MISSIONE 4
ISTRUZIONE
RICERCA

BRIEF

BIOROBOTICS

RESEARCH AND

INNOVATION

ENGINEERING FACILITIES

D.7.3 CROSS-FIELD REGULATORY ANALYSIS

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

Quadro riassuntivo rilasci documento

Data	*Stato documento*	*Realizzato da*	*Note*	*Supervisione*
22.5.23	First draft	*Denise Amram*	ToC and structure of the deliverable	*Denise Amram*
19.6.23	Content update	*Francesca Gennari*	Content update	*Denise Amram*
5.7.23	Draft review	*Denise Amram*	Content Review	*Denise Amram*
15.7.2023	Complete version	*Francesca Gennari*	Content finalisation	*Denise Amram*
25.7.2023	Final version	*Francesca Gennari Denise Amram*	Final version after stakeholders' feedback at the awareness panel of 20.7.2023	*Denise Amram*

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 RESIELEINCE 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.

Sommario

ABBREVIATIONS

List of abbreviations
AI: Artificial Intelligence CTR: Clinical Trials Regulation DA: Data Act DGA: Data Governance Act DMA: Digital Markets Act DSA: Digital Services Act EDS: European Data Strategy EHDS: European Health Data Space EU: European Union GDPR: General Data Protection Regulation ICC: Italian Civil Code MDD: Medical Devices Directive MDR: Medical Devices Regulation 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

1. INTRODUCTION

This Deliverable D.7.3. illustrates 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. Its content is 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 will focus 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 nor 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, 8 *Policy Briefs* are released to provide a more user-friendly perspective of the applicable legal framework. A panel has also been organised to better share 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. Further versions will be released in D.7.4 and D.7.5.

[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 includes a first map of 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. Preliminary policy and recommendations are finally proposed in light of the common general principles and legal enablers identified to protect and empower fundamental rights in the given matter.

The report 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 (D.7.4. *et al.*). During the event, the structure and methodologies adopted in WP7 have been considered useful and well placed to achieve the project objectives.

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, and Artificial Intelligence ones as the three 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 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.

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

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.

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 BioRobotics solutions.

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.

The reciprocal initiative respect to the GDPR is the regulation concerning the **Free Flow of Non-Personal Data** (FFNPO). 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.*

[5] Ibid.
[6] Ibid.
[7] Ibid.

- *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.

The **DGA main aim is to set the rules to facilitate data sharing and reuse from the public sector to the private one,** when the Open data directive does not apply. However, this is not the only function of the DGA, as it also strives to create new subjects whose main function will be to act as **data intermediaries to create a functioning and regulated data economy**. Moreover, it also empowers people and citizens to share their data for altruistic reasons such as research.
The **DA** proposal main aim **is to set clear rules concerning how private subjects should access data** that are generally Internet of Things (**IoT**) objects- generated in order **to create new products and services on secondary markets**. Moreover, the DA disciplines rules concerning fairness in data sharing contracts, interoperability, and switching for 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 date in emergency situations such as the case of a future pandemic.
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 (EDHS) proposal includes "*rules, common standards, and practices*"[9] and has two main functions which interest health data, whose regime of processing is described by article 9 GDPR.
The first function concerns **the primary use of data**, which is the one generally made by data subjects/patients. According to the first part of the EHDS new interoperable solutions concerning health data (such as a new version of portable electronic health records) will need to be implemented by Member States. In this way, individuals will be empowered by having access and control over electronic health data and will be also incentivised to move across Europe without the fear of losing their data, or not be able to "carry" their own health data with them should they change country or have a health emergency in another EU country.
The second one concerns **the secondary use of data**: thanks to safe infrastructures, third parties can access to health structured datasets for further reuse, overcoming the barriers related to the lack of data and avoiding the duplication of collecting activities.

[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.
[9] See more at: https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space_en, accessed 03 July 2023.

3.2. Public health

The second main EU framework to keep 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[10] (hereinafter referred to as Medical Devices Regulation, MDR) and the Regulation (EU) 2017/746 on In Vitro Diagnostic Medical Devices[11]. 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)[12] 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)[13] 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 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

[10] 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.

