MISSIONE 4
ISTRUZIONE
RICERCA

BRIEF BIOROBOTICS RESEARCH AND INNOVATION ENGINEERING FACILITIES

D.7.5 FINAL CROSS-FIELD REGULATORY ANALYSIS

Finanziato dall'Unione europea
NextGenerationEU

Ministero dell'Università e della Ricerca

Italiadomani
PIANO NAZIONALE DI RIPRESA E RESILIENZA

Quadro riassuntivo rilascio documento

Data	*Stato documento*	*Realizzato da*	*Note*	*Supervisione*
25.02.2025	Draft	*Arianna Rossi*	Table of Contents	*G. Comandé*
15.07.2025	Draft	*Arianna Rossi, Francesca Gennari*	Individual contributions added, merged and corrected	*G. Comandé*
05.08.2025	Draft	*Arianna Rossi*	Integration, summary and harmonization	*G. Comandé*
07.08.2025	Draft	*Arianna Rossi*	Language revision	*G. Comandé*
27.08.2025	Draft	*Arianna Rossi, Francesca Gennari*	Integration of missing parts	*G. Comandé*
15.09.2025	Draft	*Giovanni Comandé*	Revision	*G. Comandé*
29.09.2025	Final draft	*Arianna Rossi*	Final draft addressing comments of reviewers	*G. Comandé*
30.09.2025	Final version	*Arianna Rossi*	Submission	*G. Comandé*

DISCLAIMER

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

ACKNOWLEDGEMENTS

This report is the outcome of collaborative work. The main authors are Francesca Gennari, Arianna Rossi, Prof. Denise Amram and Prof. Giovanni Comandé. However, other researchers of the Law and Policy Hub have contributed significantly with their insights and expertise to the drafting of this deliverable, namely in alphabetical order: Andrea Blatti, Irina Carnat, Federica Casarosa, Chiara d'Elia, Andrea Parziale, Pelin Turan. We also thank the members of the LaPoH's Advisory Board, namely Irene Aprile, Annalisa Calabrò, Simona Crea, Sabrina Grigolo, Gianclaudio Malgieri and Maria Cristina Mauro, for their valuable comments on the draft version of this report.

TABLE OF CONTENTS

ABBREVIATIONS

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

1. INTRODUCTION

This Deliverable builds on the first two cross-field regulatory analyses D7.3 and D7.4 to illustrate the applicable legal framework impacting BRIEF's activities. This iterative work provides a unitary mapping of regulations at the European and national level, including the most recent ones, and identifies key enablers and gaps for BRIEF's R&D activities, which are paramount to design useful policies and recommendations for stakeholders and researchers. Contents are developed considering the results of the survey described in "D.7.2. Stakeholders engagement" as well as the evolution of the applicable legal framework that emerges from the multitude of legislative initiatives on data and emerging technologies launched by the EU.

The report focuses on the mapping of the existing laws that are comprised in the ethical legal framework for the BRIEF ecosystem and its scientific community. In addition, it pays tailored attention to current legislative initiatives (not yet approved or entered into force) and their interpretative impact on the Research & Development & Innovation sectors (hereinafter referred to as R&D&I). EU Directives and EU Regulations shall be implemented or adapted to the existing sectoral national regulatory framework with different degrees of effectiveness in the Member States (hereinafter MS). Once applicable, EU Regulations are directly effective in MS, but some provisions may find national implementations and interpretations, while EU Directives provide principles that need to be mandatorily implemented in the national law of each MS. In addition to these norms, the EU has identified new principles and obligations that may directly impact national (and even local) compliance procedures, even if the regulation has not yet entered into force. In fact, in case of normative gaps, the interpretations provided in the work-in-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 research and innovation and finds new content thanks to sectoral interpretations.

Therefore, a cross-field analysis of the existing normative constraints allows for the identification of interpretative gaps and enablers in tailored and concrete scenarios. The results are necessary for developing practical policies and recommendations to address common interpretative issues related to biorobotic activities. These have been gathered in "D7.6. Policy design and advice", in academic publications and policy briefs addressed to the Commission, as described in "D7.7. Research dissemination and awareness". Together with the publication of the three iterative versions of this report (i.e., D7.3, D7.4, D7.5), further 24 Policy Briefs were released to provide a more user-friendly perspective of the applicable legal framework. Awareness panels have also been organised to disseminate the newly produced knowledge, equip BRIEF's researchers with a fundamental understanding of the key regulatory aspects relevant to their work, and gather feedback from the BRIEF's community of stakeholders.

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's research activities and its stakeholders. The history of the document is as follows: D7.3 was released in

[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.

July 2023 and is written in black; D7.4 was released in May 2024 and its new sections are in purple; D7.5 was released in September 2025 and its new sections and edits are in green. The paragraphs that have become obsolete at the time of writing the final version of this deliverable have been included in the appendix.

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 essential to precisely identify the legal requirements and how to address those that are about to be implemented, considering the evolution of the relevant framework impacting the R&D&I sectors. It was therefore important to draw up a first map of the theoretically relevant legal acts and then carry out a survey (see 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 what extent;
- The EU legislative initiatives that are not yet in force may already perform as a useful interpretative parameter of the public health and data strategies.

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

The aim of this deliverable is to finally delve into the fields of analysis selected under D.7.2., in order to build up a more clear and understandable state of the art of ethical legal framework applicable to the BRIEF ecosystem, aiming to design cutting edge BioRobotic devices, solutions, and allied technologies.
As anticipated, considering this cross-field analysis as a preliminary one, the current workflow arises from the combination of current compliance requirements, developed legal standards, and regulatory insights.

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

D7.4 illustrated the newly approved text on European regulation on artificial intelligence (AI Act) that had not come into force yet, even though it had already become an essential frame of reference for AI deployers and developers. In addition, the report introduced relevant issues emerging within the Intellectual Property Rights domain, as well as some specific issues concerning the Medical Device Regulation. The content of D7.4 was presented to the consortium's members on 20th May 2024 workshop, titled "Biorobotic and allied technologies: the legal framework. Operational scenarios II" as well. It allowed the audience to address the

ethical legal issues emerging from the cross-field regulatory initiatives like the Intellectual Property Rights, Artificial Intelligence, and Medical Devices legislations.

During both events, the structure and methodologies adopted in WP7 have been considered valid and well placed to achieve the project objectives. The received feedback has been incorporated into the final draft of the report. Finally, the final version of the report includes relevant legislative updates, such as the European Health Data Space Regulation, which was approved in 2025. It also accounts for soft law instruments that have been issued recently, such as the European Data Protection Board's guidelines on pseudonymization, as well as the AI Office's Guidelines on the definition of AI system, among the others. The report has been reviewed by the members of the Advisory Board of the LaPoH before final publication. A selection of final results has been presented publicly in 4 awareness webinars titled "Seminari Law&Tech" organized in September 2025 (see the dissemination activities described in D7.7). In particular, the scenarios have been enriched with additional or updated case studies and some issues have been further explored in light of the new knowledge and interpretations produced throughout the work of WP7.

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 legislative initiatives is developed following the current European Commission Strategy on Data, Health Law, Product Safety and Liability, Artificial Intelligence (AI), Intellectual Property (IP), and Cybersecurity, which are the main fields in which the development of BioRobotic solutions may be framed.

In particular, data-driven research activities are daily dealing both with personal and non-personal data governance, facing also the challenges of openness, to provide replicable and reproducible studies, that may also include human volunteers. To this end, the interplay between public health interventions and the data strategy shall be addressed both to preserve individual rights of engaged volunteers in the given case, and the category of vulnerable groups.
In addition, data flows are functional to the development of innovative methodologies of data analysis, also based on algorithms, Machine Learning (ML) and other AI-based techniques. Thus, to address the values and the assessments already identified in the 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. Finally, many of these activities are bound to strict cybersecurity requirements.

The IP framework is also of pivotal importance both for the BRIEF activities and the BioRobotic field. Indeed, the IP framework informs and governs the various phases of R&D&I activities in the field, including those necessitate accessing information and technology on the state of the art in the field, conducting research activities by employing text and data mining (TDM) methods, training AI models with large datasets of various types of data, 3D-printing of robotic parts and the like. These examples are far from being exhaustive and can be easily multiplied – yet they are sufficient to justify the crucial role that IP plays in scientific research. In this regard, the interplay of IP law with the BRIEF activities and the biorobotic fields is two-folded. On the one hand, the earlier stages of the R&D&I lifecycle require defining the state of the art, hence having access to, analysis, and use of the existing knowledge and technology in order to identify the current trends and gaps as well as to develop novel solutions to the unresolved problems in the field. Successful operationalisation of this endeavour, however, requires the analysis of and building on the existing scientific content, often, protected by conventional forms of intellectual property rights (IPRs), such as copyright, patent, trade secrets, and industrial design.

On the other hand, the latter stages of such R&D&I activities are expected to result in scientific output eligible for IPRs-protection, such as scientific publications and inventions of the researchers and research organisations (ROs) included within the BRIEF network. Therefore, it is essential to lay a solid groundwork for the BRIEF consortium and activities to help clarify the ways in which the BRIEF network can tackle third-party IPRs in the context of scientific research and exploit the prospective scientific output of such research endeavours by utilising their prospective IPRs. In terms of policy making, the following analysis will be functional to

highlight how a RI could exploit the research data generated, fostering the openness principle and contributing to the common data spaces, including in the medical domain the opportunities that the European Health Data Space proposal is launching for the researchers.

3.1. The European Data Strategy

The European Data Strategy is the policy and legal framework that sets the principles and objectives to which the different EU legislative initiatives that we are analysing refer. Its main goal is to "*make the EU leader in a data-driven society*"[2]. More specifically, this means to create a single market for data. The advantage of this operation is that to have clear rules on how to use data will also allow it to freely flow within the EU[3]. This will enable public and private stakeholders, as well as EU citizens to re-use data both personal and non-personal (and by respecting at the same time Intellectual Property Rights) and across economic sectors.
The data-sharing and data-reuse will favour the creation of new products and services, especially on secondary markets and will benefit society, thus including businesses, research institutions, and public administrations[4]. Furthermore, comparing, and contrasting data and metadata extracted by documents is also of capital importance for better policy making and to allow an upgrade in public services.

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

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

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

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

3.1.1. The General Data Protection Regulation

Although the General Data Protection Regulation (Regulation 2016/679)[8] is not formally part of the current European Data Strategy, it is the initiative that influenced the creation of all the subsequent acts and proposals concerning the development of the Digital Single Market. **The GDPR sets out the rules to protect personal data**, while it also strives to outline the rules through which personal data can **be safely used and shared across and beyond the EU** for several purposes, including scientific research, archival purposes, and statistical reasons. Inheriting its scope from the Directive 95/46/CE,[9] the GDPR governs the use of personal data, namely **any kind of data that makes a person** (*i.e.* the data subject) **identified or identifiable**. Personal data might also reveal characteristics of individuals that are particularly sensitive, for example because they expose their belonging to a vulnerable group. This is the case of, for example, health-related data and biometric data that are expressly considered as "belonging to particular categories of data". In such cases, a more restrictive regime applies for their lawful processing: data processing is generally prohibited unless specific legal grounds identified in article 9 apply, such as the explicit consent of the data subject, public health interest, and archiving, research, or statistical purposes in the public interest, among others. In such cases, appropriate safeguards that protect fundamental rights and interests of data subjects must be put in place.

The GDPR's principles can be traced back to those that were first established by the Council of Europe[10] in 1980 and similarly formulated by the OECD[11] shortly afterwards. These principles were also included in the first EU-wide legislation on personal data protection, i.e., the Directive 95/46/CE. Recurring to principles provides for flexibility and universality and they can be translated into specific rules in different jurisdictions. For example, the principle of free flow of information in the internal market needed hardened rules that are similarly applicable across the Member States of the EU. This is why, the Directive was replaced by a Regulation that details such a principle in its provisions (de Hert, 2017) and thereby offers harmonization at the EU level. The GDPR lists its overarching principles in Article 5:

- **Transparency**: processing data in a transparent manner means that individuals are informed about how their data are used and for which purpose so that, when they see it necessary, they can exercise their rights concerning their data.
- **Lawfulness**: any data processing activity must be justified with a valid legal basis; without it, the processing is unlawful.

---

[8] European Parliament and Council of European Union, 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) (Published: OJ L 119, 452016, p 1–88 2016).

[9] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Published: OJ L 281, 23.11.1995, p. 31–50).

[10] Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS No. 108) (1980).

[11] OECD. (1980). OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. https://www.oecd.org/en/publications/oecd-guidelines-on-the-protection-of-privacy-and-transborder-flows-of-personal-data_9789264196391-en.html

- **Fairness**: personal information must not processed in an "unjustifiably detrimental, unlawfully discriminatory, unexpected or misleading" manner[12].
- **Purpose limitation**: the use of data is tied to processing purposes that must be specific, explicit and legitimate. Data cannot be further processed in a way that is incompatible with the initial purpose for which they were collected.
- **Data minimization:** only data that are adequate, relevant and limited to what is necessary to achieve the purpose can be collected and processed, during their whole lifecycle.
- **Storage limitation:** data can be stored in a way that identifies the individual only as long as they serve the purpose. Then they must be disposed of or anonymized.
- **Accuracy:** personal data must be accurate and up to date
- **Integrity and confidentiality**: data should be protected from unauthorized or unlawful processing and from accidental loss, destruction or damage
- **Accountability**: The data controller is invested with the responsibility of respecting these principles and of demonstrating compliance with them.

3.1.1.1. Pseudonymization

Among the various technical measures that can enhance the privacy of data and contribute to responsible data governance, the GDPR explicitly mentions pseudonymization, defined as "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person" (Art. 4(5)). Pseudonymization refers to a **set of data processing techniques aimed at removing or replacing specific identifiers within personal data**, thereby contributing to the principle of data minimization and enhancing the overall security and confidentiality of the data because it reduces the severity of risk in case of unauthorized access or disclosure[13]. Whereas anonymization involves the irreversible transformation of personal data in such a way that individuals can no longer be identified (directly or indirectly), pseudonymized data falls within the scope of the GDPR as it is still considered personal data and must thus be subject to appropriate safeguards.

Pseudonymization refers to a process whereby **identifiable elements within a dataset are replaced with artificial identifiers or pseudonyms**. This technique reduces the direct identifiability of data subjects while preserving the analytical utility of the data. Thus, it is particularly valuable in contexts such as medical research, where data utility must be retained while minimizing privacy risks. Additional information refers to the information that can be

[12] European Data Protection Board. (2019). *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*. https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf

[13] European Data Protection Board. (2025, January 16). *Guidelines 01/2025 on Pseudonymisation*.

used to attribute pseudonymized data to individuals, such as a mapping table where individuals' identities and pseudonyms are stored. This is particularly useful in those cases where data subjects should be re-identifiable, such as when they should be able to exercise their rights.[14] Importantly, the additional information that enables re-identification may exist beyond the immediate control of the data controller; thus, the effectiveness of pseudonymization must consider which information can reasonably be expected to be available and could be used for the re-attribution of data[15] (European Data Protection Board, 2025). When pseudonymized data are transmitted to third parties, the data controller must evaluate whether it should also transmit the pseudonyms or if these can be omitted, owing to the principle of data minimization. Pseudonyms should be shared, for example, when the third party needs to collate data records about the same individual but received at different times, or when it needs to return the results of a certain processing operation (e.g., when certain processing activities are outsourced to a different entity).

The process of pseudonymization involves transforming the data, specifically replacing identifiers with pseudonyms while **retaining information that can enable re-identification**, which can be referred to as the pseudonymization secret because it must be protected with technical and organizational measures. The process can be implemented through various techniques, which must be selected based on the estimated risk to the rights and freedoms of data subjects. Moreover, in line with data protection by design and by default, the effectiveness of the adopted techniques must be carefully determined, which means evaluating how difficult it is to attribute the pseudonymized data to individuals in the specific settings where it is used.[16] For the sake of simplicity, the European Data Protection Board[17] identifies two classes of techniques.[18] The first class consists of creating matching tables that associate identifiers with their pseudonyms, which are randomly generated unique identifiers. The second class consists of applying cryptographic algorithms, either as encryption algorithms or as one-way functions. The pseudonymization secret that will need to be adequately protected will be, in the first case, the matching tables, while in the second case, the secret key.

---

[14] In research settings where it is impossible to effectively anonymize data and contacting individuals would constitute a disproportionate effort, for example, these may need to be re-identifiable so that they can, at least, opt-out of research participation, see our previous work in Rossi, A., Arenas, M. P., Kocyigit, E., & Hani, M. (2022). Challenges of protecting confidentiality in social media data and their ethical import. *2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 554–561. https://doi.org/10.1109/EuroSPW55150.2022.00066

[15] EDPB (2025)

[16] The contextual nature of identifiability and personal data has been clarified in a recent ruling of the CJEU (Case C-413/23 EDPS vs SRB): whether data are personal depends on the reasonable means available to the recipient to re-identify individuals. Pseudonymized data are not automatically personal data for all parties, but this evaluation depends on contextual matters.

[17] EPDB (2025)

[18] For a more detailed overview of pseudonymization techniques, see Jensen, Meiko, Lauradoux, Cedric, & Limniotis, Konstantinos. (2019). *Pseudonymisation techniques and best practices. Recommendations on shaping technology according to data protection and privacy provisions*. European Union Agency for Cybersecurity (ENISA). https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices

Achieving effective pseudonymization is of utmost importance in the context of **reusing health data within the conditions set by the European Health Data Space Regulation** (see Section 3.1.6). In the view of achieving data minimization, the EHDS indeed prescribes that health data access bodies provide data users with access to pseudonymized data only when the latter have demonstrated that they cannot achieve their processing purpose with anonymized data. In such cases, though, the secret information that is necessary to reverse the process of pseudonymization must be available only to the health data access body or to a trusted third party (which could be, for instance, a data intermediation entity that offers services that enhance data confidentiality).[19]

3.1.1.2. The Italian Privacy Code's rules on research and health data (re)use

Within articles 100, 110 and 110*bis,* the Italian Privacy Code[20] sets the rules to process personal data in medical, biomedical and epidemiological research settings and further data-sharing for these activities. Article 100 states that public entities such as universities can communicate and share data concerning studies and research activities even to private parties and through electronic means. Articles 110 and 110*bis* respectively concern the medical, biomedical and epidemiologic research and the reuse of data for scientific research or for statistical purposes.

Article 110 of the Italian Privacy Code establishes **conditions under which health data may be processed for scientific research without the data subject's consent**. This reflects the principle that data protection must be balanced with other fundamental rights, such as the right to health, which can be signifciantly advanced through scientific research. In line with Article 9(2)(j) GDPR, consent is not required when processing is based on national or EU law and is necessary for scientific research, provided that it is proportionate, respects the essence of data protection, and includes appropriate safeguards. In such cases, a Data Protection Impact Assessment (DPIA) must be conducted and published. The article also addresses situations where obtaining consent is impractical—such as when informing data subjects is impossible or would compromise the research. In these cases, the data controller must implement safeguards, obtain ethical approval, and, until 2024, consult the Italian Data Protection Authority (Garante). Following a 2024 amendment,[21] this consultation is no longer required; instead, the Garante is responsible for defining the necessary safeguards, thereby streamlining research procedures while maintaining data protection standards.

[19] For an example of how this could work, see scenario described at (European Data Protection Board, 2025, pp. 37–39)

[20] DECRETO LEGISLATIVO 30 giugno 2003, n. 196 Codice in materia di protezione dei dati personali ((, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonchè alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE)).

[21] LEGGE 29 aprile 2024, n. 56. Conversione in legge, con modificazioni, del decreto-legge 2 marzo 2024, n. 19, recante ulteriori disposizioni urgenti per l'attuazione del Piano nazionale di ripresa e resilienza (PNRR).

Moreover, the Data Protection Authority is in charge of issuing **deontological rules**[22] that complement these provisions when processing personal data for medical, biomedical and epidemiologic research. This must be done in compliance with the Helsinki Convention and data subjects must express their willingness to be informed about possible health-related issues that they might not have been aware of. Moreover, universities and research institutes conducting medical research must ensure adherence to these deontological rules. These require that individuals be clearly informed about the specific purposes of scientific research involving their data, including any further use for statistical or scientific aims and potential data recipients. If direct notification is impractical, public disclosure through appropriate media is mandated. Further, special categories of data, such as health data, should generally be anonymized unless written consent is obtained. However, consent is not always necessary if adequate safeguards are in place for medical or scientific research.

By decision n. 298 issued on 9.5.2024, the Italian Data Protection Authority adopted new safeguards that updated the deontological rules,[23] according to which data controllers shall:

a. Obtain positive opinion from the competent ethical committee.
b. Motivate and document the presence of ethical or organisational reasons (explained below) according to which 1) data subjects are not contactable anymore; 2) trying to obtain data subjects' consent would lead to a disproportionate effort (in this case data controllers shall document the reasonable efforts made); 3) trying to obtain data subjects' consent would constitute a significant prejudice for the objectives of the research.
c. If these conditions are met, data controllers shall conduct a data protection impact assessment.

Ethical reasons that make it impossible to obtain data subjects' consent occur when the needed information would inform data subjects about research results that may cause material or psychological harm. Organisational reasons occur when the impossibility of processing data related to non-contactable data subjects would lead to significant problems for the quality of the research. To determine the quality diminution resulting from the inability to process certain data, data controllers must consider the inclusion criteria of the research, the recruitment procedures, the statistical significance of the sample, and the time elapsed since the personal data were obtained.

