiles.
Check skills and competence in your team: if you are not covering the ethical-legal implications of your idea, ask for advice.	Some issues may be addressed directly from the institutional roles (*e.g.* the Intellectual Property Office, Data Protection Officer, etc.), other tasks might require further specialistic advice.
Research Management	*Comments*

Allocate time and resources to develop the applicable ethical-legal framework to the life-cycle of the research, considering: a. The EU strategy on Data, Public Health, and AI, where relevant for your life-cycle. b. Possible specific safeguards implemented at national, or local level for a given sector.	Take into account possible initiatives entering into force in the near future/during the research life-cycle. If a conflict of application arises, you will take the decision considering the principles of accountability, transparency, and fairness.
Develop a data management plan in order to: a. Define datasets that the life-cycle of the research will generate b. Identify organisational and technical safeguards to collect, process, store, share, and reuse datasets according to the characteristics of data.	If one(more) protocol(s) shall be submitted to the competent ethical committee(s), allocate proper time and resource to develop it (them). If one(more) data sharing agreements shall be developed, allocate proper time and resources. If a data protection impact assessment / fundamental rights impact assessments shall be developed, allocate proper time and resources.
Research development	*Comments*
Identify monitoring measures to ensure the proper development of the compliance strategy.	Allocate roles and responsibilities either among partners or in your team.
Identify proper measures to ensure fundamental rights exercise from individuals and reporting activities.	If you are developing AI-based solutions, apply the ALTAI checklist by default. In addition, be mindful of the requirements of the AI Act that apply if the AI system is meant to, or could potentially, be put in use outside research settings or commercialized, especially when it comes to AI systems that can be categorized as medical devices, and thus would be classified as high-risk AI systems under the AI Act. If you are dealing with the digital data, services, platforms, software and other digital assets dimension, check the ENISA standards for cybersecurity and robustness. If you involve vulnerable individuals / groups (*eg* children, patients, refugees) check whether institutional, local, international standards are required.
Identify assessment checks to balance different principles and rights.	Compliance activities may require the interplay of different soft skills to take the more

	appropriate decision that may change over the life-cycle of the research.
Dissemination and Exploitation	*Comments*
Develop a dissemination and exploitation plan aligned with the adopted strategy of data	*e.g.,* in case of Open Science, the Data Management Plan shall be coherent with the dissemination and exploitation strategy.
Adopt a procedure for making information public: the use of website, online platforms, social media, contacts processing for communication and dissemination purposes, pictures and reports publications, newsletters, surveys etc	Keep in mind the principle of minimisation and what you have declared in the privacy information / information sheet.

Table 12: Preliminary best practices part 1

The second one refers to a guideline to address possible legislative inconsistencies, specific requirements emerging from the law in action related to national or sectorial implementations of the discussed EU legislative initiatives in order to cover possible gaps.

Unclear requirement	*Comments*
Ethical Committee Approval for non-clinical studies	It could be mandatory for the funding organisation/institution. It could be mandatory considering the involvement of vulnerable subjects (patients, minors, refugees, etc) according to local / sectorial / institutional procedures. It could be mandatory for Conference organisers or for the journal editor / publisher to disseminate your results. It could be mandatory under a contractual clause between partners.
Data retention in an ethical protocol	It should be distinguished between research data and administrative information (like informed consent templates). Personal, even if, pseudonymised data shall be stored only the necessary duration of the activities where it is relevant that the data subject could be re-identified /identifiable. Research data shall be anonymised as soon as possible: once anonymised data can be stored without any limits. Informed consents sheets and templates must be kept available for 5 years after the project ends under the Italian Data Protection Authority Ethics code on data processing for statistics and research purposes. Other terms might be introduced by funding organisations or in other legal system. In case of clinical trials, according to CTR, the content of the clinical trial master file - unless other Union law requires archiving for a longer period- shall be archived for at least 25 years after the end of the clinical trial by the sponsor and the investigator. Medical files of subjects shall be archived in accordance with national law.
Data sharing agreement	It could be required by the ethical committee as an attachment to be analysed. It could be required by the funding organisation/institution. It is recommended to set data governance and ownership, as well as to allocate roles and responsibilities in a data-driven research activity clinical and non-clinical study. It is a contractual tool, therefore, it is effective among those who are signing it.