[11] 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.

[12] 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.

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

breast-protheses case[14], 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 BioRobotic, AI, IoT and allied technologies was still at the beginning. The MDR already considers software, at certain conditions, as a medical device[15], 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*
- ***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*

[14] 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

[15] Article 2(1) MDR.

- ***improved coordination mechanisms*** *between EU countries in the fields of vigilance and market surveillance*"[16].

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[17].

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*[18]"

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

Pills of CTR

[16] See more at https://health.ec.europa.eu/medical-devices-new-regulations/overview_en accessed 03 July 2023.
[17] See more at https://health.ec.europa.eu/medical-devices-sector/new-regulations_en accessed 03 July 2023.
[18] See more at https://health.ec.europa.eu/medicinal-products/clinical-trials/clinical-trials-regulation-eu-no-5362014_en accessed 03 July 2023

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 • 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

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.

- **AI Act Proposal**[19] answering the call for legislative action to ensure a well-functioning internal market for artificial intelligence systems where both benefits and risks of AI are adequately addressed at Union level.

- **AI Liability Directive**[20] The purpose of the AI liability directive 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

[19] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0206
[20] 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

their possible exposure to liability and prevent the emergence of fragmented AI-specific adaptations of national civil liability rules.

- Assessment List for Trustworthy Artificial Intelligence (**ALTAI checklist**) developed in 2020 by the then High-Level Expert Group on Artificial Intelligence. It is a list that whoever develops new forms of technology (and, in particular, AI-powered 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, ethnicity, and robustness of a given solution. It is divided in chapters 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.

Considering the timeline of approval of the AI act, in the next versions of this report we will provide more details.

4. CROSS-FIELD ANALYSIS

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

In this paragraph, 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 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	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; • Integrity and confidentiality • Privacy-by-design and by-default
Italian Code of Privacy D. lgs 193/2003 updated with D.lgs. 101/2018 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 study ad 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. Article 110*bis* 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 interested data subject 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) [21]. 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[22] 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. Rules on the use of consent to re-use data concerning health Opinion of 30 June 2022, n. 9791886[23] 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

[21] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9124510 accessed 03 July 2023.
[22] https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9069637 accessed 03 July 2023.
[23] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9791886 accessed 03 July 2023.

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). • 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 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)	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
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	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

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)	• 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.
Proposals of EU legislation	*Main principles that will be applicable to BRIEF RI activities*
AI act proposal (general regulation for Artificial Intelligence, COM/2021/206 final), AI act	AI Act will be the most general (horizontal in EU parlance) regulation on AI, including: • AI systems definition as software (primarily); • Division in high-risk and low-risk AI systems and -possibly- in general/all-purpose AI that is used for high risk or in combination with high-risk application such as AI for health; • Compliance requirements for high-risk AI systems, including obligations to train the data fairly in a non-biased way; • ALTAI Checklist.
Data Act (rules on access and re-use of personal and non-personal data from IoT, COM/2022/68 final), DA	The DA will be the most general (horizontal in EU parlance) regulation on IoT devices. 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.
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	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.

with digital elements, COM/2022/454 final)	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 the so-called low-risk AI applications, as it refers to damages caused also by mobile objects integrated with digital elements. This means that it might apply to several of the new-generation BioRobotic devices including the ones designed within the BRIEF project which are not considered high risk (and liability issues pertaining to high-risk AI systems will be dealt with by the proposal described *infra*). It is necessary to point out the connections with the MDR of the present product liability regime and its future implementation. The MDR is directly linked to the actual product liability directive and it is possible that even the new regime will be connected to it also in the foreseeable future. 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.
Directive on machinery update (which will be converted in an updated regulation, COM/2021/202 final), MR	It will apply to the BRIEF-funded devices as some of them could be considered as high-risk machinery devices according to the present directive which will be later updated and transformed into a regulation.
Intellectual property issues SEPs	At the moment the newest field of interest concerning IP on which the EU Commission is working concerns Standard Essential Patents (SEPs). SEPs are patents that are so important to get included in technological standards. They were largely unregulated as basically only international Standard Setting/Developing Organizations (SSOs/SDOs) had the possibility to create these standards. The EU Commission recently presented a proposal of Regulation for SEPS last 23 April 2023[24] . Given its importance, this topic it will be better presented in the iteration of the deliverable.