Article 110*bis* of the Italian Privacy Code, instead, states that **the national Data Protection Authorities can authorise the reuse for scientific or statistical research when**: I) it is not possible to inform the data subject (the Italian Data Protection Authority requires the research institutions to try to reach the patients at least three times) or II) the delay risks to bring prejudice

[22] Garante per la Protezione dei Dati Personali, "Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica pubblicate ai sensi dell'art. 20, comma 4, del d.lgs. 10 agosto 2018, n. 101 - 19 dicembre 2018 [9069637]." Dec. 19, 2018.
[23] Garante per la Protezione dei Dati Personali, "Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica ai sensi degli artt. 2-quater e 106 del Codice - 9 maggio 2024 [10016146]." maggio 2024. Accessed: Jul. 14, 2025. [Online]. Available: https://www.garanteprivacy.it:443/home/docweb/-/docweb-display/docweb/10016146

to the outcome of the research. It adopts its decision within 45 days. However, appropriate measures must be implemented to safeguard the rights and freedoms of the individuals concerned, including the application of data minimization and anonymization techniques. A favorable decision by the Garante outlines the specific conditions and protective measures to be adopted in this regard. Alternatively, the Garante may issue general provisions that are applicable to specific categories of data controllers or types of processing activities.

Data protection authority provision on 5.6.2019[24] concerns the **secondary use of specific categories of data that were originally collected for medical treatment purposes,** for different research projects or derived from previously obtained biological samples. They also apply to studies involving individuals whose health condition is so severe that they are unable to comprehend the information provided or to give informed consent. This document details what can be deduced from Articles 5 and 89 of the GDPR. It allows derogations for scientific research from collecting 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 ameliorate data subjects' health). 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.

Lastly, it is worth mentioning Opinion of 30 June 2022 on **broad consent**,[25] where the Italian Data Protection Authority (Garante) addressed the issue of *consenso a fasi progressive* in response to a university hospital's plan to reuse health data for future research. The Garante clarified that broad consent is only acceptable when specific research purposes cannot be identified, especially given the sensitivity of health data. It stressed that referencing general research areas is insufficient for valid consent; instead, clearly defined research projects are required, aligned with ethical and methodological standards. Since ethical approval is only sought once a study's purpose is specific, initial broad consent must later be supplemented with more detailed consent, as data subjects initially lack the information needed for informed consent.

The EHDS modify the legal framework on the use and reuse of health data for research and other general interest purposes (see sec. 3.1.6). The Italian Law 132/2025 has also introduced new provisions that are meant to simplify the reuse of health data for the development and training of AI systems (see Sec. 3.4.1.9).

[24] Garante per la Protezione dei Dati Personali, "Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 del d.lgs. 10 agosto 2018, n. 101 [9124510]." 2019.
[25] Garante per la Protezione dei Dati Personali, "Parere ai sensi del ai sensi dell'art. 110 del Codice e dell'art. 36 del Regolamento - 30 giugno 2022 [9791886]." giugno 2022. Accessed: Jul. 14, 2025. [Online]. Available: https://www.garanteprivacy.it:443/home/docweb/-/docweb-display/docweb/9791886

3.1.2. The Free Flow of Non-Personal Data Regulation

Whereas the GDPR applies to personal data and sets the rules and conditions for their free movement, non-personal data are governed by the Regulation on a framework for the free flow of non-personal data in the European Union[26] (FFNP) (Regulation 2018/1807). The Regulation establishes the following key provisions:

- **Unrestricted movement of non-personal data within the EU**: Organisations may store and process data in any Member State without limitations. Data localization requirements should be prohibited unless they are justified due to reasons of public security (Article 4).
- **Competent authorities' access to data**: Public authorities retain the right to access data, regardless of its location within the EU or whether it is stored in cloud environments (Article 5).
- **Improved portability between cloud service providers**: The Commission is promoting self-regulation by encouraging providers to adopt codes of conduct that facilitate data portability to another cloud provider or to one's own IT systems based on interoperability, transparency and open standards (Article 6).

3.1.3. The Open Data Directive

The Open Data Directive[27] (hereinafter: ODD) is a key legislative initiative that requires public sector data to be made available in **free and open formats**, intending to strengthen the EU data economy. It plays a crucial role in European **policies concerning open science**, particularly in its focus on the re-use of research data. The ODD intends to promote fair competition, facilitate access to public information, and support cross-border innovation.

Its core principle is that public sector data should be **open by design and by default** (Article 5). Key provisions include:

- Publication of non-personal data in open, machine-readable formats and according to open standards (Article 5)
- Real-time data access and availability via APIs, where feasible (Article 5)
- Charging rules that establish free re-use as the norm (Article 6)
- Re-use of data from publicly funded research (Article 10)
- Re-use is open to all actors in the market (Article 12)
- Restrictions on exclusive agreements to prevent data lock-in (Article 12)
- Identification of the categories of High Value Datasets (HVDs) such as geospatial, meteorological and mobility data (Articles 13-14 and Annex I)

[26] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union PE/53/2018/REV/1 OJ L 303, 28.11.2018, pp. 59–68.

[27] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (recast) PE/28/2019/REV/1, OJ L 172, 26.6.2019, pp. 56–83

Public data designates documents generated and gathered by public sector bodies, but the ODD expands this traditional definition also to include research data[28]. It excludes, however, documents whose intellectual property is held by third parties, as well as personal data (Articles 1(2)(c) and i(2)(h)) – these are in the scope of the Data Governance Act (see Section 3.1.4 below).

In 2022, the Commission adopted an implementing act[29] that exactly identifies the High Value Datasets mentioned above. These datasets are particularly valuable because they can bring about economic, environmental, and social benefits. They can be reused, thereby helping generate innovative services and AI-powered innovation, and can strengthen and enhance the activities of public authorities. High-value datasets must comply with several requirements, including the use of open data licences, the provision of public documentation, and ensuring machine readability. Additionally, where applicable, these datasets must be available for bulk download and accessible via Application Programming Interfaces (APIs), free of charge. Comprehensive metadata documentation is also required to support usability and integration.[30]

3.1.3.1. Focus on open research data

The obligations on the availability and reuse of research data are particularly relevant for the BRIEF project. Article 10 mandates that Member States develop **national open access policies** and actions to support the availability of data coming from publicly funded research. Such policies should be in line with the FAIR principles:[31] data should be findable, accessible, interoperable and reusable. They should be open by default whenever possible, but follow the foundational principles "**as open as possible, as closed as necessary**" whenever there are relevant considerations of intellectual property, personal data protection, security, and legitimate commercial interests.

There are a few significant aspects that must be highlighted in terms of the scope of application of the ODD. First, the obligations concerning re-use rules do not apply to educational materials produced by universities, nor to administrative data concerning their operational activities. Second, and most importantly, they apply only to data that was generated thanks to public funding and that has already been made publicly available on data repositories. This is meant to alleviate the burden on organizations and individual researchers who would otherwise need to reply to data access requests. Third, many elements of the open access obligations need to be defined by Member States in their national policies, such as their scope, the possibility of embargo, the opt-out options, etc. The policies should also more specifically define what is

[28] The ODD provides one of the few legislative definitions of research data in the EU at article 2(9): "'research data' means documents in a digital form, other than scientific publications, which are collected or produced in the course of scientific research activities and are used as evidence in the research process, or are commonly accepted in the research community as necessary to validate research findings and results"

[29] COMMISSION IMPLEMENTING REGULATION (EU) /... laying down a list of specific high-value datasets and the arrangements for their publication and re-use. C/2022/9562 final

[30] Mancino D, 'High-Value Datasets – an Overview through Visualisation' (data.europa.eu, 2022) <https://data.europa.eu/en/publications/datastories/high-value-datasets-overview-through-visualisation> accessed 8 August 2025

[31] https://www.go-fair.org/fair-principles/

meant by data that is made publicly available on data repositories, for example, in terms of establishing the required level of openness of such repositories to fall under the obligation.[32]

Italy has taken its first steps towards this goal. The **Piano Nazionale per la Scienza Aperta** (PNSA)[33] represents the most significant institutional contribution by the Italian State to the topic of Open Science to date.[34] Through Ministerial Decree No. 268/2022[35] issued by the Ministry of Universities and Research (MUR), the PNSA acquired the status of a ministerial-level regulatory act. The PNSA constitutes the implementation of the National Research Programme (PNR) 2021–2027, approved by CIPE Resolution No. 74/2020.[36] Among the actions to be undertaken by the Ministry of Universities and Research (MUR), the PNSA identifies the implementation of Article 10 of the ODD.

The adoption of the PNSA was followed by the establishment of the Working Group for its implementation via Director's Decree No. 42 of 14 March 2023, and further supplemented by Ministerial Decree No. 120 of 11 July 2023. In 2024, the WG produced an assessment of the current state of Open Science in Italy.[37] This assessment serves as a concrete starting point for addressing the complexity and sustainability of implementing the PNSA, enabling the use of existing resources and identifying gaps that need to be filled.

3.1.4. The Data Governance Act

The Data Governance Act[38] **(DGA) sets the rules to facilitate and safeguard data sharing and reuse across sectors and Member States.** It implements the foundational statement of the 2020's European Strategy for Data's motivation: '[t]he value of data lies in its use and re-use' (European Commission, 2020, p. 1). The DGA complements the Open Data Directive (see above) since it applies to data that are held by public sector bodies and that deserve protection, for example, because they are personal data, they are protected by intellectual property rights, or carry commercial or statistical confidentiality. Whenever public entities make personal data available for re-use, they will also need to be equipped with privacy-friendly and security-enhancing tools, as well as mechanisms that ensure the anonymity and confidentiality of the data they share. Sector-specific competent authorities are entitled to support the public sector

[32] van Eechoud M, 'Study on the Open Data Directive, Data Governance and Data Act and Their Possible Impact on Research.' (European Commission Directorate General for Research and Innovation 2022) <https://data.europa.eu/doi/10.2777/71619> accessed 11 April 2025

[33] Rossi G and others, 'Piano Nazionale per la Scienza Aperta' (Ministero dell'Università e della Ricerca 2022)

[34] Gatt L and Izzo L, 'L'Open Science Fra Hard Law e Soft Law: Guida Alle Normative in Tema Di Scienza Aperta' (22 May 2024) <https://open-science.it/article?rpk=302464&prs_sel=p_researcher&tpc_sel=t_policies> accessed 13 May 2025

[35] https://www.mur.gov.it/sites/default/files/2022-06/Decreto%20Ministeriale%20n.%20268%20del%2028-02-2022.pdf

[36] https://ricerca-delibere.programmazioneeconomica.gov.it/media/docs/2020/E200074.pdf

[37] Castelli D and others, 'Processi per Individuare Le Attività Già in Essere Nel Paese Riconducibili Agli Obiettivi Del PNSA 2021-27' (Tavolo di lavoro per l'implementazione del Programma Nazionale per la Scienza Aperta 2024) <https://iris.cnr.it/bitstream/20.500.14243/519247/1/Doc%202-%20Processi%20per%20individuare%20le%20attivita%CC%80%20gia%CC%80%20in%20essere%20V2%20-%202024.02.05.pdf> accessed 8 August 2025

[38] 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) OJ L 152, 3.6.2022, pp. 1–44

bodies, for instance, through the provision of technical instruments that preserve the privacy, confidentiality, integrity, and accessibility of the data that is shared.

In addition, the DGA strives to create new entities whose primary function will be to act as **data intermediaries to create a functioning and regulated data economy**. Data intermediaries are meant to add a layer of trust between the entities that share data (i.e., the data holders) or the data subjects, and those that re-use that data (i.e., the data users), acting as "neutral" entities that provide technical, legal or other means for the sharing of data, based on commercial relationships between the two. Data intermediation services are subject to strict rules regarding the processing of data (e.g., their sole purpose should be to facilitate data users' access to the data and cannot process such data for their own purposes) and must undergo an official notification procedure with the competent national authority.

Moreover, the DGA enables people to **voluntarily share their data**, such as their health data, for general interest purposes through the newly established mechanism of **data altruism**. Such purposes are defined in national law and include healthcare, public service improvement, policy-making, scientific research, etc. The sharing of personal data is authorized through the consent of the individuals concerned, while the sharing of non-personal data is authorized by the permission of the data holders. The organizations that engage in data altruism can request to be registered in a public national register,[39] provided that they operate non-for-profit, without establishing commercial relationships between data subjects / data holders and data users, that they are established as a legal entity that pursues purposes of general interest independently from other activities. They are also required to comply with the rulebook that the European Commission is set to establish, which will lay down common rules on information requirements, technical and security requirements, interoperability, etc. Data altruism organizations must also comply with transparency obligations, including maintaining records of data access activities and publishing annual reports detailing objectives, outcomes, and privacy safeguards. In addition, the DGA introduces protections for data subjects and holders, such as clear usage disclosures and user-friendly consent tools. Additionally, a standardized yet customizable data altruism consent form will be developed to facilitate data sharing.

In conclusion, the DGA lays down general rules for the flow of data between individuals, private and public organizations within domain-specific European data spaces (e.g., health, mobility, skills, finance, etc). Vertical legislation, such as the European Health Data Space Regulation (see below), will complement the DGA by providing domain-specific rules and requirements.

3.1.4.1. Consent(s)

Consent covers a central role in the DGA when it comes to allowing personal data re-use. Not only there is a specific type of consent introduced anew by this regulation, namely data altruism consent, but also in other settings. For example, when it is impossible to anonymize personal data held by public bodies for re-use, the confidentiality and privacy of such data should be safeguarded – however, they are still considered personal data. If consent is the legal basis, whereas no contact information of the data subjects should be disclosed to data users to avoid direct contact, the public body can transmit the consent request to the relevant individuals, with the caveat that they are clearly informed of the possibility to refuse consent (Recital 15). Public

[39] Available at: https://digital-strategy.ec.europa.eu/en/policies/data-altruism-organisations. In August 2025, only three organizations have requested to be registered.

sector bodies should facilitate data re-use by establishing "adequate technical means" that would help data users to seek consent from individuals (Recital 15), also with the assistance of competent bodies that can also support public bodies in implementing secure processing environments, structuring data to increase their accessibility and applying privacy-preserving or privacy-enhancing techniques such as pseudonymization and anonymization (Article 7(4)). The necessity to resort to automated means to efficiently and effectively transmit and manage consent requests for re-use, including in data altruism cases, is central in the DGA. Member States should establish national policies and "organizational or technical arrangements" intended to promote data altruism, including making available "easily understandable tools" for consent management (Recital 45). The Commission should also establish a European data altruism consent form through implementing acts (Article 25).

Certain kinds of data intermediation services can explicitly support the decisions of individuals about data sharing, in particular, providers that "seek to enhance the agency of data subjects". This concerns cases where individuals intend to exert control over their personal data and exercise their GDPR rights including giving and withdrawing consent. Data intermediation services should thus advise data subjects on the potential uses of their data and make due diligence checks on data users against fraudulent practices (Recital 30). Such services should act in the best interest of data subjects and should inform them transparently (Article 12 (m)). Additionally, they can provide individuals with tools for consent management (Article 12 (n)). Personal data spaces can, for instance, enable individuals to enable direct access to their own data without the necessity of transmitting it to third parties (Recital 30). Another relevant form of data intermediation for consent management is represented by data cooperatives that can "strengthen the position of individuals in making informed choices before consenting to data use" (recital 31), for example by assisting them in their decisions and negotiating terms and conditions to data processing.

3.1.5. The Data Act

The EU Regulation 2023/2854[40] (the Data Act) **sets clear rules concerning how private subjects should access data** that are generally generated by Internet of Things (**IoT**) objects in order **to create new products and services on secondary markets**. However, these new products and services must never be in direct competition with the original product or service that was accessed (Article 4(10); Article 6(2)(e) DA). Moreover, the Data Act establishes rules concerning fairness in data sharing contracts, interoperability, and switching between cloud providers. In addition, a part of the DA aims at governing the relationship between the EU institutions, the MS and the private parties to share data in emergency situations such as the case of a pandemic.

The Data Act is mainly known because it creates the main framework for **data sharing contracts**. Data sharing is thought to help make the IoT and apps market fairer by taking down barriers to access data gathered by the dominant technological businesses through the means of contracts (Bygrave, 2023; Ullrich, 2020). Generally, if data is not readily accessible as prescribed by Article 3 DA in an object with integrated software (which is called connected

[40] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) OJ L, 2023/2854, 22.12.2023.

product, Article 2(5)) or in a software application which is downloaded on the object (which is called related service, Article 2(6)), then the user can ask access to the connected product or related service data. There are two kinds of contracts. A first group of contracts concerns **private individuals in a B2C or B2B relationship**. Instead, the second kind of contracts concerns **emergency cases in which businesses must give access to the same sets of data that consumers or companies can require** at the demand of either an EU institution or a national body (Chapter V DA). We will describe them subsequently.

As far as the first set of contracts is concerned, two scenarios must be considered, and they are described in Articles 4 and 5 DA. Article 4 gives the possibility to **a user** (which can be either a consumer or a professional, in terms of EU law) to **ask a data holder for access to their data**. The DA provides access to all types of data (personal and non-personal) and metadata produced by connected products (e.g., objects with interconnected software) or related services (e.g., downloadable apps). Article 5 instead involves three subjects: **a user, a data holder, and a data recipient**, which in this article is called a third party. In this article, there are two sub-scenarios. In the first scenario, the user requests that the data holder grant access to the third party, which will then use this access to create a new connected product or related services, either alone or in conjunction with the user. The second *sub-scenario* instead is the following: it is the third party, on condition of a previous user's authorization, that will ask the data holder for access to the relevant data and metadata.

All three stakeholders have duties and requirements towards one another. In both cases, the data holder cannot request information that is unnecessary to the purpose of the data sharing or make it "unduly difficult" (Article 4(4) and 5 (4) DA). However, the data holder is entitled to protect their IPRs, which might become apparent during the data sharing (especially trade secrets) and have ways to avoid future litigation (Article 4(6)(7)(8)(9); Article 5(9),(10),(11),(12) DA). There are only exceptional cases in which the data holder can refuse to give access, and that is when EU or national security requirements might be breached by giving access to data (Article 4(2) DA). Exceptionally, the data holder can restrict access if this can cause them economic harm, as a result of a trade secrets disclosure (Article 4(8), 5(11) DA). Respectively, the user cannot abuse their position and cannot appoint as a third party an entity that is considered to be a gatekeeper according to the Digital Markets Act (DMA)[41]. In any case, the third-party data recipient or the user cannot take advantage of their position to try to coerce or abuse gaps in the data holder's technical infrastructure (Article 4(11), Article 5(5) DA).

As far as the **Business to Government (B2G) data sharing contracts**, they should be enforced only in exceptional circumstances, such as public emergencies, when there is no time to obtain the relevant data in any other way (Article 15(1)), such as during the COVID-19 pandemic. In alternative, these contracts can be used to access non-personal data whenever there is an exceptional need to use data or whenever not having access to data prevents a EU or national body to fulfil a specific task in the public interest, and the public body has exhausted all other

[41] A gatekeeper is either a platform or another internet service provider whose importance on a specific market is so apparent that it can allow, restrict or ban access to any new incumbent. In EU law, to identify a gatekeeper one must combine the definition set in Articles 2(2) of core platform service with the quantitative thresholds set in Article 3 concerning the number of users and annual revenue. Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA relevance) PE/17/2022/REV/1 OJ L 265, 12.10.2022, p. 1–66, http://data.europa.eu/eli/reg/2022/1925/oj.

means to obtain access to the relevant data (Article 15(1)). Despite the non-explicit and imprecise definition of emergency, Article 17 DA details how the EU or national sector body must write the request for data during emergencies, which must be extremely precise. This kind of contracts will be applicable from 12 September 2025 and it appears that this will be a cumbersome procedure for data holders despite the promise of compensation set at Article 20.[42]

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

3.1.6. The European Health Data Space

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

In particular, the European Health Data Space (EHDS) established by Regulation 327/2025 (EHDS Regulation)[43] includes "*rules, common standards, and practices*"[44] for the **safe and secure exchange of electronic health data**, which are considered special categories of personal data and thus undergo the safeguards provided by law and has two main functions which interest health data, whose regime of processing is described by article 9 GDPR. The EHDS aims to facilitate access to electronic health data for primary and secondary use purposes. Primary use essentially comprises the processing of electronic health data for the provision of healthcare and related services. Conversely, secondary use refers to the processing of electronic health data for purposes other than those for which they were initially collected.

---

[42] Paseri L and Verhulst SG, 'Unpacking B2G Data Sharing Mechanism under the EU Data Act' [2025] BioLaw Journal - Rivista di BioDiritto 259

[43] Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847.

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

3.1.6.1. Primary use

Priority categories of electronic health data for primary use include patient summaries, electronic prescriptions, electronic dispensations, medical imaging studies and related reports, medical test results, and discharge letters (Article 14). EU Member States must ensure that these data are recorded in Electronic Health Record (EHR) systems and exchanged through the cross-border infrastructure MyHealth@EU. Patient rights include immediate and free access to their own data; insertion of information into their own EHR; data rectification; data portability; access restriction; and opt-out for primary use (with some limitations, for example in case of emergency).

In order to ensure the protection of health data collected in the EHR systems, Annex II of the EHDS provides a list of essential requirements, including a section dedicated to security issues. The requirements follow the principles of Recommendation 2019 on the standard exchange format for HER, focusing on preventing unauthorised access to electronic health data, requiring the adoption of reliable mechanisms for identification and authentication of health professionals, allowing different access rights depending on the specific role and supported by digital signature.[45] Moreover, the EHR system should enable patients (i.e. data subjects) to restrict access to electronic health data, except for emergencies. These measures align with the security-by-design perspective envisaged in the General Data Protection Regulation, which requires that any data processing activity be adequately secured against unauthorised access or unlawful processing, accidental loss, disclosure, destruction or damage, and identity theft or fraud.

3.1.6.2. Secondary use

The EHDS Regulation provides for secondary data uses a legal basis under Article 9(2), letters g), h), i) and j) GDPR, including related safeguards (recital 52). Access to data for secondary use is **limited to the purposes listed in Article 53(1),** including: public interest in the area of public and occupational health; policy making and regulatory activities; statistics; education and training; scientific research, including development and innovation activities; improvement of healthcare performance.