	It may include data processor appointments, agreements of joint controllership under the GDPR, as well as terms and condition for data sharing and reuse. It could be signed by those who have the power on behalf of the CEO in signing activities related to the matter.
Unclear definition of sole purpose of scientific research and development (AI Act)	If the AI system is meant to be put into service or on the market (and thereby exit the pure research settings), researchers should understand early on if their device will be categorized as high-risk system. If it is the case, such as when it is a medical device, researchers should comply with the requirements set forth for the developers of high-risk systems.

Table 13: Preliminary policy recommendations part II

CONCLUSIONS

This deliverable summarises the main ethical legal challenges that arise in a R&D&I life-cycle, providing methodological solutions to deal with the balance between different rights and obligations.

After a comprehensive introduction, a section is dedicated to the applied methodologies combining bottom-up and normative approaches. An outline of how to actually deal with all practical ethical legal implications followed. It addressed through tables and checklists the existing barriers to innovation in order to drive the researcher among the fragmented applicable legal framework.

In particular, thanks to the identification of gaps and enablers, concrete scenarios have been developed in order to provide interpretative solutions able to be applied and replicated in similar contexts.

The next iterations will take into account the further advances made on this subject.

BIBLIOGRAPHY

EU legal acts/proposals

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on standard essential patents and amending Regulation (EU)2017/1001 COM/2023/232 final

Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on liability for defective products COM/2022/495 final

Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive) COM/2022/496 final

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 COM/2022/454 final

Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (Text with EEA relevance) PE/85/2021/REV/1

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the European Health Data Space COM/2022/197 final

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

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), https://data.consilium.europa.eu/doc/document/PE-24-2024-INIT/en/pdf

Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (Text with EEA relevance.) OJ L 117, 5.5.2017, p. 1–175.

Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU (Text with EEA relevance.) OJ L 117, 5.5.2017, p. 176–332.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) OJ L 119, 4.5.2016, p. 1-88

Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC Text with EEA relevanceOJ L 158, 27.5.2014, p. 1–76

Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 (Text with EEA relevance) OJ L 218, 13.8.2008, p. 30–47 (CE Marking Regulation)

Council Directive 93/42/EEC of 14 June 1993 concerning medical devices OJ L 169, 12.7.1993, p. 1–43

Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs (Codified version) (Text with EEA relevance) OJ L 111, 05.05.2009, p. 16-22.

Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, OJ L 77, 27.03.1996, p. 20-28.

Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, OJ L 167, 22.06.2001, p. 10-19.

Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (Text with EEA relevance), OJ L 130, 17.05.2019, p. 92-125.

Directive 2006/116/EC of the European Parliament and of the Council of 12 December 2006 on the term of protection of copyright and certain related rights (Codified version), OJ L 372, 27.12.2006, p. 12-18.

Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (Text with EEA relevance), OJ L 157, 15.06.2016, p. 1-18.

Directive 98/71/EC of the European Parliament and of the Council of 13 October 1998 on the legal protection of designs, OJ L 289, 28.10.1998, p. 28-35.

Council Regulation (EC) No 6/2002 of 12 December 2001 on Community designs, OJ L 3, 05.01.2002, p. 1-24.