Table 1: First part of the cross-field analysis

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.

[24] See more at: https://single-market-economy.ec.europa.eu/publications/com2023232-proposal-regulation-standard-essential-patents_en.

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[25].
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.
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

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

	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[26] 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 2: second part cross-field analysis

[26] 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. 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.

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 3: 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 proposals like the AI Act and Data Act ones, we may immediately remark an interpretive issue arising from the related fields of application.

In the AI act proposal, thus, it is still not clear how the main division between high and low risk AI systems will turn out to be applied in practice. Similarly, the Data Act proposal 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 length of time by which these proposals will not only get officially approved from the European Parliament and the Council of the EU but also they will be effectively implemented: we can take as a wake-up call the implementation of the CTR. It was officially approved in 2014 but we are in 2023 and yet the CTR is not yet fully operational. This could be potentially the near future concerning this first group of proposals (meaning the AI Act, the DA, 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[27] 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*

[27] 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.

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 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).

Table 4: Legislative acts gaps and interpretative barriers

Proposal	*Gaps*
AI Act (AIA) proposal	Some forms of AI are forbidden, such as the ones that overtly or subconsciously discriminate against a person or certain groups. Among the forms of AI systems that are admissible there is a main division between high-risk and low-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 will be many compliance obligations as far as the design and the implementation of the AI system itself, based on self-perception and whose sectorial and national implementations could represent a barrier for innovation.
Data Act (DA) proposal	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 proposal 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.
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) proposal	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)[28].
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

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

	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 5: 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. 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	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	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.

	and data protection authorities. Data Protection Officer to drive compliance activities.	controllers, as well as between research and Research & Development & 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 subjects through data cooperatives pursuing mutualistic scope.	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.
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 *robustness* pillar under AI Act.	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 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	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.

	objects with digital elements		
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 (proposal)	All of the above principles plus a general principle of protection of fundamental rights	The division between high and low risk AI system will almost always depend also on the concrete features of the software and its functions.	Guidelines are already available to perform the ethical legal assessment.

Table 6: 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)

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[29].

[29] Source cited in Table 1.

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 [30], 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).
- 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[31] also introduced the concept of "*consenso a fasi progressive*" (progressive consent) concerning health data. This means that whenever consent is the legal

[30] 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.

[31] 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

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 third 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 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[32]. Once the platform has been developed and used to create research results data, then, the new dataset could:

[32] 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

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 on algorithms training the platform

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 final approval and enactment 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.

Once developed issues addressed by design, which steps to put it in 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 future 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.

5.2. Scenario B)

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***[33]" (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:

- 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

[33] Emphasis added.

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*"[34]. 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[35]. 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 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

[34] 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.
[35] One can take inspiration from the one drafted by Scuola Superiore Sant'Anna.

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.

III) 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.

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[36], 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[37].

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[38]. 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.

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

[36] 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.
[37] 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.
[38] Council of Europe and EU Fundamental Rights Agency (FRA), *Handbook on European data protection law* (Luxembourg: 2018), 119-122.

read at article 5(1)(a) GDPR[39]. 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*"[40]. 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.
Accountability	To define roles and responsibilities in the clinical protocol and	Roles and responsibilities shall be allocated considering the concrete activities and life-cycle of the research more than possible formal constrains.

[39] 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.
[40] Ibid.

Transparency	for the data governance purposes	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 7: Principles

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 BioRobotics 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.	Take into account possible initiatives entering into force in the near future/during the research life-cycle.

b. Possible specific safeguards implemented at national, or local level for a given sector.	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. If you are dealing with the digital 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,	Keep in mind the principle of minimisation and what you have declared in the privacy information / information sheet.

pictures and reports publications, newsletters, surveys etc	

Table 8: Preliminary policy suggestions 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.

Table 9: Preliminary policy suggestions part II

9. 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

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on harmonised rules on fair access to and use of data (Data Act)COM/2022/68 final

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS COM/2021/206 final

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

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):

- proviso 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