Five categories of secondary uses are prohibited: making decisions detrimental to individuals or groups based on their health data; discrimination; advertising or marketing; development of harmful products; activities that violate ethical provisions in national law.

The EHDS Regulation establishes procedures for obtaining access through (i) data permits; (ii) health data request approval; or (iii) access approval from the relevant authorised participant within the HealthData@EU infrastructure.
The procedure under (i) includes the following steps:

1. **Access application**. The data user applies for access to health data to a health data access body. Such application must include a) Information about the applicant. b) The specific

[45] Note that according to point 3.4 Annex II EHDS, the logging information that should be recorded are the following: "(a) identification of the health professional or other individual having accessed electronic health data;
(b) identification of the individual;
(c) categories of data accessed;
(d) time and date of access;
(e) origin(s) of data."

purposes for which access is requested (Article 53(1), EHDS Regulation). c) The explanation of the intended use of the data and expected benefit. d) The description of the requested data. e) A justification if access to data in pseudonymised format is requested. f) Security measures to prevent misuse of the data. g) The data retention period. h) The ethical assessment in accordance with national law.

2. **Assessment by the health data access body**. The body must verify a) Compliance of purposes with admissible purposes (Article 53(1), EHDS Regulation). b) Necessity, adequacy and proportionality of the requested data. c) Presence of a legal basis for data processing under Article 6(1), GDPR and justification for access to pseudonymised data. d) Adequacy of technical-organisational measures. e) Compliance of the ethical assessment with national law.
3. **Issuance of the data permit**. The health data access body has three months to decide. The data permit has a maximum validity of 10 years, extendable for another 10 years, if justified.
4. **Secure access**. The health data holder must make the data available in secure processing environments, with complete access tracking[46] (Rak, 2024).

The procedure under (ii) allows requesting health data from a health data access body in anonymised statistical form.
The procedure under (iii) concerns EU institutions, health research infrastructures (or analogous infrastructures), third countries and international organisations.
The fourth point is relevant in particular as regards the cybersecurity dimension, as the secure processing environment (SPE) should guarantee not only compliance with the GDPR but also with intellectual property rights, commercial and statistical confidentiality, integrity and accessibility.[47] In practice, the health data access body will retain control over the data processing actions carried out in the SPE by the data user, including the display, storage, download and export of data. In order to achieve such objective, the virtual environment dedicated to data sharing will require some specific security features, such as strong access control, communication control, and pre-defined operational protocols.

Individuals have the **right to opt-out of data processing for secondary use** (Article 71(1), EHDS Regulation). If an individual opts out, their data cannot be made available or otherwise processed in accordance with a data processing permit (Article 71(3), EHDS Regulation). However, national laws may establish mechanisms to make data available after an individual has opted out. This is provided that (i) the health data access application comes from a public sector entity or EU institution; (ii) data access is necessary to achieve the public interest or for research for important reasons of public interest; (iii) the data cannot be obtained by alternative means in an equally timely and effective manner; (iv) the health data requester provides justification.

The secondary use of data is especially relevant for those **research projects that develop new tools that need health-related datasets for training and validation.** The EHDS will make

[46] Rak, R. (2024). Anonymisation, pseudonymisation and secure processing environments relating to the secondary use of electronic health data in the European Health Data Space (EHDS). *European Journal of Risk Regulation*, 15(4), 928-938. https://doi.org/10.1017/err.2024.67
[47] The definition relies on the one included in Art. 2(20) Data Governance Act.

available relevant data, such as medical images in a secure manner to e.g., optimize the performance of AI-based medical decision-support systems, among the others.[48]

3.1.6.3. The National Level: The Fascicolo Sanitario Elettronico 2.0

The implementation of the EHDS in Italy fits into an already articulated national regulatory context, characterised by the **Fascicolo Sanitario Elettronico 2.0** (Electronic Health Record 2.0, FSE 2.0) and the Ecosistema Dati Sanitari (Health Data Ecosystem, EDS).
In particular, the decree of the Ministry of Health of 7 September 2023 (FSE 2.0 Decree)[49] established the FSE 2.0. The FSE contains identifying and administrative data of the patient, reports, emergency department records, discharge letters, synthetic health profile, prescriptions, medical records, drug dispensation, vaccinations, specialist services, patient's personal notebook, data from cards for implant carriers and screening invitation letters.

The **feeding of the FSE is automatic and does not require the patient's prior consent**. The activation of the FSE is equally automatic. The Ministry of Health and the Ministry of Economy and Finance clarified this by circular of 17 February 2021[50] addressed to the health departments of Regions and Autonomous Provinces[51]. This is deduced via interpretation from the elimination of the patient's prior consent to FSE feeding (Legislative Decree 19 May 2020 No. 34, which repealed Article 12 paragraph 3-bis of Legislative Decree 179/2012).

The following actors contribute to feeding the FSE:

(a) local health companies (aziende sanitarie locali), public health structures of the National Health Service and regional social-health services and SASN (Servizi territoriali per l'assistenza sanitaria al personale navigante, marittimo e dell'Aviazione civile), through their different organisational articulations,

(b) health structures accredited with the National Health Service and regional social-health services,

(c) authorised health structures,

(d) healthcare professionals, including those contracted with the National Health Service, when operating independently (Article 12, paragraph 1, FSE 2.0 Decree), insofar as they are data controllers for care purposes (Article 12, paragraph 2, FSE 2.0 Decree).

Such entities feed the FSE within five days of healthcare service provision and are responsible for non-feeding, late or inaccurate feeding (Article 12, paragraph 3, FSE 2.0 Decree).
For healthcare, prevention and international prophylaxis purposes, FSE data can be consulted by third parties only after the patient has read the information notice and given consent (Article 8, FSE 2.0 Decree). Consent can be revoked at any time.
The entity providing the healthcare service must inform the patient of the possibility of having **data obscured**. The obscured document is not removed from the FSE. Obscuring can be revoked at any time.

---

[48] See other examples at: https://ec.europa.eu/commission/presscorner/detail/en/QANDA_24_2251, accessed 30 April 2024.
[49] Ministero della Salute, Decreto 7 settembre 2023, Fascicolo sanitario elettronico 2.0 (23A05829), in GU, Serie Generale n. 249 del 24-10-2023.
[50] Ministero della Salute e Ministero dell'Economia e delle Finanze, circolare 17 febbraio 2021, Fascicolo sanitario elettronico (FSE): indicazioni per eliminazione consenso all'alimentazione del FSE (art. 11 DL 34/2020), 0002031-17/02/2021-DGSISS-MDS-P.
[51] Corso, S. (2024). Il Fascicolo Sanitario Elettronico 2.0. Spunti per una lettura critica. *Nuove Leggi Civili Commentate*, *2*, 334-362, p. 345.

Data subject to greater anonymity protection (Article 6, FSE 2.0 Decree) include data governed by provisions protecting HIV-positive persons, women undergoing voluntary pregnancy termination, victims of sexual violence or paedophilia, persons using drugs or alcohol, women who decide to give birth anonymously, as well as data and documents relating to family planning clinic services. In these cases, the patient can freely choose to make them visible to third parties.

Focusing now on **the use of data contained in the FSE 2.0 for research purposes**, Article 27, paragraph 5, FSE 2.0 Decree establishes the following transitional discipline:
"The decree of the President of the Council of Ministers 29 September 2015, No. 178, [...] ceases to be effective from the day of entry into force of this decree, except for Chapters III and IV, which remain in force until the adoption, with subsequent decrees under paragraph 7 of Article 12 of Legislative Decree 18 October 2012, No. 179, [...] of specific provisions for the processing of FSE data and documents for research and governance purposes." [courtesy translation by the Author]

This means that, until the issuance of new specific decrees, Articles 15, 16 and 17 of d.p.c.m. 178/2015[52] continue to apply for processing for research purposes. These Articles provide that: **Regions, autonomous provinces and the Ministry of Health are data controllers** for scientific research purposes, within the limits of their respective competences assigned by law (Article 15, d.p.c.m. 178/2015).

FSE data can be processed for research purposes only if they are deprived of the patient's direct identifiers and in compliance with the principles of indispensability, necessity, pertinence and non-excess. Name, surname and tax code, specific birth dates, identity document details, residence or domicile addresses, personal contacts, copies of analogue documents, unstructured textual, graphic or video information are all expressly excluded from processing (Article 16, d.p.c.m. 178/2015).

Regions, autonomous provinces and the Ministry of Health must process FSE data for study and scientific research purposes in accordance with the principles of **proportionality, necessity, indispensability, pertinence and non-excess**, in compliance with Articles 39, 104 and 110 of the Italian Privacy Code and the related Annex A.4 (Code of ethics for statistical and scientific processing) (Article 17, d.p.c.m. 178/2015).
These provisions will cease to be effective on 31 March 2026, pursuant to Article 17, paragraph 5, Decree of the Ministry of Health of 31 December 2024 (EDS Decree, see below).[53]

3.1.6.4. The National Level: The Ecosistema Dati Sanitari

By decree of 31 December 2024 (EDS Decree), the Ministry of Health established the EDS. **The EDS is designed to process, among others, data extracted from FSE documents and make them available for specific purposes, including scientific research**. The EDS services will be operational by 31 March 2026 (Article 25, paragraph 1, EDS Decree).

[52] Decreto del Presidente del Consiglio dei ministri, 29 settembre 2015, n. 178, Regolamento in materia di fascicolo sanitario elettronico (15G00192).
[53] Ministero della Salute, Decreto, 31 dicembre 2024 Istituzione dell'Ecosistema dati sanitari (25A01321), in GU Serie Generale n. 53 del 05-03-2025.

The EDS contains data conferred to the FSE system and those made available through the Sistema tessera sanitaria (Article 3, paragraph 1, EDS Decree). Regions and autonomous provinces are data controllers for data extraction and their transmission to the EDS (Article 6, EDS Decree). Data obscured under the FSE 2.0 Decree do not feed the EDS (Article 3, paragraph 2, EDS Decree).

For care, prevention and international prophylaxis purposes, health and social-health structures, contracted doctors and healthcare professionals who take care of the patient even outside the National Health Service can access EDS data only after the patient has read the information notice and given consent (Article 8, EDS Decree).

The EDS adopts an architectural solution based on distinct and independent storage units (Article 4, EDS Decree), which ensures **full segregation of data based on type** (clear, pseudonymised and anonymised) **and related risk level**. In particular, the EDS consists of:

1. 21 storage units dedicated to clear data for regions and autonomous provinces and one unit for SASN (Navigation Personnel Health Assistance Services).
2. One unit dedicated to pseudonymised data.
3. One unit dedicated to anonymous data.

Turning now to the use of EDS data for study and scientific research purposes in the medical, biomedical and epidemiological field, the EDS:

1. **Makes available to personnel of the Ministry of Health, National Agency for Regional Health Services (AGENAS) and Regions or Autonomous Provinces services for extracting anonymised data for scientific research purposes** (Article 17, paragraph 1, EDS Decree).
2. **Makes available services for extracting anonymised data to public and private entities that institutionally pursue scientific research purposes** (Article 17, paragraph 2, EDS Decree). In particular: a) Public and private entities that institutionally pursue scientific research purposes may submit a request for anonymised data extraction to AGENAS, accompanied by a research project compliant with methodological and ethical rules; if applicable, with ethical rules for statistical and scientific processing (Annex A5, Italian Privacy Code); and with the Data Protection Authority's prescriptions for special categories of data (provision of 29 July 2019) (Article 17, paragraph 2, EDS Decree). b) As data processor, AGENAS evaluates requests considering the purposes pursued by the requesting entity and accesses the data extraction service to provide anonymised data. The anonymised data made available are not stored in the EDS after provision (Article 17, paragraph 3, EDS Decree).

Regarding the processing of personal data for study and scientific research purposes in the medical, biomedical and epidemiological field (in compliance with the adequate safeguards provided by Article 89 of the GDPR), the EDS Decree refers to a subsequent decree for specific provisions.
Finally, as anticipated above, Chapter III of d.p.c.m. 178/2015 ceases to be effective from 31 March 2026, when the EDS should become operational (Article 17, paragraph 5, EDS Decree).

3.2. Health law

The second main EU framework to take into consideration while mapping the relevant applicable EU laws and proposals concerns public health. It focuses on mainly three instruments that have been modified recently and that are still being implemented at a national level because of their complexity. Those legislative acts are Regulation (EU) 2017/745 on Medical Devices[54] (hereinafter referred to as Medical Devices Regulation, MDR) and the Regulation (EU) 2017/746 on In Vitro Diagnostic Medical Devices[55]. 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)[56] 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)[57] 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, the level of risk to human health posed by the device necessitates differentiation in the certification and audit procedures that the medical device must undergo before being placed 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. Previously, there was no way to monitor its functioning after it had been marketed. This necessity emerged after the defective breast prostheses case[58], which made

---

[54] 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.

[55] 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.

[56] 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.

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

[58] 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

it clear that the system needed to be updated and that also post-market surveillance duties needed to be implemented. Moreover, the previous MDD was drafted in a time when the development of technologies applied to health, including biorobotics, AI, IoT and allied technologies, was still at the beginning. The MDR already considers software, at certain conditions, as a medical device (Article 2(1) MDR), 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 based on 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. Still, 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 a regulation and not a directive anymore.

Summing up, 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*
- ***improved coordination mechanisms*** *between EU countries in the fields of vigilance and market surveillance*"[59].

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

[59] See more at https://health.ec.europa.eu/medical-devices-new-regulations/overview_en accessed 03 July 2023.

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[60].

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

According to the MDR a custom-made device is '*specifically made in accordance with a written prescription of any person authorised by national law by virtue of that person's professional qualifications which gives, under that person's responsibility, specific design characteristics, and is intended for the sole use of a particular patient exclusively to meet their individual conditions and needs.*'[61] For instance a teeth retainer or an orthopaedic corset or a limb prosthesis.
To have a custom-made device **a specific kind of prothesis** to be made, **then this is a custom-made device** if it is done according to the patient's characteristics and needs. However, '*mass-produced devices which need to be adapted to meet the specific requirements of any professional user and devices which are mass-produced by means of industrial manufacturing processes in accordance with the written prescriptions of any authorised person shall not be considered to be custom-made devices*'[62]. This means that a mass-produced pace-maker is not a custom-made device, but a soft and artificial organ designed for a specific person is.
The difference is relevant as custom-made device manufacturers have specific obligations, such as to draw up technical documentation[63] and will need to follow the procedure described at Annex XIII of the MDR. Here is a brief sum-up of the procedure explained.

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

Section 2: The manufacturer needs to make all the documentation concerning the custom-made devices for the Member State authority (The Ministry of Health in Italy) to allow the conformity assessment with the MDR requirements including the site where the custom-made devices are manufactured.

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

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

---

[60] See more at https://health.ec.europa.eu/medical-devices-sector/new-regulations_en accessed 03 July 2023.
[61] Article 2(3) MDR
[62] Article 2(3) MDR
[63] Article 10(2) (4) MDR

Section 5: The manufacturer will review and document its marketing experience after the product is manufactured and marketed by following the Post Market Clinical Follow-Up (PMCF) described at Annex XIV part B and '*implement appropriate means to apply any necessary corrective action'* [64]. This means that **there must be a plan, which shall be periodically revised in which there will be the specification of methods and procedures to proactively collect and evaluating clinical data to confirm the safety of the custom-made device and of identifying unknown side effects**[65]. This procedure aims to manage the risk that custom-made devices might have on an individual's health. Another important obligation is to report accidents to the competent authorities (the Italian Ministry of Health) according to the Article 87(1) MDR procedure.

BRIEF internal actors could fall under the definition of custom-made medical devices. Moreover, Italy has started implementing this part of the MDR with a specific decree (see Policy Brief no. 9).

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

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

[64] Annex XIII MDR Section 4
[65] Annex XIV MDR Section 6.1

3.2.1.2. When is Software a medical device?

Article 2 of the Medical Devices Regulation (MDR[66]) **expressly includes software as a medical device**. It is the same for the In Vitro Devices Regulation (IVDR[67]) at Article 2(1) IVDR. Although software must be considered a medical device **if it has a medical function** as explained in the same article 2 it is difficult to tell in practice whether software has a medical function or not.
The Medical Devices Coordination Group[68], which is an EU expert pool on medical devices, affirmed it in a policy document in 2019. The impact of this perspective is relevant for all BRIEF actors as they might develop software with a medical function and need to follow the MDR rules in order to put it into service in the EU market (see Policy Brief no. 10).

Consider that **when software is a medical device it will need to be certified** as such, following the rules on Software risk at Annex VIII MDR section 6.3. This can affect the marketing and sale of the medical device as such. Moreover, the guidance definition of software is very general and can include also the definition of AI systems. As a consequence, the AI Act provisions could be applicable also alongside the MDR procedures, once into force.
In order to better understand the decisional process because of which a manufacturer can understand whether it has created or not a software as medical device, it is better to look at the decision tree drafted by the MDCG and that is reproduced below.

[66] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC *OJ L 117, 5.5.2017*, p. 1–175.
[67] Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU *OJ L 117, 5.5.2017, p. 176–332.*

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

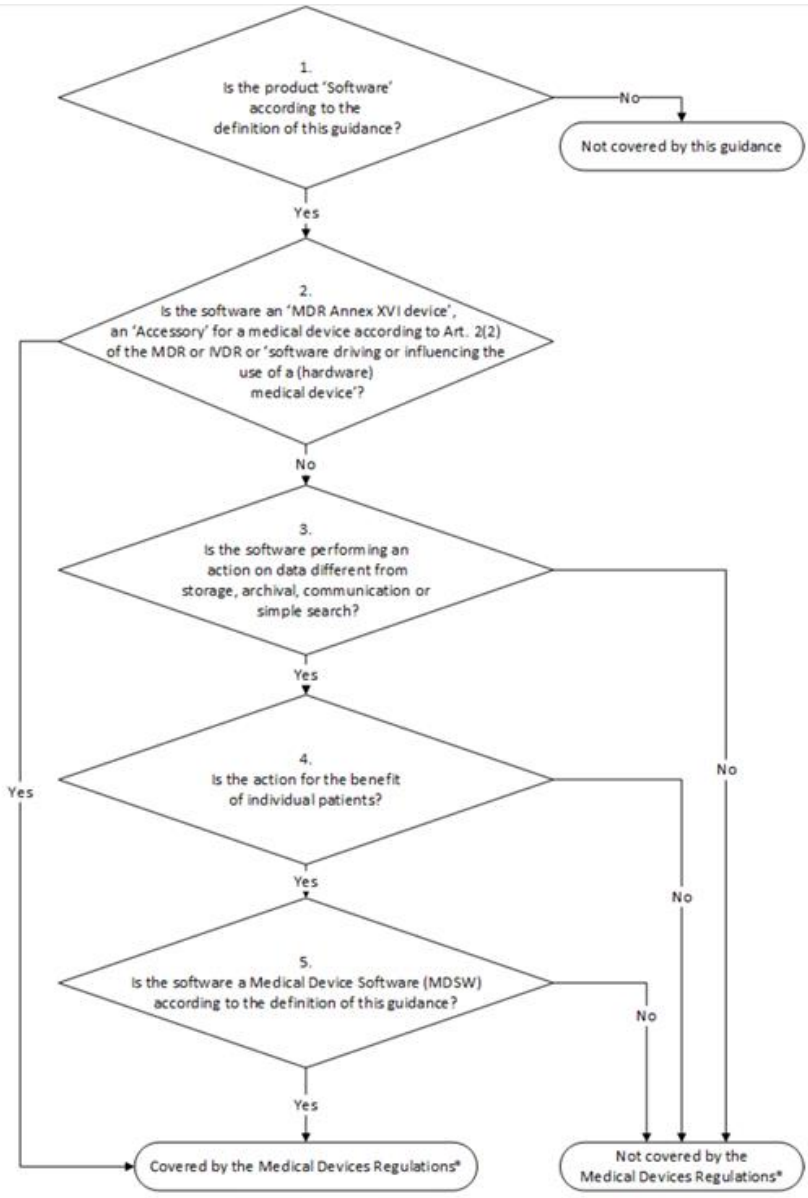

Figure 1 – Decision steps to assist qualification of MDSW

Medical Devices Regulations* refers to the two applicable regulations: Regulation (EU) 2017/745 on Medical Devices (MDR) and Regulation (EU) 2017/746 on *In Vitro* Diagnostic Medical Devices (IVDR)

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

A future rising problem, as far as SaMD is concerned, is implementing rule 3.1 of Annex VIII. In this rule, the manufacturer's intended purpose for the device plays a significant role. This rule will become increasingly important in the coming years as more medical devices incorporate AI systems, as mandated by the AI Act. More and more apps in fact claim they are not medical devices, but they work with sensitive data concerning health (Gennari, 2024a). Hence, the MDR still concedes a leeway to the manufacturer: in case there is a doubt about the fact that it is in fact Software as a Medical Device (SaMD), it is the intended purpose that counts (Gennari, 2024b). Moreover, there is also another rising issue, and it is that it is not yet clear

how compliance will be carried out in practice between the MDR and the AI Act with a high-risk AI system used for medical purposes (it will be basically all the classes except class I). Article 8 AI Act sets the rule that if the high-risk system is within the list of Annex I section A, then the manufacturer can follow the older conformity procedure (in this case, the MDR), and can add the relevant AI Act rules for high-risk systems. Nevertheless, this rule is brutal to put in place as, for instance, there are several parts of the MDR, such as the Quality Management System, which is general for all medical devices, and there is also the principle of quality management in the AI Act, which does not consider the medical implications of software. That is why the MDCG and the AI Office started coordinating with a set of guidelines (AIB 2025-1 MDCG 2025-6 Interplay between the Medical Devices Regulation (MDR) & In Vitro Diagnostic Medical Devices Regulation (IVDR) and the Artificial Intelligence Act (AIA), 2025) in form of Q&A that will be gradually implemented. At a first reading, the document does not give clear indications on how to practically implement the high-risk AI Act principles in a more concrete setting and what to select from the MDR conformity procedures when AI-powered SaMD is involved. As this document is a living document, it is expected that a better level of clarity will be achieved by the joint MDCG and AIB action.