Italian legislation

National Implementation of the MDR D.lgs 137/2022

And decrees 12 April 2023- publication GU 13 June 2023 n.136 Concerning respectively

- Administrative procedures of national relevance for the submission of communications relating to clinical investigations for devices bearing the CE marking used in the context of their intended use referred to in Article 16(3) of Decree No 137 of 2022.
- B) Administrative procedures of national relevance for the submission of the application for clinical investigation for medical devices not bearing the CE marking referred to in Article 16, paragraph 2 of Legislative Decree No. 137 of 2022. (G.U. General Series, no. 136 of 13/06/2023)

Implementation of clinical trials Italian discipline: 26 27, 30 January 2023 decrees GU serie Generale n.31 07/02/2023

Italian Data Protection Authority (garante per la protezione dei dati personali):

- Provision, 5 June 2019 https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9124634 accessed 03 July 2023
- Deontological rules on processing for scientific research, https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9069637 accessed 03 July 2023
- Rules on the use of consent to re-use data concerning health https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9791886 accessed 03 July 2023.
- "smart toys", https://www.garanteprivacy.it/temi/iot/smarttoys
- Garante Protezione Dati Personali "Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario – 7 marzo 2019 [9091942]" https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9091942 accessed 03 July 2023
- Garante per la Protezione dei Dati Personali "Parere ai sensi dell'art.110 del Codice e dell'art.36 del Regolamento- 30 giugno 2022 [9791886]" https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9791886 accessed 03 July 2023

Policy et al.

Council of Europe and EU Fundamental Rights Agency (FRA), *Handbook on European data protection law* (Luxembourg: 2018), 119-122.

EDPB, " Guidelines 07/2020 on the concepts of controller and processor in the GDPR", https://edpb.europa.eu/our-work-tools/documents/public-consultations/2020/guidelines-072020-concepts-controller-and_en accessed 03 July 2023

EU Commission:

- https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en, accessed 03 July 2023
- https://digital-strategy.ec.europa.eu/en/policies/non-personal-data#:~:text=The%20Regulation%20on%20the%20free,and%20IT%20systems%20in%20Europe. Accessed 11 July 2023.
- https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space_en, accessed 03 July 2023
- https://health.ec.europa.eu/medicinal-products/clinical-trials/clinical-trials-regulation-eu-no-5362014_en accessed 03 July 2023
- https://health.ec.europa.eu/medical-devices-new-regulations/overview_en accessed 03 July 2023 accessed 03 July 2023
- ICO (UK Data Protection Authority) Age Appropriate Design: A code of practice for online services, (2020) https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/introduction-to-the-childrens-code/ accessed 03 July 2023.

Regione Toscana "Antitrust la commissione UE ha adottato una revisione dei regolamenti orizzontali di esenzione per categoria sugli accordi di ricerca e sviluppo" https://www.regione.toscana.it/-/antitrust-la-commissione-ue-ha-adottato-una-revisione-dei-regolamenti-orizzontali-di-esenzione-per-categoria-sugli-accordi-di-ricerca-e-sviluppo-r-s-e-di-specializzazione accessed 03 July 2023

Scuola Sant'Anna, "CHILDREN'S PROTECTION IN RESEARCH ACTIVITIES" approved by the Academic Senate with Decision n.267 of 10/12/2020, https://www.santannapisa.it/en/node/55403, accessed 13 July 2023.

EU Judgments

Judgment of the Court (Third Chamber) of 4 May 2023. *UI v Österreichische Post AG.*, C-300/21, ECLI:EU:C:2023 :370.

Judgment of the Court (First Chamber) of 16 February 2017. *Elisabeth Schmitt v TÜV Rheinland LGA Products GmbH.,* Case C-219/15, ECLI:EU:C:2017:128

International Legal Instruments

Berne Convention for the Protection of Literary and Artistic Works (as Amended on September 28, 1979), World Intellectual Property Organisation.

Paris Convention for the Protection of Industrial Property (as Amended on September 28, 1979), World Intellectual Property Organisation.

Agreement on the Trade-Related Aspects of Intellectual Property Rights as Amended by the 2005 Protocol Amending the TRIPs Agreement, World Trade Organisation.