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*[69]"

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

Pills of CTR

[69] 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

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

3.2.2.1. Clinical Trial Regulatory Streamlining

The Italian Medicines Agency (AIFA) issued Determination 424/2024 to simplify and decentralize clinical trial operations under the Clinical Trials Regulation (CTR). This guidance clarifies responsibilities for sponsors, principal investigators, and third-party service providers. Key principles include comprehensive documentation of all parties' roles, maintaining the Principal Investigator's ultimate medical responsibility regardless of outsourcing arrangements, and ensuring adequate training for service providers on study protocols and data protection requirements.

When third-party providers handle sensitive participant data, they must be formally designated as data processors under GDPR, with either the healthcare facility or sponsor serving as data controller. The data controller must ensure providers implement sufficient technical and organizational safeguards.

AIFA emphasizes the need for clear contractual frameworks defining each party's obligations, particularly regarding data privacy and security. All contracts must explicitly address third-party involvement, with Principal Investigators receiving advance notice of relevant terms.

3.2.2.2. Ethics Committee Restructuring

The CTR transformed EU ethics committee roles by creating a dual-track authorization system: Part I addresses technical-scientific aspects (evaluated by a reporting Member State), while Part II covers ethical and local considerations (handled by ethics committees).

A decree by the Ministry of Health of 26 January 2023 reorganized the ethics committee system, consolidating it into forty territorial committees distributed across regions.[70] These committees have exclusive jurisdiction over Part II evaluations while participating in Part I assessments alongside regulatory authorities.

Another decree by the Ministry of Health of 30 January 2023 clarified the composition and tasks of territorial committees and specialized national committees for advanced therapy medicinal products, pediatric trials, and public research entity studies.

TYPE OF BODY	***COMPETENCIES***
TERRITORIAL ETHICS COMMITTEES	1. Clinical trials on medicines 2. Clinical investigations on medical devices 3. Pharmacological observational studies
National Ethics Committee for pediatric trials	1. Clinical trials in pediatrics
National Ethics Committee for advanced therapies	1. Gene therapies, cell therapies and regenerative medicine
National Ethics Committee for EPR and public entities	1. Trials of public research institutes and other national public entities
National coordination center for territorial ethics committees	1. Coordination, guidance and monitoring 2. Operational support to territorial committees

Committee composition requires multidisciplinary expertise including clinical researchers, pharmacologists, bioethics specialists, and patient representatives. Members serve three-year terms with one possible renewal, while presidents are limited to two consecutive terms. These independent bodies are tasked with protecting participant rights, safety, and welfare when evaluating clinical trials, medical device investigations, and pharmacological observational studies. They can also provide broader ethical guidance and bioethics training.

The decree ensures committee independence through provisions preventing hierarchical subordination, requiring annual conflict-of-interest declarations, and establishing impartiality standards. All documentation must be submitted through official digital platforms, specifically the European Clinical Trials Information System. Notably, negative committee opinions result in nationwide trial denial, and evaluation fees are set by regional authorities.

3.3. Product safety and liability

The legal framework governing product safety and liability in the European Union is designed to protect consumers while fostering innovation and fair competition. This section outlines the key instruments shaping this domain, including the Machinery Regulation, the Product Liability

[70] Ministero della salute, Decreto 26 gennaio 2023, Individuazione di quaranta comitati etici territoriali.

Directive, and its recent update. Together, these measures establish clear responsibilities for manufacturers and ensure effective remedies for harm caused by defective products. They also reflect the EU's commitment to adapting legal standards to emerging technologies and market developments.

3.3.1. Machinery regulation (MR)

In June 2023, the EU approved a regulation that is an update of the previous machinery directive (MD)[71] due to several reasons, such as the **emergence of AI systems that act as safety components in the interaction with machinery**. This updated document is the machinery regulation (**MR**)[72] which sets harmonized minimum standards for health and safety requirements, but also for the design and construction of complex machines, such as biorobotic products (e.g., co-bots, robotic industrial arms, etc) (Article 1).
Both in the MD and MR (but also the MDR), the manufacturer must comply with a set of requirements if they want to market their product or service in the EU Single Market. The manufacturer's objective is to **obtain the CE marking**, which certifies the conformity of the product or service with the EU standards for health and safety. The change from directive to regulation is relevant because the Member States will need to apply the new text without deciding autonomously how to implement it. This will lead to a higher level of harmonization across the machinery sector. BRIEF researchers can look at the regulatory requirements to understand how to comply with the new rules, except when the national ministries give further clarifications on unclear passages of the regulation (see Policy Brief no. 16). Here follows a short preview.

PILLS OF MR
The MR has a **well-defined scope**, and it applies to the list of Article 2(1) objects, including software as a safety component. The same article also provides a list of excluded objects, such as weapons and aeronautical products. The concept of machinery is an encompassing one and it is generally understood as 'an assembly, fitted with or intended to be fitted with a drive system other than directly applied human or animal effort, consisting of linked parts or components, at least one of which moves, and which are joined together for a specific application' (Article 3(1) and following paragraphs)
All the ***actors*** involved in the machinery or related product's value chain have **duties and obligations.**
The objective is to obtain the **CE marking** through a **third-party conformity check**. Depending on the level of risk of the machinery, the conformity procedure will also vary.
The regulation sets a series of **essential health and safety requirements** that must be respected also to not be liable under the **new product liability framework.** This is important because software as a safety component is considered also **for high-risk AI systems by Annex I and Article 6(1) of the AI Act.** This means that the two regulations (MR and AI Act) will need to be respected at the same time in this case, otherwise, there might be liability consequences (see *infra*).

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

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

3.3.2. Product Liability Directive

The Product Liability Directive (PLD)[73] has survived unmodified for almost 40 years. Despite a new Product Liability Update being approved in November 2024 (see below Sec. 3.3.3), the actual PLD will be applied until 9 December 2026. Three articles of the PLD need to be known. If a consumer has experienced damage from using a consumer product, they will have to sue the producer to ask for damages.

To do that, a consumer must prove:
1) the **defect** of the product, which must be evaluated against the level of safety that one can legitimately expect (Article 6)
2) that the **damage** is either material or non-material. In the former case it can concern the consumer or other people and goes from physical injuries to death; if it concerns property, it must be above the threshold of 500 ECU (around 300 euros) and the item damaged must be a consumer object and was used by the injured person mainly for his private use or consumption (Article 9)
3) a **causal link** between the defect and the damage (Article 4)

The producer can exempt themselves from liability if they can demonstrate that one of the liability exemptions in Article 7 applies. Article 7(1)(e) is the so-called "**risk development exemption**". It means that the producer must prove that the kind of damage demonstrated in court by the consumer was unknown to them, given the state of technical knowledge at the time when the product was designed and subsequently put into the market.
The update of the PLD was expected due to the development of **new technologies such as AI, robotics, and IoT**, specifically because most cases involved:

- Consumers' difficulty in finding the producer and not being time-barred from action[74]
- Consumers' struggle to demonstrate the causality link, especially when side effects became apparent after many years of using a product [75]
- Consumers' indecision about whether to use national contractual and extra-contractual liability schemes, which could turn out to offer a higher degree of protection.[76]

3.3.3. Product Liability Directive Update

3.3.3.1. Background:

As explained above, new technologies such as AI, Robotics, and the IoT made it more evident that some aspects of the directive needed to be rethought, such as

- The **precise identification of the producer/manufacturer**: having complex product and value chains for consumer objects made it difficult for the complainant to sue the actual manufacturer, who could escape their responsibility[77].

[73] COUNCIL DIRECTIVE of 25 July 1985 on the Approximation of the Laws, Regulations and Administrative Provisions of the Member States Concerning Liability for Defective Products (85/374/EEC), OJ L 210 29
[74] SkovÆgvBilka LavprisvarehusA v Jette Mikkelsen and Michael Due Nielsen EU:C:2005:46
[75] C-621/15 N.W. and Others v. Sanofi Pasteur MSD SNC and Others
[76] González Sánchez. Case C- 402/03
[77] Gennari F, 'A Tale of Two Cities? Fennia v Philips and Article 7 of the Product Liability Directive Update' (2023) 12 Journal of European Consumer and Market Law

- The **causal link between damage and the defective product**. Sometimes, such as in cases of complex medicinal products such (e.g. anti-morning sickness medicinal products, or products containing dangerous materials (e.g. asbestos), side effects were latent or manifested genetically onto kids (such as paraplegic kids cases surge because of anti-morning sickness medicines) and demonstrating the causal link was actually very complex as those products had passed tests before being put into the markets. It was debated if the use of national legal presumptions was admitted or not[78]
- The **risk development exemption from liability** was deeply fought by some Member States, which did not consider it acceptable to have potentially unsafe products just because the state of science and technology did not allow them to know their side-effects in advance.
-

3.3.3.2. How does the PLDU work in practice?

The PLDU[79] works in the same way as the PLD. **The complainant must prove**:

- A defect that makes the product unsafe as far as the **safety expectation of an average consumer** is concerned, with a longer list of things that might make the judge opt for evaluating that a product might be defective. This list considers the automation and learning capacities of products and the disrespect of the cybersecurity and conformity requirements.
- A damage that can concern the person and includes physical injuries, including documented psychological damage and death, and property damage. A novelty is that, for the latter kind of damage, there is **no monetary threshold** below which it is not permitted to sue the producer. However, the property damage must not be on professional products as well as on data that is used also for professional purposes.
- A causal link that can be demonstrated through either Article 9 or 10. Article 9 is titled "**disclosure of evidence**" and allows, whenever the claimant has demonstrated the plausibility of the causal link between the damage and the product, to ask the judge to get access to how the product works. This must be done by ensuring that IP rights of the producer are protected. Article 10 instead allows the complainant to **use presumptions** both to prove the causal link, and the defect or both. However, it will be the judge to evaluate whether the presumptions can be applied to the specific case. Hence, even an indirect demonstration of plausibility of causality or defectiveness is needed to employ those
- The claimant has **3 years** to start proceedings from when the consumer becomes aware or reasonably becomes aware of the damage, the defectiveness and the identity of the relevant economic operator. After 10 years from which the legal proceedings should have begun, the claimant should not be able to sue the relevant economic operator. This time can be increased to 10 years to sue the manufacturer (former producer) but the time in which the claimant can act can be increased to 25 years in case the damage has a long time of latency before appearing.

[78] Gennari F, 'What Liability with the Internet of Things? Insights from the European Case-Law of the PIP Affair' (2023) 23 Global Jurist 125

[79] Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on Liability for Defective Products and Repealing Council Directive 85/374/EEC (Text with EEA Relevance) OJ L, 2024/2853, 18.11.2024

3.3.3.3. Where are the main criticalities of the PLD solved by the PLDU?

The reply to this question is nuanced. On the one hand, the articles that were challenged the most were changed to **take into account technologies and the previous CJEU case-law**, but it is still to early to tell whether this update is successful.

1) **The widened notion of manufacturer**

The manufacturer (once producer), according to Article 4(10) PLDU is not different in substance from the definition of producer of the PLD as it is the natural or legal person who "(a) develops, manufactures or produces a product ; (b) has a product designed or manufactured, or who, by putting their name, trademark or other distinguishing features on that product, presents themselves as its manufacturer; or (c) develops, manufactures or produces a product for their own use". The manufacturer is also the subject that substantially modifies a product. This applies to second-hand or refurbished technological object sellers/traders. Moreover, a software developer can also be considered a manufacturer as Article 4(1) includes software within the definition of product. What is important is the definition of whether software is a product according to Article 4(1) PLDU, **a software developer (including AI providers according to the AI) is a manufacturer according to the PLDU**. The notions of the manufacturer's control at Article 4(5) and the list of economic operators on which the original manufacturer's liability can be shifted at Article 8 shed light on the identification of the manufacturer. Manufacturer's control is especially relevant if a manufacturer decides to interconnect **third-party software** into their product. If the manufacturer can also only consent to the integration of software and provision of updates to be considered liable for damages and defects that have been caused by the third-party software and not by the hardware part of the product. As far as Article 8, it is true that it envisions contemporary product and value chains. Not only the manufacturer, **but also the importer, the authorized representative, the distributor, and hosting platforms** that respect the criteria of Article 6(3) Digital Services Act[80] are liable if the manufacturer itself and economic operators that follow them are outside of the EU, or not identifiable. Finally, there is also a residual clause which states that if none of the previous economic operators can be found in the EU or are available, then MS can set up dedicated compensation funds. All this has been done in order not to let EU citizens who sustained damage without any stakeholder to turn to in case the manufacturer cannot be found easily.

2) **Easier ways to demonstrate the causal link**

As mentioned supra, the causal link demonstration was difficult for a complainant to prove even before the advent of technologies such as AI, Robotics or the IoT. Article 9 remedy is conditional to the fact that the consumer has presented plausible elements for the judge to consider as to whether to get access to how the product (including AI systems according to the AI Act. Nevertheless**, judges must concede this remedy by also safeguarding the IP rights of the manufacturer.** It is still not clear how this will be done. Most likely, it will be each MS that will have to modify its civil code procedure to enact this rule. The same can be said concerning the presumptions concerning the burden of proof at Article 10 PLDU. All these presumptions are tied to the concept of **plausibility**. This can be a blunted sword for both consumers and manufacturers, as it will be a case-by-case evaluation scenario, which might make similar situations evaluated quite differently by judges. It is probable that if the damage

[80] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) OJ L 277, 27.10.2022, pp. 1–102.

is serious and visible, the threshold to prove the presumption possibility might be lower than in cases in which the damage is not clearly visible but might create a profound impact on a person's life.

3) **The risk liability exemption**
As far as this last point, Article 11 (1) (e) maintains the risk development exemption. However, the parameter that has been introduced to evaluate the applicability of this exemption is the **"objective state" of scientific knowledge**, which means that the manufacturer cannot exempt themselves by limiting the carefulness in designing a product to their subjective knowledge of science and technology, but to what is established in relevant fora such as well-reputed scientific journals. **It is possible for MS to not include this exemption in their legal systems** according to Article 18(1), but they have to notify the EU Commission. Moreover, they can also decide to implement the exemption as a general rule but to introduce an exception to it only if the following three conditions are respected: the exception to the exemption is limited to specific categories of products, it is justified by public interest and is "proportionate in that they are suitable for securing attainment of the objectives pursued and not going beyond to what is necessary to reach those objectives" (Article 18(2) and (3)). Also in this case, the EU Commission should be notified.

3.4. The EU Strategy on Artificial Intelligence

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

3.4.1 The AI Act

Finally approved by the European Parliament in 2024, the AI Act[81] is the world's first binding regulation that sets harmonized rules for the development and use of artificial intelligence (AI). The AI Act intends to ensure the safety of AI systems put into service or commercialized in the EU and uphold European fundamental rights, while boosting innovation in this field, leveraging the many benefits that can be envisioned, such as better healthcare. As part of the European approach to AI, this regulatory framework is accompanied by policies that support research and innovation such as the AI innovation package to support AI startups and SMEs[82] and dedicated investments in Horizon Europe.[83]
To this end, the AI Act adopts a **risk-based approach** that lays down rules to determine whether an AI system is prohibited, high-risk or not high-risk. From this categorization derive the obligations for developers and deployers and the relative requirements for the AI systems.

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

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

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

3.4.1.1. Scope of application: providers and deployers

The AI Act applies to providers (i.e., natural or legal persons, public authorities, agencies or other bodies) that develop AI systems or have them developed and place them on the Union market, or put them into service under their name or trademark (Article 3 (3)). If they are established or located outside the EU, the AI Act applies if they place those systems on the market or put them into service in the Union (Article 2(1)(a)), or if the output of the AI system is used in the Union (Article 2(1)(c)).
It also applies to deployers (again, natural or legal persons, public authorities, agencies, or other bodies) who use AI systems under their authority, unless this is for a personal, non-professional activity (Article 3 (4)). Similarly to providers, the AI Act applies even if they are not established in the EU but the output of the system is used within the EU territory.

3.4.1.2. The definition of AI system

An AI system is defined as "[a] ***machine-based*** *system designed to operate with* ***varying levels of autonomy*** *and that may* ***exhibit adaptiveness*** *after deployment and that, for explicit or implicit objectives,* ***infers, from the input it receives, how to generate outputs*** *such as predictions, content, recommendations, or decisions that can* ***influence*** *physical or virtual environments*" (Article 3 (1)). The AI Office's "Guidelines on the definition of an artificial intelligence system"[84] specify that these are cumulative conditions that, however, do not need to be present in both the pre-deployment phase and the post-deployment phase. The notion of autonomy is key, as it refers to the AI system's independence of actions from human involvement and capabilities to operate without human intervention (Recital 12) and is strongly related to its capacity to infer, i.e., to generate outputs "on its own" and understand how to do that. The system's capacity to change behavior while in use (i.e., adaptiveness) is also paramount for an AI system to fall within the AI Act's definition.

The Guidelines identify four exceptions of systems that ''have the capacity to infer in a narrow manner but may nevertheless fall outside of the scope of the AI system definition because of their limited capacity to analyse patterns and adjust autonomously their output" (p. 8): i) optimization methods; ii) basic data processing (e.g., data filtering); iii) classical heuristics (i.e., a rule-based form of inference); iv) simple prediction systems.[85]

3.4.1.3. Prohibited AI systems

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

1) use **subliminal, manipulative or deceptive techniques** impairing informed decision-making and causing significant harm; this risk is particularly present when brain-machine interfaces are implemented or virtual reality is used since these

[84] European Commission, 'ANNEX to the Communication to the Commission. Approval of the Content of the Draft Communication from the Commission - Commission Guidelines on the Definition of an Artificial Intelligence System Established by Regulation (EU) 2024/1689 (AI Act)' <https://ec.europa.eu/newsroom/dae/redirection/document/112455> accessed 10 April 2025

[85] Rossi, A., Gennari, F., Fagioli, I., Mazzarini, A., Moncelli, F., Amram, D., Crea, S., & Parziale, A. (In press). The AI system definition under the AI Act, a new nomen rosae? Proceedings of 2nd Workshop on Law, Society and Artificial Intelligence: Interdisciplinary Perspectives on AI Safety, June 10, 2025. Co-Located with HHAI: The 4th International Conference Series on Hybrid Human-Artificial Intelligence.

technologies allow for great control over the stimuli presented to the person (Recital 29).

2) **exploit vulnerabilities** of individuals or groups (i.e., age, disability, socio-economic situation) to distort behaviour and thereby cause harm; for example, children are generally considered more vulnerable than adults and at risk of being more easily affected in digital settings because of their lack of experience and their lower ability to resist influence;[86] data-driven algorithms can target such vulnerability to external undue influences and exacerbate the harmful repercussions that people may experience.
3) resort to **social scoring** that results in detrimental or unfavourable treatment of certain people; social scoring refers to the classification or evaluation of individuals or groups based on data related to their social behaviour in certain contexts or to their personal or personality traits over a period of time; it becomes particularly problematic when it is used to disadvantage people in contexts that are unrelated to those where the data was gathered or to treat people in a disproportionate or unjustified detrimental manner (Recital 31), such as when it is used to restrict the freedom of movement or the access to certain services.
4) perform **risk assessments** based on profiling or personality traits to **predict the likelihood of committing a criminal offence**; such assessments are not based on the actual behaviour of a person, but rather on other traits that are not objective verifiable facts such as the place of residence or the level of debt (Recital 42).
5) compile **facial recognition databases from scraping** activities carried out on the internet or CCTV footage because this practice can violate fundamental rights such as the right to privacy (Recital 43).
6) **recognise emotions** in **educational institutions or the workplace**, for example when emotion-recognition systems are used to determine access to education and career progression; there are general concerns about the reliability of such technologies since they carry the risk of performing inaccurate analyses of facial expressions and providing mistaken conclusions about the inner state of individuals (Recital 44).
7) use **biometric categorisation systems that deduce sensitive attributes** from biometric data, such as the processing of people's face or fingerprints to deduce whether they belong to categories of race, political affiliation, religious or philosophical beliefs, sex life or sexual orientation.
8) use **real-time remote biometric classification systems in public spaces for law enforcement** unless the use is strictly necessary under specific conditions (e.g., searching for missing people, preventing terrorist attacks); such systems, such as those that enable facial recognition, may be experienced as surveillance tools and dissuade people from exercising their rights such as the freedom of assembly; the fact that they are used in real-time reduces or annihilates the potential for oversight and correction (Recital 32).

9) Key insights on Biometric Systems

Biometric identification systems can uniquely identify a person through their face, voice, iris, or fingerprints.
Biometric systems use biometric data as input, which is considered a special category of personal data under Article 9 of the GDPR, and its processing is prohibited unless specific

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

conditions apply (e.g., the explicit consent of the data subject). National data protection authorities have already prohibited the processing of biometric data when it is not used for law enforcement purposes (Recital 39). Other biometric data that can uniquely identify individuals are of non-sensitive nature, such as behavioral aspects e.g., keystroke analysis.[87]
The AI Act prohibits the use of biometric systems when they are employed to make deductions, and consequently categorize individuals, on sensitive attributes, such as race, sexual orientation and political affiliation (see point 7 above). This kind of biometric categorization systems do not uniquely identify an individual or verify their identity (see below), but they need to categorize individuals into specific groups.[88] This prohibition does not apply to biometric datasets that are filtered, labelled or categorized in a lawful manner such as the sorting of images based on eye color. The purpose of these operations may be to avoid bias by equally representing all demographic groups.[89]
When **AI systems are used for biometric categorization** that infers sensitive attributes from biometric data, but the prohibition does not cover these cases, **they are classified as high-risk systems**.
Biometric systems are also increasingly used for verifying digital identities, providing users with access to specific services and strengthening security measures, such as multi-factor authentication. **When used for verification purposes, including authentication, biometric systems are not considered as high-risk.**
The use of real-time remote biometric classification systems for identifying people in public spaces for law enforcement purposes is prohibited (see point 8 above). Such systems are often based on facial recognition, where they seek to match a face captured by a video camera in a public space with those that are present in a database, for example to identify people on a watchlist (large scale face matching), or where they track an individual's movements in a geographical zone (targeted face tracking). It is prohibited to use such systems to identify people in real-time in public spaces, apart from specific cases with high public interest, which outweigh the risk (Recital 33) (such as searching for missing people or preventing terrorist attacks, among others) (Article 5(1)(h)). In these cases, **the use of a real-time remote biometric classification system is authorized only if the relevant law enforcement authority has made a fundamental rights impact assessment and has registered the system in the relevant database** (Recital 34). When the same system is used for **remote identification but not in real-time, the system is classified as high-risk** and subject to the additional safeguards for the deployment of such systems. The development of such systems is not prohibited, but it is subject to the rules of high-risk systems when they enter the market or are put into service.[90]

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

[87] Article 29 Working Party, 'Opinion 3/2012 on Developments in Biometric Technologies' (2012) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf>
[88] Ibid.
[89] European Commission, 'Commission Guidelines on Prohibited Artificial Intelligence Practices Established by Regulation (EU) 2024/1689 (AI Act)' (2025)
[90] Ibid.

3.4.1.4. High-risk AI systems

AI systems are categorized as **high-risk** (Article 6) whenever they significantly affect safety or fundamental rights, in particular when:
(a) they are used **as safety components or a product and need a third-party conformity assessment**, thus fall under the EU's product safety legislation (see Annex II), such as toys, aviation, cars, **medical devices** and lifts; or
(b) they are used in the following domains (listed in Annex III):

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

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

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

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

3.4.1.5. Obligations for developers of high-risk AI systems

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

Such a system should:
a) identify and analyse known and reasonably foreseeable risks to health, safety and fundamental rights when used for its intended purpose, as well as establish mitigation measures that should eliminate the risk or, when impossible, address it so that the relevant residual risk

is deemed acceptable, plus provide information and training to deployers that are relevant for transparency purposes (Article 13);
b) estimate and evaluate risks that may emerge when the AI system is used for its intended purpose or when misused in foreseeable ways;
c) evaluate other risks that may emerge from post-market monitoring.

To identify appropriate risk management measures, the AI system shall be tested, including in real-world conditions (see below). At date, there exist many risk management methods for AI[91] that take into consideration different factors. To this end, providers can make use of the **regulatory sandboxes** that will be established at the national, or even local, level by the competent authorities (Article 57). Regulatory sandboxes are meant to offer a controlled environment that enables the development, training, testing and validation of innovative AI systems for a limited time before they are made available on the market or put in use. Regulatory sandboxes enable the limited testing of innovative technologies in a real-world environment under regulatory supervision.[92] Provided that AI providers observe the agreed sandbox plan and the conditions for participation, no administrative fine will be imposed on them for violations of the AI Act and other regulations, if the competent authorities were involved in the supervision of the AI system testing. Since the goal is to **determine whether a specific innovative AI system is legally compliant, such regulatory sandboxes can foster innovation and competitiveness, accelerate access to the EU market, particularly for SMEs and start-ups, and enhance** legal certainty for innovators. Competent authorities achieve this objective also thanks to the drafting of guidelines and sharing of best practices based on the results and lessons learnt from the experiences carried out within the sandboxes. Regulatory sandboxes are also meant to **identify risks upfront and devise mitigation measures**, on which competent authorities will provide guidance and support. Authorities will also produce a final report that AI providers can use to demonstrate compliance with the AI Act.

AI providers of systems listed in Annex III (see above) can also test their systems outside of regulatory sandboxes in "**real-world testing**" environments (Article 60) under specific conditions, such as the submission of a plan to the market surveillance authority that needs to authorize the testing; the registration of the testing under a unique identification number; a limited time period (no longer than 6 months); the informed consent of participants; effective oversight; and the possibility of reversing or disregarding the predictions, recommendations and decisions of the AI system.
Both regulatory sandboxes and real-world testing environments constitute relevant novelties for the AI systems developed within BRIEF, since they could offer safe environments where to test the AI systems and reach the market more rapidly, with enhanced legal certainty.

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

[91] For a recent overview, see e.g., Xia B and others, 'Towards Concrete and Connected AI Risk Assessment (C2AIRA): A Systematic Mapping Study', *2023 IEEE/ACM 2nd International Conference on AI Engineering – Software Engineering for AI (CAIN)* (2023)
[92] Thomas Buocz, Sebastian Pfotenhauer and Iris Eisenberger, 'Regulatory Sandboxes in the AI Act: Reconciling Innovation and Safety?' (2023) 15 Law, Innovation and Technology 357.

requirement on data governance also impacts other requirements for high-risk AI systems, such as the one on technical documentation, transparency, human oversight and risk management. We refer the reader to Policy brief no. 14 for more accurate information on data governance.
Providers of high-risk AI systems are also required to provide **technical documentation** to demonstrate compliance (Article 11). The documentation should include (see Annex IV) i) a general description of the system concerning e.g., the version of relevant software or firmware, the hardware and the user-interface provided to the deployers; ii) a detailed description of the system design covering elements such as expected outcomes, system architectures, training datasets, among many others; iii) a detailed description of the monitoring, functioning and control of the AI system, such as its capabilities and limitations in performance and the foreseeable unintended outcomes and sources of risks; a description of iv) the appropriateness of the performance metrics; of the v) risk management system; and of vi) relevant changes made during the lifecycle; vii) a list of the applied harmonised standards; viii) a copy of the EU declaration of conformity and xi) a description of the post-market surveillance system.

In addition, high-risk AI systems should technically allow for **record-keeping** of the systems' activities (Article 12) for traceability and monitoring purposes. Moreover, they are subject to **transparency** obligations so that deployers can interpret a system's output and use it appropriately (Article 13) – see also Policy brief no. 12 on transparency. In particular, information should be disclosed in a concise, complete, correct and clear manner about its functioning, such as i) the purpose, ii) the accuracy, robustness and cybersecurity; iii) circumstances that may lead to risks to the health and safety or fundamental rights; iv) the technical capabilities that are relevant to explain the output; v) when appropriate, its performance regarding specific persons or groups; vi) input data; vii) where applicable, information that can help deployers interpret the output and use it appropriately. In addition, the disclosure should regard human oversight and the computational and hardware resources needed, along other informational items.
The AI Act also establishes **human oversight** requirements (Article 14) to ensure the prevention or minimization of harm through the establishment of commensurate measures that can be developed by both the provider and the deployer. This means that human beings should be able to be meaningfully involved in the development and use of AI systems with the goal of detecting and addressing anomalies, being aware of automation bias, providing a correct interpretation of the system's output and the decision on whether to use it or not, as well as halting the system with a dedicated function when needed.

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

appoint an authorised representative established in the EU, when they are established in third countries (Article 22).

3.4.1.6. Obligations for deployers of high-risk AI systems

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

Deployers that are public bodies, private entities providing public services (in the areas of education, healthcare, social services, housing, administration of justice), entities performing creditworthiness assessment and risk assessment and pricing for health and life insurances must perform a **Fundamental Rights Impact Assessment** (hereinafter FRIA) for high-risk AI systems (Article 27), which is an evaluation of the risks that the AI system pose to fundamental rights of the individuals or groups of individuals likely to be affected (recital 96). Fundamental rights that may be impacted concern the presumption of innocence and right to an effective remedy and to a fair trial, the right to equality and non-discrimination, the right to freedom of expression and information, the right to privacy and data protection, among the others.[93] The FRIA consists in i) a description of the processes, period and frequency where the AI system will be used; ii) the affected people and the specific risks of harms; iii) a description of the implementation of measures of human oversight and measures against the identified risks. Deployers should then notify the market surveillance authority of the results.

3.4.1.7. Requirements for general-purpose AI

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

Provisions in **Article 51 distinguish between general-purpose AI models with system risks and those that do not pose systemic risks**. This difference is based essentially on the model's size determined by its computing power (and the amount of data used for training). More specifically, all providers of such GPAIs are subject to the obligation to provide the relevant technical documentation and information for downstream developers (Article 53). However, providers of GPAI whose FLOPs (floating point operations) is greater than 10^25 are considered as posing systemic risks, and thus subject to additional requirements, such as performing model evaluations, report serious accidents, and adopt cybersecurity measures (Article 55).

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

In July 2025, a code of practice for GPAI[94] was adopted by the European Commission and signed by many enterprises, including industry leaders. The code helps providers of GPAI demonstrating compliance with their obligations under Article 53 AI Act concerning transparency and copyright, as well as providers of GPAIs with systemic risks demonstrate compliance with the obligations under article 55 concerning safety and security.

3.4.1.8. Scientific research

The AI Act strives to foster experimentation, innovation and international competitiveness, while ensuring safety and fundamental rights.[95] This is why, the provisions of the AI Act do not apply to AI systems and models that are "specifically developed and put into service for the sole purpose of scientific research and development" (Article 2(6)). An additional relevant provision describing the scope excludes "any research, testing or development activity regarding AI systems or AI models prior to their being placed on the market or put into service. […] Testing in real world conditions shall not be covered by that exclusion" (Article 2(8)).

This means that **research activities are excluded only if the systems are designed and used exclusively for the purpose of research and development, or before they are released to the market or put into service**. In such cases, even prohibited practices (see Section 3.3.1.3) may be implemented for experimentation and testing purposes during the R&D phases.[96] However, any activity should be conducted in line with relevant ethical and professional standards (see Section 3.3.3) and in compliance with applicable laws,[97] such as data protection (see Section 3.1.1). Furthermore, to identify the exact scope of application, it is crucial to define the material scope of the exemption. First, "placing on the market" refers to the "first making available of an AI system on the market" (Article 3(9)), where "making available" means supply of the system "for distribution or use on the Union market in the course of a commercial activity, whether in return for payment or free of charge" (Article 10). Very importantly, supply may mean access to the AI system through an API, via cloud or via its embedding in a physical product, its download from a repository or similar, its availability on physical copies, etc. Even though financial payment is not a prerequisite and the AI system can be accessed for free, its availability should be part of a commercial activity, which excludes pure academic research activities (e.g., when a system is uploaded to GitHub for reasons of open science), but of course includes commercial practices of a spin-off. Second, "putting into service" is "the supply of an AI system for first use to the deployer or for own use in the Union for its intended purpose" (Article 3(11)), which includes its provision to third parties, as well as in-house development and deployment, for the purpose intended by the provider for the first time.[98]

That said, it is plausible that at least some, if not most, of the AI models developed within BRIEF may be later introduced on the market or used outside of research laboratory settings and therefore will need to comply with the requirements set forth by the AI Act and addressed to providers. Moreover, certain of these AI systems, such as those used as medical devices, are

[94] European Commission, 'The General-Purpose AI Code of Practice' <https://digital-strategy.ec.europa.eu/en/policies/contents-code-gpai> accessed 17 September 2025
[95] European Commission. Directorate General for Research and Innovation., *Successful and Timely Uptake of Artificial Intelligence in Science in the EU* (Publications Office 2024) <https://data.europa.eu/doi/10.2777/08845> accessed 18 April 2024
[96] European Commission, 'Commission Guidelines on Prohibited Artificial Intelligence Practices Established by Regulation (EU) 2024/1689 (AI Act)' (2025)
[97] Ibid.
[98] Ibid.

classified as high-risk systems under the AI Act and are therefore subject to stringent requirements that address both developers and deployers (see Scenario B).
Note also that the research exception covers the AI under development, it does not cover the AI systems and models used for the research and development that have been already put into service. Hence if a researcher is using an AI system already put into service or available on the market (e.g., GPT), the exception would not apply to it and the researcher would be constrained as a deployer, if applicable.

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

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

Another relevant scenario for researchers concerns the regulatory sandboxes and other conditions of real-world testing described earlier. Such activities should be conducted in compliance with the requirements for sandboxes and real-world testing described above and should be carried out in accordance with the guidelines produced by the competent authority. Further, in real-world testing settings, scientists should be mindful of applicable Italian and European legislations.

Moreover, as we argue below, the **AI ethics framework** applies to any R&D activity. Overall, even when commercialization is not envisaged, scientists are held accountable for the decisions they take at any stage of the research. Thus, it is recommended to follow the ethical guidelines that the European Commission and other authoritative bodies publish, and respect the seven principles for the development of trustworthy AI reported below. Indeed, one of these cornerstones is accountability, accompanied by human agency and oversight, technical robustness and safety, privacy and data governance, transparency, diversity, non-discrimination and fairness, environmental and social well-being. As it can be noted, the requirements introduced by the AI Act build on such principles. More broadly, all researchers need to embed into their conduct the principles of reliability, honesty, respect and accountability of the European Code of Research Integrity. Whenever the AI systems may be foreseeably deployed on people, a good practice of scientific research conduct with human subjects (Oates et al., 2021) should be based on the following four tenets: i) respect for the autonomy, privacy and dignity; ii) scientific integrity; iii) social responsibility and iv) maximize benefits and minimize harms.

3.4.1.9. The Italian Law on Artificial Intelligence[99]

On 17 September 2025, the Italian Senate definitively approved the *Disegno di Legge n. 1146*, titled *Disposizioni e deleghe al Governo in materia di intelligenza artificiale*, which was published on the *Gazzetta Ufficiale* on the 25th September (*Legge 132/2025*). The law establishes Italy's national framework for artificial intelligence (AI) aligned with the AI Act, and will enter into force on October 10th.

Article 3 outlines the foundational criteria for the research, development, deployment, and use of AI systems in Italy, without introducing new obligations beyond those set by the AI Act. These activities must comply with fundamental rights and freedoms enshrined in the Italian Constitution and EU law, and adhere to principles such as transparency, proportionality, security, data protection, confidentiality, accuracy, non-discrimination, gender equality, and sustainability. The law requires that AI systems be developed using data and processes that are correct, reliable, secure, high-quality, appropriate, and transparent, with proportional safeguards tailored to the sector of application. Human autonomy and decision-making must be preserved, and systems must ensure transparency, explainability, knowability, and human oversight. Importantly, AI must not interfere with democratic processes or institutional autonomy, nor compromise the integrity of public debate or national sovereignty. The law also mandates cybersecurity as a precondition throughout the AI lifecycle, with risk-based security controls to ensure resilience against manipulation. Finally, the law guarantees full, equal, and non-discriminatory access to AI systems and functionalities for persons with disabilities.

Among its key provisions for BRIEF research activities, Article 8 concerns the data processed by public and private non-profit entities, IRCCS, and private actors involved in collaborative research with those entities and used for scientific research and experimentation in the healthcare sector for developing AI systems. Article 8 declares that data to be of public interest (under Art. 9(2)(g) GDPR) when used for scientific research and experimentation in the development of AI systems; prevention, diagnosis, and treatment of diseases; development of drugs, therapies, and rehabilitative technologies; creation of medical devices, including prosthetics and interfaces between the body and support tools for patient conditions; public health; personal safety; health and sanitary security; and study of human physiology, biomechanics, and biology, including in non-health contexts (e.g., sports).

Moreover, the secondary use of personal data without direct identifiers is always authorized, but subject to a public notice published on the data controller's website (according to Art. 13 GDPR). No further consent from the data subject is required if initially provided by law. In addition, the processing for anonymization, pseudonymization, or data synthesis purposes is always permitted (but AGENAS will publish guidelines, subject to the Data Protection Authority's opinion). The processing may begin 30 days after notification to the Data Protection Authority (and without its objection), which must be informed of: technical and organizational measures adopted to ensure and demonstrate compliance (Art. 24 GDPR); measures to ensure data protection by design and by default (Art. 25 GDPR); security measures appropriate to the risk, including pseudonymization (Art. 32 GDPR); impact assessment (Art. 35 GDPR); ad the data processors (Art. 28 GDPR).

[99] Legge 23 settembre 2025, n. 132 "Disposizioni e deleghe al Governo in materia di intelligenza artificiale". GU: n. 223 del 25-09-2025.

Of interest is also Article 9: an implementing decree by the Ministry of Health is expected within 120 days from the publication of the law to regulate, in a simplified manner, the processing of data (including secondary use) for research and experimentation purposes based on AI and machine learning, also through the creation of experimentation spaces. This will be done in consultation with the Data Protection Authority, research institutions, healthcare facilities, and relevant authorities and operators.
Moreover, Article 16 delegates the Government to adopt legislative decrees to "define a comprehensive framework regarding the use of data, algorithms, and mathematical methods for training artificial intelligence systems", including the rights and obligations of data users, within 12 months.

3.4.2 Ethical guidelines for AI development

In addition to the requirements laid down by the AI Act, the framework of reference remains the 2019's Ethics guidelines for trustworthy AI developed by the independent AI High-Level Expert Group appointed by the Commission. The framework is based on seven pillars that ensure that the **AI is trustworthy, human-centric and ethically sound.** The seven principles have also been further declined in the ALTAI checklist (see below) and are recommended by many research funding agencies, such as in the European Commission's guidelines on "Ethics By Design and Ethics of Use Approaches for Artificial Intelligence"[100] addressed at Horizon Europe's applicants and beneficiaries, to which we refer our readers for further information. As mentioned earlier, even though the AI Act excludes pure research activities from its scope, researchers nevertheless have accountability and other ethical duties. In the EU, several instruments have been produced to provide guidance to developers of AI and researchers that develop or somehow make use of AI, such as generative AI.

3.4.2.1. Assessment List for Trustworthy Artificial Intelligence (ALTAI)

The Assessment List for Trustworthy Artificial Intelligence (**ALTAI checklist**) developed in 2020 by the then High-Level Expert Group on Artificial Intelligence is a list that whoever develops new forms of technology (and, in particular, AI-based ones) is supposed to follow in order to check the compliance of their technology with EU values on technology. The checklist is not binding, it is a guideline shaping how a developer shall address the lawfulness, ethics, and robustness of a given solution. It is divided in 7 chapters and 63 questions to address, aiming to assess different features:

- **Human agency and oversight:** it is important that no AI system is left completely unsupervised.
- **Technical robustness and safety**: it is necessary that the technology is sound also from a cybersecurity point of view.
- **Privacy and data governance**: it is mandatory to respect both data protection and privacy as fundamental rights under the GDPR obligations.

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

- **Transparency**: it is important to share with other researchers the results and also with the data subjects but there must be a counterbalance whenever relevant intellectual property is involved and data protection.
- **Diversity, non-discrimination and fairness:** it is important that data for algorithms training is selected and processed in a way that the highest variety of information is gathered and processed not to have biased results.
- **Environmental and social well-being**: it is necessary to think about durable and sustainable technology starting from the design of the solution as we are all witnessing a climate emergency.
- **Accountability:** this task is solved not only through the compliance with legal tasks, but also by being able to explain and justify each decision taken on ethical legal implications of the R&D&I.

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

In March 2024, the European Commission published guidelines on the **responsible use of generative AI in research addressed to various stakeholders,** within the ERA Forum, including universities, research organisations, funders and publishers: "*Living guidelines on the responsible use of generative AI in research*".[101] They build on the main principles of research integrity and on existing frameworks regarding the use of AI, such as the ALTAI checklist and the European Code of Conduct for Research Integrity.[102]
In particular, the guidelines are promoting a responsible use of generative AI, providing recommendations for organisations and researchers, inspired to the following 4 key principles of EU research conduct:

1) **Reliability**: strongly connected to the quality of research, it concerns the verification and reproduction of AI-generated content, with an eye on potential inequalities and discrimination issues as well as the falsification or manipulation of data; this also means to be aware of the limitations of generative AI, such as the risk of hallucinations, bias and inaccuracies.
2) **Honesty**: applied to all stages of research, it also means disclosing whether generative IA has been used, for instance in interpreting data analysis, carrying out a literature review, identifying research gaps, formulating research aims, developing hypotheses and drafting articles.
3) **Respect**: towards collaborators, research participants, society and environment at large, responsible use of generative AI should also account for its limitations, its environmental impact and its societal effects concerning fairness, non-discrimination, prevention of harm, privacy, confidentiality and intellectual property rights; for example, researchers do not upload unpublished or confidential work, since it could be used for further training; they do not feed the tool with others' personal data unless they have gathered the consent of those people and unless they have a clear goal for doing

[101] European Commission. Directorate General for Research and Innovation., 'Living Guidelines on the Responsible Use of Generative AI in Research' (2024) <https://research-and-innovation.ec.europa.eu/document/2b6cf7e5-36ac-41cb-aab5-0d32050143dc_en> accessed 18 April 2024
[102] ALLEA, *The European Code of Conduct for Research Integrity - Revised Edition 2023* (ALLEA - All European Academies 2023) <https://doi.org/10.26356/ECoC> accessed 18 April 2024

so; they also need to be mindful about how and where the tool uses personal data and by whom it is managed.

4) **Accountability:** from the research idea to publication, but also beyond (societal impact), researchers are responsible for any output of the research (see also reliability), which should be sustained by human agency and oversight; this also means that researchers respect applicable laws (e.g., on the protection of personal data and of intellectual property).

3.5. Intellectual Property Rights (IPRs)

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

- **For copyright:** the Software Directive,[103] the Database Directive,[104] the Information Society Directive (InfoSoc Directive),[105] the Copyright in the Digital Single Market Directive (CDSMD),[106] and the Term Directive.[107]
- **For patents:** the Unitary Patent Protection Regulation,[108] Intellectual Property Rights Enforcement Directive (IPRED),[109] the Directive on the Legal Protection of Biotechnological Inventions,[110] and the Proposed Regulation on Standard Essential Patents.[111]

[103] Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs (Codified version) (Text with EEA relevance), OJ L 111, 05.05.2009, p. 16-22.
[104] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, OJ L 77, 27.03.1996, p. 20-28.
[105] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, OJ L 167, 22.06.2001, p. 10-19.
[106] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (Text with EEA relevance), OJ L 130, 17.05.2019, p. 92-125.
[107] Directive 2006/116/EC of the European Parliament and of the Council of 12 December 2006 on the term of protection of copyright and certain related rights (Codified version), OJ L 372, 27.12.2006, p. 12-18.
[108] Regulation (EU) No 1257/2012 of the European Parliament and of the Council of 17 December 2012 implementing enhanced cooperation in the area of the creation of unitary patent protection, OJ L 361, 31.12.2012.
[109] Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights (Text with EEA relevance), OJ L 157, 30.04.2004, p.45-86.
[110] Directive 98/44/EC of the European Parliament and of the Council of 6 July 1998 on the legal protection of biotechnological inventions, OJ L 213, 30.07.1998, p. 13-21.
[111] Proposal for a Regulation of the European Parliament and of the Council on standard essential patents and amending Regulation (EU) 2017/1001 (Text with EEA relevance), 27.04.2023, COM(2023) 232 final.

- **For trade secrets:** the Trade Secrets Directive.[112]
- **For industrial design:** the Design Directive,[113] and the Community Design Regulation.[114]

3.5.1. Copyright

In broad terms, copyright refers to a bundle of economic and moral rights granted to the author or the creator of an original intellectual creation, which is often required to be fixed on a tangible or an intangible medium.[115] Such an intellectual creation could be in literary, scientific and artistic domains. Regardless of the domain, mode or form of expression, the quality or content thereof, an intellectual creation would, in principle, be eligible for copyright protection if it is the outcome of the author's/creator's own intellectual creativity[116].

Copyright subsists in literary works – including software, artistic works, cinematographic works, musical works, architectural works, and original databases. Nevertheless, it is essential to emphasise that copyright protects merely the expression of an idea rather than the idea itself[117].

The economic rights encompassed within copyright consist of the rights to reproduction, communication to the public, making available to the public, and distribution (including lending and rental)[118]. Complementary to these rights of an economic nature are moral rights, which, generally, comprise the rights to claim authorship, and to object to certain modifications and other derogatory actions[119].

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

The author/creator of a work is, in principle, the first copyright owner of the work. Whereas the moral rights comprised in copyright remain with the author/creator, the economic rights thereof can be transferred or licensed to third parties. The transfer of copyright results in the change of the copyright owner; however, copyright licenses enable certain uses of a copyright-protected work without creating changes in the copyright owner's title.

---

[112] Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful, use and disclosure (Text with EEA relevance), OJ L 157, 15.06.2016, p. 1-18.
[113] Directive 98/71/EC of the European Parliament and of the Council of 13 October 1998 on the legal protection of designs, OJ L 289, 28.10.1998, p. 28-35.
[114] Council Regulation (EC) No 6/2002 of 12 December 2001 on Community designs, OJ L 3, 05.01.2002, p. 1-24.
[115] WIPO Intellectual Property Handbook, World Intellectual Property Organization, Geneva-Switzerland, 2004.
[116] Ibid. Also see: Directive 96/9/EC, Art. 3(1); Directive 2009/24/EC, Art. 1(3); Directive (EU) 2019/790, Art. 14.
[117] Agreement on the Trade-Related Aspects of Intellectual Property Rights as Amended by the 2005 Protocol Amending the TRIPs Agreement, Art. 9(2). Also see: Directive 2009/24/EC, Art. 1(2).
[118] Berne Convention for the Protection of Literary and Artistic Works, Art. 5.
[119] Ibid, Art. 6bis.

The use of copyright-protected work, however, is not restricted to the transfer of copyright or the voluntary licensing of copyright by the copyright owner. The EU copyright acquis and the national copyright legislations of the EU Member States consist of several exceptions and limitations (E&Ls) to copyright, which facilitate the use of copyright-protected works in certain special cases (e.g. for research purposes) without the authorization of and, often, remuneration of the copyright owner.[120] Additionally, the EU and national legislative frameworks have other mechanisms to achieve the same result, such as compulsory licenses tailored for certain uses of copyright-protected works. Last but not last, copyright does not confer eternal economic rights to its holder. As a general rule, copyright lasts during the lifetime of the author and at least an additional fifty-year post-mortem.[121] Once this term of protection is over, the work in question falls into the public domain and can be freely used by anyone.

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

3.4.1.1. Software Directive

Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs, or the so-called Software Directive, was adopted on 14 May 1991 in order to ensure the protection of software by copyright in all the EU Member States. The Directive was expected to be transposed to the national laws of the Member States by 1 January 1993.[122] The Directive had retrospective effect, without prejudice to any acts concluded and rights acquired before this date[123].

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

The Software Directive of 1991 was later codified by Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs, which entered into force on 25 May 2009[124].

As revised, the Software Directive applies to computer programs "in any form, including those which are incorporated into hardware"[125] as well as the "preparatory design work leading to the development of a computer program"[126]. In line with the general principles of copyright law, the Software Directive provides legal protection to the expression of a computer program. For the same reason, "the ideas and principles which underlie any element of a program, including those which underlie its interfaces"[127] – hence, the logic, algorithms and programming languages – are neither eligible for nor protected by copyright under the Software Directive[128].

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

3.4.1.2. Database Directive

Directive 96/9/EC of 11 March 1996 on the legal protection of databases entered into force on 16 April 1996, and the Member States were required to transpose the Directive to their national laws by 1 January 1998.[129]. The Directive was amended by the CDSMD in 2019.

As amended, the Database Directive defines a database as "a collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means"[130]. Broadly articulated as such, this definition encompasses databases available in any form, including online and offline databases[131]. However, computer programs involved in the making or operation of such databases are excluded from the scope of the Database Directive[132].

---

[124] Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs (Codified version) (Text with EEA relevance) *OJ L 111, 5.5.2009, pp. 16–22*

[125] Ibid, Recital 7.
[126] Ibid.
[127] Ibid, Art. 1(2).
[128] Ibid, Recital 10.
[129] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases *OJ L 77, 27.3.1996, pp. 20–28*, Art. 16(1).
[130] Ibid, Art. 1(2).
[131] Ibid, Art. 1(1).
[132] Ibid, Art. 1(3).

The Database Directive regulates the legal protection of databases by copyright or by sui generis rights, with respect to their defining characteristics. Databases that are original in their structure and arrangement are protected by copyright,[133] whereas databases that required qualitatively or quantitatively substantial investments in the collection, verification and organization of their materials are protected by sui generis rights[134]. Copyright protection entails the bundle of economic and moral rights indicated above; whereas the sui generis protection comprises the rights for extraction and re-utilization, which respectively refer to "the permanent or temporary transfer of all or a substantial part of the contents of a database to another medium by any means or in any form"[135] and "making available to the public all or a substantial part of the contents of a database by the distribution of copies, by renting, by on-line or other forms of transmission"[136]. Copyright protection applies to databases created before 1 January 1998,[137] while the sui generis protection extends to databases completed from 1 January 1983[138].

As emphasized by the Database Directive, the copyright and sui generis protection envisaged for databases do not extend to works and other subject-matter (such as personal and non-personal data, public sector information, open data and the like) contained in the databases.[139] The works and other subject-matter compiled under the copyright-protected or sui generis-protected databases might be subject to disparate and multiple legal regimes (such as GDPR, Open Data Directive as well as copyright, patent, trade secrets, industrial design rights, and legal norms on unfair competition).

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

3.4.1.3. Information Society Directive (InfoSoc Directive)

Directive 2001/29/EC of 22 May 2001[140] on the harmonisation of certain aspects of copyright and related rights in the information society, or the so-called InfoSoc Directive, is the cornerstone of the EU copyright framework, as it represents the most comprehensive harmonization intervention on EU copyright law. Due to this, the InfoSoc Directive encompasses a wide spectrum of copyright-related matters, including the technological protection measures (TPMs) and digital rights management (DRM) systems, while also containing the largest set of copyright flexibilities introduced in the EU copyright acquis so far. In this regard, the InfoSoc Directive is essential for the BRIEF activities since it is the main - or the prominent - EU instrument that helped the EU and its Member States to adapt their copyright regimes to the particularities of the digital era and the technological advancements. In fact, the mandatory E&L to facilitate temporary reproduction, enshrined in Article 5(1) of

[133] Ibid, Art. 3(1).
[134] Ibid, Art. 7(1).
[135] Ibid, Art. 7(2)(a).
[136] Ibid, Art. 7(2)(b).
[137] Ibid, Art. 14(1).
[138] Ibid, Art. 14(3).
[139] Ibid, Artt. 1(3), 3(2).
[140] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society *OJ L 167, 22.6.2001, pp. 10–19.*

the InfoSoc Directive, still constitutes the lynchpin of researchers' and ROs' time- and cost-efficient endeavours to train AI models by using copyright-protected works.

The InfoSoc Directive entered into force on 22 June 2001,[141] with a deadline set for 22 December 2002 for the Member States' implementation of the Directive into their national laws.[142] The operational text of the Directive was modified first, in 2017, by the Marrakesh Directive, and then, in 2019, by the CDSMD. As amended, the Directive applies to works and other subject-matter protected by copyright or related rights,[143] yet without prejudice to acts concluded and rights acquired before this date[144].

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

Directive (EU) 2019/790 of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (CDSMD)[145] entered into force on 7 June 2019. The Member States were given time to transpose the Directive into their national laws by 7 June 2021[146]. Despite the significant delays in the process, the transposition of the CDSMD was finalized in 2023.

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

3.4.1.5. Term Directive

Directive 2006/116/EC of 12 December 2006 on the term of protection of copyright and certain related rights (Term Directive)[147] is also worth noting in the context of the BRIEF activities, given that this Directive is aimed at harmonizing the duration of the legal protection granted upon copyright-protected works as well as the duration of the legal protection provided for other subject-matter (first fixations of films, phonograms, broadcasts, performances) protected by related rights (rights of film producers, phonogram producers, broadcasting organisations, and performers).

The Term Directive is of particular importance for two main reasons. First, it contours the borders of the public domain, which, in its broadest terms, refers to the sum of works and other subject-matter that are not protected by copyright or related rights or materials as such whose

[141] Directive 2001/29/EC, Art. 14(1).
[142] Ibid, Art. 13.
[143] Ibid, Art. 10(1).
[144] Ibid, Art. 10(2).
[145] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (Text with EEA relevance.) PE/51/2019/REV/1 *OJ L 130, 17.5.2019, pp. 92–125.*
[146] Directive (EU) 2019/790, Art. 29.
[147] Directive 2006/116/EC of the European Parliament and of the Council of 12 December 2006 on the term of protection of copyright and certain related rights (codified version) *OJ L 372, 27.12.2006, pp. 12–18*

copyright protection has lapsed. Therefore, the public domain is a generic term to collectively refer to the materials that can be used, in theory, without authorization and payment of royalties/fees. Second, the Directive crystallizes the rules regarding the duration of the economic and moral rights of the authors and creators of original works. Therefore, this Directive is essential for researchers and research organisations involved in the BRIEF network to contemplate the term of their copyright over their prospective scientific output.

3.5.2. Patent

Patent, also in its broadest terms, is a document issued, upon application, by the competent authority (often an industrial property office) which, on the one hand, consists of the detailed description of an invention and, on the other hand, provides a legal monopoly in favour of the applicant, as the patent owner, to prevent the unauthorized commercial exploitation of the patented invention.[148] The term "invention", in this context, refers to "a solution to a specific problem in the field of technology"[149], which may relate either to a product or a process.

To be eligible for legal protection originating from a patent, an invention shall meet certain criteria. These criteria comprise **(1)** the existence of a patentable subject-matter, **(2)** the industrial applicability of the subject-matter, **(3)** the novelty of the subject-matter, **(4)** the existence of a sufficient inventive step, also known as the "non-obviousness" of the subject-matter, and **(5)** the disclosure of the invention in the patent application.[150]

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

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

3.5.3. Trade secrets

Trade secrets, also known as know-how or undisclosed information, are broadly articulated by the EU legislator as "valuable know-how and business information that is undisclosed and

[148] WIPO Intellectual Property Handbook.
[149] Ibid.
[150] WIPO Intellectual Propery Handbook.

intended to remain confidential"[151]. Therefore, trade secrets differ from the other forms of IPRs due to their holders' interest in preventing them from becoming available to the public, whereas IPRs such as patent and design rights require registration of the invention and the design to secure a legal monopoly to appropriate them for a limited period of time. In this regard, the legal protection envisaged for trade secrets constitutes an alternative to patent and design rights whilst enabling the appropriation of the results of research and innovation. Due to this, trade secrets are acknowledged by the EU legislator as "the currency of the knowledge economy"[152] given the economic value and the competitive advantage they provide to their holders, especially in innovative industries and fields.

3.5.3.1. Trade Secrets Directive

Directive (EU) 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (Trade Secrets Directive)[153] entered into force on 5 July 2016[154]. The EU Member States were required to transpose it to their national laws by 9 June 2018[155].

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

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

[151] Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use or disclosure [2016] OJ L 157/1, Recital 1.
[152] Ibid.
[153] Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (Text with EEA relevance) OJ L 157, 15.6.2016, pp. 1–18.
[154] Directive (EU) 2016/943, Art. 20.
[155] Ibid, Art. 19(1).

3.5.4. Industrial design

Industrial design is yet another conventional form of IPR which protects the ornamental and non-functional features of an article or product.[156] In other words, it is not the article or the product, but the design embodied in such article or product that is protected by industrial design rights.[157] The design that is subject to the industrial design rights may be two-dimensional as well as three-dimensional, including those generated with the aid of 3D-printing technology. Nevertheless, not every design is eligible for legal protection. In principle, "designs dictated essentially by technical or functional considerations"[158] are carved out of the scope of legal protection envisaged for industrial designs. Additionally, designs that do not meet the novelty threshold set by the applicable law would also not be entitled to legal protection.[159]

In the EU, the acquisition of design rights, in principle, requires the registration of the design to the competent intellectual/industrial property office of the State in which legal protection is sought. However, the Community Design Regulation also acknowledges legal protection, with a more restricted term of protection, to unregistered designs. Indeed, the Union's IP framework envisions a five-year legal protection, renewable up to 25 years,[160] for registered designs and three-year protection unregistered ones.[161]

During the term of legal protection, the rightsholder holds the exclusive right to use and prevent third parties from using the design in question.[162] Whereas the design rightsholder will be the only one to use, also to commercially exploit, the design through the sale, import, or export of products bearing the design or by licensing or transferring the design rights, with the lapse of the term of legal protection the design will become part of the public domain to be freely used by anyone.

3.4.4.1. Design Directive

Directive 98/71/EC on the legal protection of designs (Design Directive) is one of the two EU legislations that set the legal framework for industrial designs at the Union level. Entered into force on 17 November 1998[163] and had to be implemented in the national laws of the Member States by 28 October 2001,[164] the Design Directive harmonises the design protection legislation of the Member States by setting the Union standards. To do so, it provides a unitary definition for the term "industrial design", clarifies the legal consequences of the registration of industrial designs, approximates the eligibility criteria to grant legal protection to industrial designs and sets the scope and term of such legal protection as well as the limitations to the exclusive rights of the industrial design holder to enable the use of registered designs in certain special cases.

---

[156] WIPO Intellectual Property Handbook.
[157] Ibid.
[158] Agreement on the Trade-Related Aspects of Intellectual Property Rights, Art. 25(1).
[159] Ibid, Art. 25(1); Directive 98/71/EC, Art. 4.
[160] Council Regulation (EC) No 6/2002, Art. 12.
[161] Ibid, Art. 11.
[162] Agreement on the Trade-Related Aspects of Intellectual Property Rights, Art. 26(1).
[163] Directive 98/71/EC, Art. 20.
[164] Ibid, Art. 19.

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

The Design Directive[165] adopted on 23 October 2024, represents a significant recast of Directive 98/71/EC concerning the legal protection of designs within the European Union. The new directive aims to modernise and harmonise substantive and procedural aspects of design law across Member States, thereby enhancing the internal market's functioning and supporting innovation. It reflects the EU's broader intellectual property strategy and responds to calls from both the Council and the European Parliament to make design protection more accessible, particularly for SMEs. The directive introduces clearer definitions of "design" and "product", accommodates digital and animated designs, and reinforces the principle of cumulation with copyright protection.

A key objective of Directive 2024/2823 is to align national and EU-level design protection systems, ensuring legal certainty and reducing fragmentation. It establishes minimum procedural standards for design registration and invalidation, while allowing Member States flexibility in its implementation. The directive also addresses the visibility requirement for design features, clarifies the scope of protection for component parts of complex products, and promotes the interoperability of design registers. By updating the legal framework in light of technological developments and market needs, the directive seeks to foster competitiveness, facilitate the free movement of goods, and strengthen the EU's position in global design innovation.

3.4.4.2. The Community Design Regulation and the EU Design Regulation

Last but not least, Council Regulation (EC) No 6/2002 on Community designs (Community Design Regulation), which entered into force on 6 March 2002,[166] shall be briefly mentioned herein for it sets the rules concerning the registration of an industrial design to the European Union Intellectual Property Office (EUIPO) (previously known as the Office for Harmonization in the Internal Market (OHIM)) in order to secure legal protection within the borders of the EU. The Regulation tackles the procedural aspects of the legal framework revolving around industrial designs as it regulates the steps to register a design to the EUIPO and the legal consequences of the acceptance or rejection of such an application. Additionally, it sets the Union rules on the legal protection provided to unregistered industrial designs.

In this regard, the Regulation, mainly, provides the procedural details for EU-wide legal protection which co-exists with the national legal protection that stems from the registration of the design to a national intellectual/industrial property office. Whereas the legal protection

[165] Directive (EU) 2024/2823 of the European Parliament and of the Council of 23 October 2024 on the legal protection of designs (recast) (Text with EEA relevance) PE/97/2023/REV/1. OJ L, 2024/2823, 18.11.2024

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

envisioned in the latter case remains within the borders of the State in which the design is registered, registration of the design to the EUIPO secures the protection and enforcement of the rights of the industrial design holder across the EU.

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

The EU Design Regulation,[167] adopted on 23 October 2024, amends the Community Design Regulation. The regulation updates the legal framework for the protection of designs at the EU level, now referred to as "EU designs" rather than "Community designs" and aligns terminology with the Lisbon Treaty and Regulation (EU) 2017/1001 on EU trademarks. It introduces substantive and procedural changes to improve accessibility, legal certainty, and enforcement, particularly in light of technological developments such as digital design, 3D printing, and AI-assisted creation. The regulation also strengthens the role of the European Union Intellectual Property Office (EUIPO) in promoting awareness and convergence of practices across Member States.

The reform was prompted by a comprehensive evaluation of the EU design protection system, which revealed that while the system was largely fit for purpose, it required updates to remain effective and relevant in a rapidly evolving innovation landscape. The European Commission, supported by the Council and the European Parliament, identified several areas needing improvement: simplification of procedures, better alignment with national systems, enhanced protection against counterfeiting, and clearer rules for emerging design formats. The regulation responds to these needs by broadening the definition of protectable designs to include non-physical and animated features, clarifying visibility requirements, and introducing new enforcement tools—such as the ability to block infringing goods in transit. These changes aim to make design protection more attractive and accessible, especially for SMEs and individual designers, while ensuring that the EU remains competitive in global innovation ecosystems.

3.6. Cybersecurity

3.6.1. Cyber Resilience Act

The heightened awareness at the European level regarding the security risks emanating from the increased interconnectedness of devices was the catalyst for the adoption of the Cyber Resilience Act.[168] This challenge was first identified in the EU's Cybersecurity Strategy for

[167] Regulation (EU) 2024/2822 of the European Parliament and of the Council of 23 October 2024 amending Council Regulation (EC) No 6/2002 on Community designs and repealing Commission Regulation (EC) No 2246/2002 (Text with EEA relevance) PE/96/2023/REV/1. OJ L, 2024/2822, 18.11.2024

[168] Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act), OJ L, 2024/2847, 20.11.2024.

the Digital Decade,[169] which was presented in 2020. Subsequently, it was translated into a legislative intervention aimed at preventing and mitigating the impact of malicious attacks that can exploit vulnerabilities of any product connected online.

The CRA's primary focus is on **'products with digital elements'** available on the European market. Article 3(1) CRA stipulates that the latter is to be defined as "any software or hardware product and its remote data processing solutions, including software or hardware components to be placed on the market separately". It is imperative to emphasise that the ambit of the Regulation **does not apply to products incorporating digital components that are classified as medical devices**. This is a significant distinction that enables manufacturers of medical devices to prioritise the security and safety requirements stipulated in the Medical Device Regulation.[170]

Therefore, products incorporating digital components must adhere to the stipulated pre-market and post-market requirements as outlined by the CRA. The Regulation addresses both the design and development phases, as well as the monitoring and updating activities carried out after the product is available on the market.

It is incumbent upon manufacturers to **design, develop and manufacture any product with digital elements in such a way as to ensure an appropriate level of cybersecurity.** In order to achieve this, it is essential that no known exploitable vulnerabilities are present and that secure default configurations are available. The fundamental stipulations are delineated in Annex II, encompassing both security considerations and vulnerability management parameters. Within the initial category, the following measures are encompassed: security by default, confidentiality protection, integrity and availability of data and networks, data minimisation measures, resilience measures (particularly against DoS attacks), safeguards against network effects, records on internal activity, and data portability. Furthermore, products must incorporate adequate control mechanisms to ensure protection against unauthorised access. In addition, such mechanisms should be implemented to safeguard the confidentiality of the data to be protected. This may be achieved through the use of encryption techniques and other secure methods.

Manufacturers should prepare the requested **technical documentation prior to the release** of their products. This documentation must contain an assessment of the cybersecurity risks associated with the products, as well as a detailed description of the manufacturer's methods for meeting the essential cybersecurity requirements and mitigating the identified risks.

Upon completion of the **conformity assessment procedure**, the manufacturer is issued with a declaration of conformity for the product, thereby confirming its compliance with the requirements stipulated in Annex II.[171] The type of conformity assessment applied is contingent on the class of risk of the product in question. The range of assessments extends from internal control procedures to those based on full quality assurance. Nevertheless, the type of products encompassed by this analysis are excluded from the possibility of adopting an internal control procedure. According to Art. 7(2) CRA, a product with digital elements that "performs a function which carries a significant risk of adverse effects in terms of its intensity and ability

[169] Commission 'The EU's Cybersecurity Strategy for the Digital Decade' JOIN(2020) 18 final.
[170] Art. 2 (2) and recital 25 CRA.
[171] Art. 2 (2) and recital 25 CRA.

to disrupt, control or cause damage to a large number of other products or the health and safety of a large number of individuals through direct manipulation, such as a central system function, including network management, configuration control, virtualisation, processing of personal data", are qualified as important. Consequently, they are subject to the conformity assessment procedures stipulated in Article 32(2) and (3) CRA. Furthermore, point (19) of Annex III of the CRA encompasses 'personal wearable products to be worn or placed on a human body that have a health monitoring (e.g. tracking) purpose' within the category of Class I of the significant products.

It is essential to acknowledge that the obligations of manufacturers do not conclude with the declaration of conformity. The product is subject to **post-market surveillance controls by authorities** that have been specifically defined for this purpose. These authorities have the power to take all appropriate corrective actions, including bringing the product into compliance, withdrawing it from the market, or recalling it, and they are required to do so within a reasonable period. Furthermore, manufacturers are obligated to **inform the national Computer Security Response Team (CSIRT)**[172] of any vulnerabilities that have been exploited or incidents that have an impact on the security of the product within 24 hours of becoming aware of such events. The notification provides the essential information about the event, in addition to the corrective and mitigating measures that have been implemented. In the event that the deployment of corrective measures necessitates the collaboration of the user, it is imperative that the user be apprised of the incident.

3.6.2. NIS and NIS 2 Directives

The Network and Information Security Directive[173] is widely regarded as a cornerstone of European cybersecurity legislation. This was subsequently supplemented and replaced by the NIS 2 Directive.[174]

3.6.2.1. NIS

The original NIS Directive concentrated on two particular groups: **essential service operators (ESOs) and digital service providers (DSPs)**. Essential service operators encompass public and private entities that facilitate services of paramount importance for sustaining societal and economic activities within critical sectors. These sectors include, but are not limited to, energy, transportation, financial markets, healthcare, water distribution, and digital infrastructure. The ongoing provision of these services is contingent upon the secure and efficient functioning of their networks and information systems. The identification of ESOs is achieved through the implementation of specific procedures conducted by the competent authorities in each member state. Digital service providers comprise entities offering services such as e-commerce, cloud computing, and search engines.

---

[172] The CSIRT is the body designated according to the Directive 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive) [2022] OJ L 333/80.
[173] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016, pp. 1–30.
[174] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), OJ L 333, 27.12.2022, pp. 80–152.

The Directive imposes **significant obligations** on these entities. Firstly, the adoption of appropriate and proportionate security measures is imperative to **manage the risks associated with the security of networks and information systems**. The objective of this management is to mitigate the impact of potential incidents. Furthermore, they are required to inform the CSIRT (**Computer Security Incident Response Team**) of any incident that has a substantial impact on service continuity. As a complementary measure, Article 19 of Legislative Decree No. 65 of May 28, 2018[175]—implementing the directive in Italy—grants entities not classified as ESOs or DSPs the option to notify the CSIRT of incidents impacting their service continuity voluntarily.

3.6.2.2. NIS 2

While Member States were engaged in the process of implementing the NIS Directive, the Commission presented a new legislative instrument in December 2020. The purpose of this instrument was to replace the NIS Directive, to overcome some of the shortcomings of the latter. The objective of the NIS 2 Directive is to enhance security measures to safeguard the digital internal market. This is to be achieved by establishing **harmonised standards in the fields of cybersecurity risk management and incident reporting.** This approach is further substantiated by the **broadening of the scope of NIS 2**, which will consequently lead to an increase in the number of entities subject to the obligations and requirements.

It is important to stress that the present configuration of NIS 2 is predicated on the evaluation and reporting of the impact of the NIS directive. One of the earliest challenges to emerge from the configuration of NIS was the identification of the actors encompassed within the scope. NIS 2 differentiates between essential entities (EEs) and important entities (IEs) with minimal discrepancies in terms of reporting requirements and obligations. The identification criteria have been subject to alteration; the initial criterion is now **enterprise size,** with small and micro enterprises excluded from the scope of the legislation (Art. 2(1) NIS 2). While acknowledging that this criterion may not represent an optimal standalone metric for evaluating the importance and criticality of an entity, it serves as a notable indicator of entities that play pivotal roles within society and the economy.

It is evident that the text presents a comprehensive enumeration of **exceptions**, which are applicable irrespective of the company's size. In the following cases, for example, size is irrelevant:

- services provided by providers of public electronic communications networks or publicly accessible electronic communications services;
- services provided by providers of trust services;
- services provided by top-level domain name registries and domain name system service providers;
- services provided by entities that are the sole provider in a member state of a service essential to the maintenance of critical social or economic activities;
- services provided by entities that could have a significant impact on public safety, public security or public health; or
- services provided by public administration entities.

[175] DECRETO LEGISLATIVO 18 maggio 2018, n. 65. Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.

The second criterion pertains to the **undertaking of activities within one of the sectors delineated in Annexes I and II of NIS 2.** A notable aspect of NIS 2 is its substantial expansion of the scope of the NIS Directive, incorporating new sectors such as **telecommunications, social media platforms, and public administration.**

With regard to the matter of reporting requirements, NIS 2 employs a two-step approach to incident reporting, thereby overcoming the issues that have arisen in the implementation of NIS. During the first phase, the affected entity is required to **inform the national authority or CSIRT without delay, within 24 hours of becoming aware of an incident.** Subsequent to this, the aforementioned entity will furnish a comprehensive report within 72 hours of becoming aware of the incident. The second stage involves the full recovery of the problem, with a final report to be submitted one month after the initial report.

In terms of enforcement, the directive establishes a minimum list of **administrative fines** for cases where entities violate the cybersecurity risk management rules or notification requirements under NIS 2. These are then complemented by the powers provided for national authorities, which include the ability to issue warnings, adopt binding instructions, and implement recommendations (Art. 32(4) NIS 2).

4. CROSS-FIELD ANALYSIS

In the preceding section, the principal objectives of legislative initiatives pertaining to the EU data strategy, public health, product safety, artificial intelligence, intellectual property and cybersecurity were briefly outlined. This overview served to delineate regulatory boundaries across these sectors, thereby providing a rationale for the selection criteria employed in our analysis.
In the present section, we present the findings from the cross-sectoral analysis. This step aimed to identify, for each legislative initiative, the core characteristics and the ethical-legal principles pertinent to research, development, and innovation (R&D&I), with particular emphasis on data-driven research infrastructures involving robotic technologies—such as the BRIEF's Research Infrastructures.

EU/national legal framework	*Main principles applicable to BRIEF RI*
General Data Protection Regulation 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	The GDPR sets paramount guiding principles for the respect of the fundamental rights to privacy and data protection such as: • **Transparency:** individuals must be clearly informed about how and why their personal data are being used. This enables them to exercise their rights effectively. • **Lawfulness:** data processing must rely on a valid legal basis (e.g. consent, contract, legal obligation). Without it, the processing is considered unlawful. • **Fairness:** personal data must not be used in ways that are unjustifiably harmful, discriminatory, misleading, or unexpected.

	• **Purpose limitation:** data must be collected for specific, explicit, and legitimate purposes. It cannot be reused for incompatible purposes. • **Data minimization:** only data that are strictly necessary, relevant, and adequate for the intended purpose should be collected and processed. • **Storage limitation:** personal data should be kept in identifiable form only for as long as necessary. Afterwards, they must be deleted or anonymized. • **Accuracy:** data must be kept accurate and up to date. Inaccurate data should be corrected or erased without delay. • **Integrity and confidentiality:** data must be protected against unauthorized access, unlawful processing, and accidental loss or damage. • **Accountability:** the data controller is responsible for complying with these principles and must be able to demonstrate such compliance. • **Data protection by design and by default:** the data controller has the obligation of integrating privacy and data protection principles into the design of systems, processes, and technologies from the outset. It ensures that only necessary personal data are processed, access is limited, and safeguards are in place by default—without requiring user intervention. **Pseudonymization** techniques constitute technical measures that can be adopted by research institutions to implement data minimization and data protection by design and by default. They ultimately serve to demonstrate accountability. The selection of the most appropriate technique(s) depends on the risk assessment that is carried out on the particular data processing operation performed during a research activity and cannot be simply determined in a standardized format. This is particularly important for the use and re-use of health data.
Italian Code of Privacy D. lgs 193/2003 updated with D.lgs. 101/2018, as amended by L.D. 37/2024 **Italian Data Protection Authority provisions** implementing and /or clarifying some aspects of the GDPR	The Italian Codice Privacy and the Italian DPA's provisions foresee that : • Article 110 permits processing **health data for scientific research without consent when justified by law and appropriate safeguards**, such as a Data Protection Impact Assessment (DPIA). Since 2024, prior consultation with the Garante is no longer required. The provision of 5.6.2019 permits the secondary use of health data for research purposes without consent, subject to ethical or organizational constraints. It requires safeguards, including data minimization and anonymization. Consent may be waived if informing subjects risks harming them, is

	unfeasible, or would compromise research. A **DPIA and ethical oversight** remain mandatory • The 2024 update to the deontological rules requires ethical approval, a DPIA, and justification when consent is unobtainable due to ethical or organizational reasons**. Data subjects must be clearly informed, anonymization is preferred, and public disclosure is required** if direct contact is impractical. Universities must ensure compliance with these safeguards when they process biomedical data • Article 110-bis allows **the Garante to authorize data reuse for research when informing data subjects is impossible or delays would hinder the study.** A DPIA and safeguards, such as anonymization, are required. The Garante may issue case-specific decisions or general provisions for certain data controllers or processing types. • **Broad consent** is valid only when specific research purposes are initially unknown; later, specific consent must be obtained once the study's aims are clearly defined ("consenso a fasi progressive")
Open Data Directive Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information	The ODD plays a crucial role in European policies concerning open science, particularly in its focus on the **re-use of research data**. • Public data designates documents generated and gathered by public sector bodies, but the ODD expands this traditional definition also to include research data. • Article 10 encourages the **availability of research data generated through public funding**, promoting transparency, reproducibility, and broader access for scientific advancement. • Article 10 also requires Member States to develop **national open access policies** for publicly funded research data, aligned with the FAIR principles (Findable, Accessible, Interoperable, Reusable). Policies should follow the principle "as open as possible, as closed as necessary", balancing openness with considerations of IP rights, personal data, security, and commercial interests. Member States must define key aspects of open access policies, including scope, embargo periods, opt-out options, and the criteria for repository openness. • The ODD identifies **high-value datasets** that can support innovation, including AI applications, and enhance public sector activities. These datasets must be free, machine-readable, accessible via APIs, and accompanied by metadata and documentation.

	Italy's **Piano Nazionale per la Scienza Aperta (PNSA)**, adopted via Ministerial Decree No. 268/2022, is the country's main institutional response to Open Science and implements Article 10 of the ODD. The PNSA is part of the **National Research Programme (PNR) 2021–2027** and is supported by a Working Group established in 2023, which produced an assessment of the current state of Open Science in Italy in 2024. This assessment provides a **starting point** for sustainable implementation, identifying existing resources and gaps to be addressed.
Data Governance Act 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	The DGA aims to effectively create a data governance system among public institutions, companies, research organizations, NGOs and citizens, promoting mechanisms of data sharing and reuse, including "data altruism". The DGA's main aspects that are relevant for scientific research are: • **Facilitated access to protected public sector data:** the DGA enables the reuse of public sector data that are protected (e.g. personal data, IP-protected content, confidential commercial or statistical data), expanding the pool of data available for research. • **Privacy and security safeguards**: public bodies must implement tools that ensure anonymity, confidentiality, and security when sharing personal data. Sector-specific authorities may support them with technical solutions. • **Trusted data intermediaries**: the DGA introduces data intermediaries—neutral entities that facilitate data sharing between holders and users (e.g. researchers), under strict rules prohibiting the use of data for their own purposes. • **Data altruism for general interest purposes**: individuals can voluntarily share personal data (e.g. health data) for purposes such as scientific research, via data altruism organizations. These must be non-profit, registered, and compliant with EU transparency and security standards. • **Consent and transparency mechanisms**: data sharing must be based on informed consent (for personal data) or permission (for non-personal data). Organizations must maintain access logs, publish annual reports, and use standardized consent forms. • **Integration into European Data Spaces:** the DGA provides a framework for cross-sectoral data flows within European data spaces (e.g. health, mobility, finance), which sector-specific regulations like the European Health Data Space will complement.

Data Act
Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828
	The Data Act is an horizontal regulation on connected products and related services. In theory, it will apply to all IoT objects also used for e-health purposes.
	• **Access to IoT and app-generated data**: researchers may access data—including personal, non-personal, and metadata—generated by connected products and related services, as long as the use does not compete with the original product.
	• **Structured data sharing contracts**:
	  ○ B2C/B2B contracts: users can request access to their data or authorize third parties (e.g. research institutions) to access it.
	  ○ B2G contracts: public bodies may request access to data in emergencies or when needed to fulfill public interest tasks, including scientific research.
	• **Fair compensation for data access**: non-profit research organizations, micro-enterprises, and SMEs can access data at cost, meaning they only pay for the expense of making the data available.
	• **Emergency data sharing for research**: in exceptional circumstances (e.g. pandemics), public bodies may access data from private entities and share it with research-performing or funding organizations, provided the use aligns with the original purpose.
	• **Interoperability and data spaces:** the DA promotes harmonized standards, shared vocabularies, and technical requirements to enable data flow across data spaces—facilitating collaborative and cross-border research.

European Health Data Space Regulation Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847	The EHDS Regulation is a vertical regulation that is interrelated with the DGA. It lays down the conditions for primary and secondary use of health data. The following key aspects of secondary use are of particular relevance for scientific research activities: • **Legal basis for secondary use of health data**: for data users, the EHDS provides a legal basis for secondary use of health data under Article 9(2) GDPR, including safeguards. Scientific research is explicitly listed among the permitted purposes (Article 53(1)). For data holders, it provides a legal obligation to share data once a data permit is issued (see below). Still a legal basis under art. 6 GDPR. • **Prohibited uses of health data**: five categories of secondary use are prohibited, including discrimination, advertising, and development of harmful products, ensuring ethical boundaries for research. **Access procedures for researchers**: researchers can obtain access to health data through:

	○ Data permits: a formal application process involving ethical and security assessments, with permits generally valid up to 10 years. ○ Requests for anonymised statistical data. ○ Access via HealthData@EU infrastructure for EU institutions and research infrastructures. • **Secure processing environments** (SPEs): data must be accessed in SPEs that ensure GDPR compliance, protection of intellectual property, confidentiality, and cybersecurity. The health data access body retains control over data processing actions within the SPE. • **Right to opt-out and exceptions**: individuals can opt out of secondary data use. However, national laws may allow access in specific public interest cases, especially for research, if no alternative data sources are available. The EHDS facilitates access to datasets like medical images for training and validating AI-based tools, supporting innovation in medical decision-support systems.
Clinical Trials Regulation 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	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 database.**
National implementation of Clinical Trials Regulation into the Italian discipline: 26, 27, 30 January 2023 decrees and AIFA determination 424/2014	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, i.e., the 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; now GDPR • 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). AIFA Determination 424/2024: aims to simplify and decentralize clinical trial procedures in Italy, aligning with the CTR and adapting to technological and organizational innovations. The key aspects are: • Defined roles and responsibilities: sponsors, principal investigators (PIs), and third-party service providers must have clearly documented roles. The PI retains ultimate medical responsibility, even when tasks are outsourced • Use of third-party service providers: external providers may support trial activities (e.g. home delivery of investigational drugs, remote procedures), but must be properly trained and integrated into the trial framework

	• Data protection compliance: when handling sensitive participant data, third-party providers must be formally designated as data processors under the GDPR. The data controller (either the sponsor or healthcare facility) must ensure appropriate technical and organizational safeguards • Contractual clarity: contracts must explicitly define each party's obligations, especially regarding data privacy and security. PIs must be informed in advance of any third-party involvement.
Medical Devices Regulation 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	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 the following points: • **Risk-based classification and certification:** medical devices are classified by risk (Classes I to III), which determines the level of scrutiny and certification required. This affects research involving investigational devices, especially high-risk ones. • **Role of notified bodies:** independent EU-registered bodies assess compliance and grant CE marking. Their involvement is crucial for researchers developing or testing new devices. • **Post-market surveillance:** manufacturers must monitor device performance after market entry. This supports evidence generation and long-term safety studies in clinical research. • **Recognition of software as medical devices:** software can qualify as a medical device under certain conditions, relevant for research involving digital health tools, algorithms, or AI-based diagnostics. • **Clinical evidence requirements:** stricter rules apply to clinical investigations, including coordinated EU-wide procedures for multi-centric trials. This enhances consistency and reliability in research outcomes. • **Transparency and traceability:** the MDR introduces a centralized EU database and unique device identification system, improving access to device-related data for research and regulatory analysis. • **Regulatory harmonization:** the MDR applies uniformly across Member States, reducing legal fragmentation and facilitating cross-border research collaborations. • **Timeline:** fully applicable since 26 May 2021; therefore, it is extremely important that medical device producers comply with these rules and monitor both the Italian Health Ministry and the Medical Devices

	Coordination Group for more info on conformity procedures at a national and EU level .
CE Marking Regulation 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	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 for clinical investigation for medical devices not bearing the CE marking referred to in Article 16, paragraph 2 of Legislative Decree No. 137 of 2022. (G.U. General Series, no. 136 of 13/06/2023)	A) **CE marking**: it concerns: • official communication for products bearing the CE marking until the EUDAMED database is fully operational (communications are officially addressed at the Italian Health Ministry). • The documentation sent must be compliant with the MDR requirements. • The official communication to the Health Ministry must happen after an Ethical Committee approval (local, CET, or national CEN) • Communication of the trials beginning within 30 days to the competent authority B) **no CE marking**: it concerns: • official communication for products not bearing the CE marking until the EUDAMED database is fully operational (communications are officially addressed at the Italian Health Ministry) • legal entities/subjects habilitated to officially communicate information to the Italian Health Ministry is the sponsor • official communication for products bearing the CE marking until the EUDAMED database is fully operational (communications are officially addressed at the Italian Health Ministry) • The request for the start of clinical trials are done after having acquired a favourable opinion of an Ethical Committee (local, CET, or national CEN) • The sponsor communicates the beginning of the trial promptly to the competent authority.
Machinery Regulation	The MR is important for the BRIEF project because:

Regulation (EU) 2023/1230 of the European Parliament and of the Council of 14 June 2023 on machinery and repealing Directive 2006/42/EC of the European Parliament and of the Council and Council Directive 73/361/EEC	• It can apply to parts of the devices built if they fall in its field of application (such as motor transmission parts or security software) • It creates a set of rules and procedures to follow based on a risk-assessment rationale in order to obtain the CE marking • It is important as it sets in its Annex II essential health and safety requirements which, if not respective, might trigger a product liability claim • The fact that it also applies to security software makes it possible that, as far as software is concerned, the AI Act regime for high-risk AI system will need to be applied at the same time with the MR requirements
Product Liability Directive Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products **Product Liability Directive Update** Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products and repealing Council Directive 85/374/EEC	The PLD is the main liability regime that is applicable as a consequence of non-compliance with the MDR, MR and AI Act duties whenever a connected object and software are involved. The PLD is being updated to address challenges posed by AI, robotics, and IoT, such as the difficulty in identifying the producer, challenges in proving causality, especially with long-term effects and uncertainty about whether to rely on EU or national liability regimes. 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. From 9 December 2026, the PLDU will apply. Researchers need to be cognizant of the following elements: • **Expanded definition of manufacturer**: the PLDU broadens liability to include software developers, AI providers, refurbishers, and other actors in complex value chains. Researchers involved in developing or modifying digital products may be considered manufacturers and thus subject to liability. • **Improved access to evidence and presumptions**: the PLDU introduces mechanisms to ease the burden of proof for claimants, including judicial access to technical documentation (Article 9) and the use of legal presumptions (Article 10). These are relevant for researchers working on complex or opaque technologies like AI and IoT. • **Updated risk development exemption**: the exemption now depends on the objective state of scientific knowledge, not the manufacturer's subjective awareness. Scientific publications and expert consensus are key references, which are important for researchers contributing to or relying on cutting-edge knowledge.

	• **Broader scope of compensable damage**: the PLDU removes monetary thresholds for property damage and includes psychological harm. However, damage to professional-use property or data is excluded. • **Extended limitation periods**: claimants have 3 years to initiate proceedings and up to 25 years in cases of latent damage. This point is relevant for long-term research involving health or environmental risks. • **Residual liability mechanisms**: if no liable party can be identified, Member States may establish compensation funds—ensuring protection for users of research-based technologies.
Artificial Intelligence Act Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828	The AI Act is the world's first binding law on artificial intelligence that establishes the European framework for the development and deployment of artificial intelligence systems whenever they are put into service or commercialized within the European Union. It is a complex piece of legislation that includes provisions on: • AI systems definition as software (primarily); • Risk classification of AI systems, encompassing prohibited, high-risk and low-risk AI systems; • Prohibited systems such as systems that use manipulative, deceptive and subliminal techniques, that exploit vulnerabilities, that implement emotion recognition and biometric categorization, social scoring and predictive policing; • General-purpose AI systems have general transparency obligations, combined with additional requirements e.g., on risk assessment and mitigation whenever they pose systemic risks; • Compliance requirements for high-risk AI systems such as risk assessment, transparency, accuracy, data governance, human oversight There are specific **exemptions** applicable to AI **systems developed and used exclusively for scientific research** which are very relevant for BRIEF's activities. This includes activities prior to market placement or deployment, but excludes real-world testing, which must comply with the regulation (Article 2(8)). Market placement and deployment are defined as: • Placing on the market refers to making an AI system available as part of a commercial activity, even if free of charge (e.g. via API, cloud, or download). • Putting into service means first use by a deployer or for internal use, including in-house deployment.

	These definitions clarify when research transitions into regulated activity, especially relevant for spin-offs or collaborative projects. However, if AI systems developed in research are later commercialized or deployed (e.g. as medical devices), they must comply with the AI Act's requirements, particularly those for high-risk systems. This is why researchers should document decisions during development to support future compliance, especially regarding transparency, data governance, and human oversight. Even exempt research must follow ethical guidelines, data protection laws, and the European Code of Research Integrity, which emphasizes reliability, honesty, respect, and accountability. Researchers are encouraged to follow the EU's seven principles for **trustworthy AI**: • Accountability • Human agency and oversight • Technical robustness and safety • Privacy and data governance • Transparency • Diversity, non-discrimination and fairness • Environmental and social well-being **Real-world testing** must follow specific rules and be conducted under the supervision of competent authorities. Regulatory sandboxes offer a controlled environment for experimentation, but require compliance with national and EU laws.
Interoperable Europe Act Regulation (EU) 2024/903 of the European Parliament and of the Council of 13 March 2024 laying down measures for a high level of public sector interoperability across the Union	Particularly noticeable are: • The obligation for the public infrastructure to have an interoperability assessment • The obligation for a Union or public sector body to share its own interoperability measures so that other Union or national public sector bodies can re-use them • The Commission's obligation to share its interoperable Europe solutions on a dedicated portal
Software Directive Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs (Codified version)	The Software Directive, whilst harmonising the EU Member States' national copyright laws, **clarifies the scope of copyright protection for software, the authorship of software, the exclusive rights** conferred to the copyright owner of the software, the E&Ls introduced to the exclusive rights of the copyright owner of the software, and the special measures of protection envisioned for the software.

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

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

	of databases, the exclusive rights over databases and the E&Ls to such rights, as well as the term of protection for the sui generis rights. The following can be presented as the highlights of the Database Directive, which are also of crucial importance for the BRIEF activities: • The **author of a database can be a natural person or a group** of natural persons. In the latter case, the exclusive rights deriving from database authorship shall be jointly exercised by the members of the group. • In the Member States whose legislative framework permits, a legal entity may, as well, be designated as the author hence the rightsholder of the database • According to Article 5 of the Database Directive, the author of a copyright-protected database would have the **following exclusive rights:** o temporary or permanent reproduction by any means and in any form, in whole or in part; o translation, adaptation, arrangement and any other alteration; and the reproduction, distribution, communication to the public, display or performance to the public of the results of the aforementioned acts; o distribution to the public of the database or of copies thereof, o any communication, display or performance to the public. • Article 6(1) of the Directive introduces a mandatory exception or limitation (E/L) to the copyright of the database author in favour of **lawful users** of a database or of a copy thereof. This provision allows the performance of any of the acts covered by the above-mentioned exclusive rights of the database author, without seeking authorization, however only for the purposes of access to and normal use of the contents of the database. When the lawful user is authorized to use only part of the database, the provision applies only to that part. • Additionally, Article 6(2)(b) of the Directive introduces another E/L to copyright, specifically, for **research purposes**. Indeed, this provision holds that the Member States can adopt laws to permit "the use of databases for the sole purpose of illustration for teaching or scientific research, as long as the source is indicated and to the

	extent justified by the non-commercial purpose to be achieved". • As to the scope of sui generis rights, Article 7 of the Directive refers to two rights**: extraction**, which refers to "the permanent or temporary transfer of all or a substantial part of the contents of a database to another medium by any means or in any form", and **re-utilisation** which stands for "any form of making available to the public all or a substantial part of the contents of a database by the distribution of copies, by renting, by on-line or other forms of transmission". • Article 8 of the Directive provides an E/L to **sui generis rights in favor of the lawful user** of such a database. It permits the lawful user of the database to extract and/or re-utilize insubstantial parts of its contents, evaluated qualitatively and/or quantitatively, for any purposes. Where the lawful user is authorized to extract and/or re-utilize only part of the database, these actions can be performed only to that part. • Additionally, Article 9(b) of the Directive introduces an optional E/L to sui generis rights. It allows the lawful user to **extract a substantial part of the contents of a database, without the authorization** of the database maker, for the purposes of illustration for teaching or scientific research. However, such practices shall be accompanied by the indication of the sources of the database, and they shall be performed for non-commercial purposes. • It shall be underlined that the copyright or sui generis protection envisioned for the databases **does not extend to the contents of the database.** Indeed, the contents of the database might be subject to different sets of norms, including but not limited to IPRs and data protection. • The term of legal protection for copyright-protected databases is subject to the general rules encompassed within the Term Directive, whereas the legal protection for sui generis is regulated in detail in Article 10 of the Database Directive. Setting the main rule, Article 10(1) of the Directive grants **15 years of legal protection** to such databases. This term shall be calculated from the 1st of January of the year that follows the date of the completion of the making of the database. • Article 10(3) of the Directive includes a provision that can be an incentive for database makers, given that it

	acknowledges that **any substantial change** executed on the contents of the database might lead to a new **database eligible for sui generis protection** if such alteration is considered to be a substantial new investment.
InfoSoc Directive Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society	The InfoSoc Directive is one of the building blocks of the EU copyright legislation due to constituting the EU's first comprehensive attempt to **harmonize the key economic rights** of copyright holders whilst introducing a set of mandatory and optional E&Ls to these exclusive rights. In this context, Article 5(1) of the InfoSoc Directive, which comprises the only mandatory E/L to copyright within the Directive, is of significant importance to research activities that involve AI technologies as this provision is deemed to **facilitate training AI models with copyright-protected works and other legally protected subject-matter** without any infringement and without having to seek authorization from the rightsholders. • Article 5(1) of the Directive obliges the Member States to adopt an E/L which would **restrict the exclusive right to reproduction** of authors, performers, phonogram producers, film producers, and broadcasting organisations. • The provision permits **temporary acts of reproduction,** which are transient or incidental, and which are an integral and essential part of a technological process, for the sole purpose of enabling transmission in a network between third parties by an intermediary or for the lawful use of a work or other-subject matter. • The temporary reproduction of a work, fixation of a performance, phonogram, cinematographic work, or the fixation of a broadcast can be made **by any means and in any form, in whole or in part, and it shall not have any independent economic significance.** Additionally, the InfoSoc Directive introduces **Union standards** to prevent the harmful effects of technology on copyright and related rights, by taking into account the ways in which technology has eased the infringement of copyright and complicated the enforcement of such. Thus, it allocates Article

	6 to the so-called **technological protection measures (TPMs),** which is articulated as "any technology, device or component that, in the normal course of its operation, is designed to prevent or restrict acts, in respect of works or other subject-matter, which are not authorised by the rightholder of any copyright or any right related to copyright as provided for by law or the sui generis right provided for in [the Database Directive]" (Article 6(3)). Thus, while promoting the adoption of measures by the Member States to prevent the circumvention of TPMs, Article 6(4) of the Directive also **requires the adoption of measures to enable the enjoyment of the E&Ls to copyright and related rights** in order to secure the use of such content despite the TPMs. Also in this context, the InfoSoc Directive dedicates Article 7 to tackle the **digital rights management** (DRM) system. For the purposes of the Directive, rights-management information refers to "any information provided by rightsholder which identifies the work or other subject-matter (...), the author or any other rightsholder, or information about the terms and conditions of use of the work or other subject-matter, and any numbers or codes that represent such information" (Article 7(2)). Considering the facilitation of the removal or circumvention of DRM measures vis-a-vis the technological advancements, the Directive **requires the EU Member States to adopt measures to prevent such actions** as well as the distribution, importation, broadcasting, communication or making available to the public of content whose DRM information has been removed or altered.
CDSMD Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC	Constituting the most recent legislative attempt of the EU legislature to adapt the EU copyright framework to the necessities of the digital era, the CDSMD provides key provisions for research activities, including the E/L it introduced for **text and data mining** (TDM) purposes. The E&Ls to enable TDM, which are introduced to the EU copyright law by the CDSMD, contours the ways in which the data analytics tools can be used over legally protected works and other subject-matter without leading to infringement of IPRs. For the purposes of the CDSMD, TDM is defined as “any automated analytical technique aimed at analysing text and data in digital form to generate information including but not limited to patterns, trends, and correlations.” The CDSMD contains two legal provisions addressed to this purpose: Articles 3 and

	4. The focus of this report will be on Article 3 of the CDSMD as it introduces an E&L, specifically, for the purposes of **scientific research**, without necessarily elaborating on what "scientific research" refers to. However, Recital 12 CDSMD leaves no doubt that the scientific research herein encompasses both natural sciences and human sciences. Article 3 CDSMD **limits the exclusive rights** of the author of a copyright-protected database, the sui generis right of the database maker, the right of reproduction under the InfoSoc Directive, and the exclusive rights of press publishers against reproductions and extractions made by ROs and CHIs. These **beneficiaries are permitted to reproduce and extract works or other subject-matter to which they have lawful access** in order to undertake TDM for scientific research. In light of Recital 14 of the CDSMD, the notion of "lawful access" within this provision shall be understood as having obtained access to content through open-access policies, contractual agreements including subscriptions, and other "lawful means", including the access to "content that is freely available online". Aside from using the works and other subject-matter for TDM purposes as such, beneficiaries are allowed to **store copies of the reproductions or extractions of works** made in the TDM process in so far as their storage is subject to an appropriate level of security. The Directive does not impose any temporal restrictions on the act of storage. The only requirement is that the retention of the mined results is justified by scientific research purposes, including verifying research results. Recital 15 of the CDSMD further stipulates that the copies may also be retained for scientific research applications beyond TDM, such as scientific peer-review and joint research, if such acts are covered by the E&L provided in Article 5(3)(a) of the InfoSoc Directive, again with no temporal limitation. The Directive envisions the possibility for rightsholders to take some **measures to guarantee the security and integrity of networks and databases** where their works and other subject matter are hosted. As clarified by Recital 16 of the CDSMD, these measures should be adopted considering the potentially high number of access requests to and downloads of works and other subject matter. Such measures may encompass, for instance, tools to ensure that only authorized beneficiaries with legal access can access their data, including IP address validation or user authentication. However, these measures must be strictly limited to achieving their intended objective. To this end, the Directive calls the Member States to facilitate the development of best practices mutually agreed upon by rightsholders and beneficiaries of the exception.

	As a last remark to Article 3 of the CDSMD, it shall be emphasized that Article 7(1) of the CDSMD **prevents this exception from being overridable by contractual arrangements**. The TDM exception envisioned in Article 3 CDSMD has been implemented in **Article 70-ter l.aut,** by adopting the letter of the EU provision almost verbatim. Still, it is important to note that the Italian legislature, also by adopting the letter of the EU provision, clarifies that ROs, for the purposes of Article 70-ter l.aut, refers to universities, including their libraries, research institutes or any other entity whose primary objective is to conduct scientific research or to carry out teaching activities that include scientific research, which alternatively: (a) **operate on a non-profit basis** or whose bylaws provide for the reinvestment of profits in scientific research activities, including in the form of public-private partnerships; (b) pursue an aim **of public interest** recognised by a Member State of the European Union. Also in this context, the Italian provision clarifies that the ROs on which business enterprises can exert a decisive influence, such as having preferential access to the results generated by scientific research activities, cannot benefit from this TDM E/L.
Term Directive Directive 2006/116/EC of the European Parliament and of the Council of 12 December 2006 on the term of protection of copyright and certain related rights	The Term Directive **harmonised the duration of legal protection envisioned for copyright-protected works, including software and databases**, while also setting the standards concerning the calculation of the term of protection as such as well as the duration of legal protection envisioned for copyright-protected works originated in non-EU countries. Whereas it is neither possible nor desired to enlist the details of such calculation methods for each category of copyright-protected works, the following shall be included herein as the key points of the Term Directive: • In principle, the copyright protection envisioned for literary and artistic works, including "original" software and database, lasts during the **lifetime of the author(s) and 70 years after the death of the (last surviving) author** (Article 1). • As a general principle, Article 8 of the Directive stipulates that the term of protection begins simultaneously in all EU Member States, and it is calculated from the 1st of January of the year following the event giving rise to it.

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

	or consultation regulated within the Union or national laws. o Any other practice that is in conformity with honest commercial practices. • Aligned with the lawful acquisition, use or disclosure of trade secrets, Article 4 of the Directive enlists the **unlawful acquisition, use and disclosure** of such confidential information. According to Article 4(2), the following acts would be deemed unlawful acquisition of a trade secret: o "Unauthorised access to, appropriation of, or copying of any documents, objects, materials, substances or electronic files" which are under the control of the trade secret holder and which contain the trade secret or from which the trade secret can be deduced. o Performance of any other act that would be contrary to honest commercial practices. Likewise, the following acts, enlisted in Article 4(3), would be considered unlawful use or disclosure of a trade secret: o The use or disclosure of a trade secret that has been unlawfully acquired. o The use or disclosure of a trade secret carried out in a way that would breach a confidentiality agreement or any other duty not to disclose such information. o The use or disclosure of a trade secret carried out in a way that would breach a contractual or any other duty which limits the use of the trade secret. • Last but not least, Article 5 of the Directive introduces certain **limitations to the exclusive rights of trade secret holders**. According to this provision, the acquisition, use or disclose of a trade secret would be exempted from the scope of unlawful practices if they are performed under the following circumstances: o For exercising the right to freedom of expression and information. o For revealing misconduct, wrongdoing or illegal activity if performed for protecting the greater public interest. o The communication between workers and their representatives as long as such communication is happening as part of the exercise of rights justified by the Union or national laws. o For protecting a legitimate interest recognised by the Union or national laws.

Design Directive
Directive (EU) 2024/2823 of the European Parliament and of the Council of 23 October 2024 on the legal protection of designs (recast)
	The recast Design Directive (EU) 2024/2823 modernises and harmonises the legal framework for the protection of industrial designs across the EU, building upon the foundations laid by Directive 98/71/EC. It introduces **updated and technologically neutral definitions for key terminology**, clarifies the eligibility criteria for legal protection, and **refines the scope and duration of protection conferred upon registered designs**. The directive also strengthens the principle of cumulation with copyright law and introduces procedural alignment across Member States to enhance legal certainty and accessibility, particularly for SMEs. Importantly, it **expands the concept of design to include digital and animated features**, reflecting the evolution of design practices in the digital economy.
	
	The key takeaways of Directive 2024/2823, especially relevant to BRIEF activities, are as follows:
	
	• **Article 1** defines the key terminology:
	  ○ The term **"design"** now explicitly includes the appearance of the whole or a part of a product resulting from features such as lines, contours, colours, shape, texture, materials, ornamentation, and **animation (movement or transition)**—a notable addition that accommodates digital and non-physical designs.
	  ○ The term **"product"** is defined as any industrial or handicraft item, including inter alia parts intended to be assembled into a complex product, packaging, get-up, graphic symbols, typographic typefaces, and **spatial arrangements of items forming interior or exterior environments**. The directive maintains the exclusion of computer programs but confirms applicability to **3D printed products** and digital visualisations.
	• **Articles 2 and 3(1)** reaffirm that legal protection requires registration at the competent intellectual/industrial property office.
	• **Article 3(2)** sets the eligibility criteria: a design must be **new** and possess **individual character**.
	• **Article 4** defines novelty as the absence of identical designs made available to the public before the filing date.
	• **Article 5** states that a design has individual character if the overall impression it produces on the informed user differs from that of any prior design.

	• **Article 7** excludes designs dictated solely by technical function or interoperability standards from protection. • **Article 8** excludes designs contrary to public policy or morality. • **Article 12** grants exclusive rights to the registered design holder, including use, import, export, and marketing. • **Article 10** maintains the protection term: 5 years from filing, renewable up to 25 years. • **Article 13(1)** outlines limitations to exclusive rights, including private use, experimentation, and reproduction for citation or teaching, provided these acts are fair and include source attribution.
EU Design Regulation Regulation (EU) 2024/2822 of the European Parliament and of the Council of 23 October 2024 amending Council Regulation (EC) No 6/2002 on Community designs and repealing Commission Regulation (EC) No 2246/2002	The newly amended EU Design Regulation (Regulation (EU) 2024/2822) sets the legal framework for the EU-wide protection of industrial designs, now referred to as **EU designs** instead of **Community designs**, in line with the terminology of the Lisbon Treaty. The Regulation continues to be largely procedural in nature, governing the application process for design registration at the European Union Intellectual Property Office (EUIPO), the examination of such applications, and the legal consequences of registration. It also regulates the establishment and jurisdiction of design courts and dispute resolution mechanisms. However, the reform introduces several substantive updates to **reflect technological developments and improve legal clarity.** These include provisions on the visibility of design features, the treatment of animated and digital designs, and the enforcement of rights against infringing goods in transit. While the substantive provisions of the Regulation remain aligned with the Design Directive (now recast as Directive (EU) 2024/2823), the Regulation continues to provide a distinct legal basis for the protection of **unregistered designs**, which are not covered by the Directive. This remains a key feature of the EU design system. The Regulation retains the same definitions for "design" and "product," but expands them to include **graphic visualizations**, **spatial arrangements**, and **animated features** such as movement or transitions. For unregistered designs, the criteria of novelty and individual character are assessed based on the date the design was first made available to the public, rather than the date of application. Article 5(1)(a) confirms that novelty is determined by comparing the design to those made available prior to its public disclosure.

	Article 11(1) stipulates that protection for unregistered designs begins on the date of first public disclosure within the EU and lasts for **three years**, without the possibility of renewal. Importantly, Article 19(2) clarifies that the rightsholder of an unregistered design may only prevent third-party use if such use **results from copying** the protected design, maintaining a high threshold for enforcement.
Cyber Resilience Act Regulation (EU, Euratom) 2023/2841 of the European Parliament and of the Council of 13 December 2023 laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union	The CRA establishes **cybersecurity requirements for digital products (**such as software, hardware, and connected devices) throughout their lifecycle, aiming to **prevent and mitigate vulnerabilities** that could be exploited in malicious attacks. The key provisions that are relevant for BRIEF researchers are: • **Scope and exclusions**: the CRA applies to all products with digital elements (hardware, software, and remote data processing solutions), but **excludes medical devices**, which remain governed by the Medical Device Regulation. This distinction is important for research involving health technologies. • **Pre-market and post-market requirements**: manufacturers must ensure cybersecurity throughout the product lifecycle—from design and development to post-market monitoring and updates. This includes eliminating known vulnerabilities and implementing **secure default configurations**. • **Essential cybersecurity requirements**: Annex II outlines key requirements relevant to research and development of digital products: o security by default o protection of confidentiality, integrity, and availability of data and networks o data minimisation and resilience against attacks (e.g. dos) o safeguards against network effects and unauthorized access o use of encryption and secure methods o internal activity logging and data portability • **Technical documentation and risk assessment**: before market release, manufacturers must prepare documentation detailing cybersecurity risks and mitigation strategies—relevant for research projects involving product development or testing. • **Conformity assessment procedures**: products with significant risk (e.g. those managing networks or processing personal data) must undergo stricter conformity assessments. Wearable health-monitoring devices are classified as significant products (Class I), which may affect research involving such technologies.

	• **Post-market surveillance and incident reporting**: manufacturers are required to: o monitor product performance after release o report exploited vulnerabilities or security incidents to national CSIRTs within 24 hours o inform users if their cooperation is needed to deploy corrective measures
NIS Directive Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union **NIS 2 Directive** Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148	The NIS Directive applied to essential service operators (ESOs) and digital service providers (DSPs), including sectors like healthcare, digital infrastructure, and cloud computing, many of which are directly relevant to research environments. **NIS 2 Directive** expands this scope to include essential entities (EEs) and important entities (IEs), covering additional sectors such as telecommunications, social media platforms, and public administration. In the following the main provisions are summarized: • **Security and incident reporting obligations**: entities must implement appropriate cybersecurity measures and report incidents to national authorities or CSIRTs. NIS 2 introduces a two-step reporting process: o Initial notification within 24 hours of becoming aware of an incident. o Detailed report within 72 hours. o Final recovery report within one month. These obligations are particularly relevant for research institutions managing sensitive data or digital infrastructure. • **Inclusion of public administration and critical services**: NIS 2 includes public administration entities and services essential to public health and safety, which may encompass public research bodies and health-related research infrastructures. • **Exemptions and size-based criteria**: while small and micro enterprises are generally excluded, exceptions apply for entities providing critical services or having significant impact on public health—potentially including small research labs or specialized data providers. • **Enforcement and penalties**: national authorities are empowered to issue warnings, binding instructions, and fines for non-compliance. This reinforces the importance of cybersecurity governance within research institutions.
Proposals of EU legislation	*Main principles that will be applicable to BRIEF RI activities*

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

The mapping also needs to be supplemented with areas of private law that are expressly regulated in the civil code or special laws in Italy (or in the given legal system). In the technological and digital dimension, the known paradigms require in fact adaptations to EU regulations or practical applications to align the different legal institutions and develop common procedures applicable to the daily life-cycle of R&D&I.
The table below reports some examples of cross-field legal areas that are impacting on the ethical legal framework shaped by the above illustrated legislations referred to the EU data strategy on R&D&I sectors.

Cross-field legal areas	*Paradigms and issues to be addressed*
Insurance issues	The insurances legal discipline in Italy is divided between the Italian civil code (general dispositions) and special laws. • The articles from 1882 to 1932 of the Italian Civil Code deal with the general aspects of insurance contracts. This discipline has not been modified since the publication of the Civil Code but the Court of Cassation has interpreted the general articles in order to admit, at certain conditions, the use of the so-called 'claims-made' clauses in 2016 and 2018. These insurance policy clauses were originally born in Common law countries but are becoming increasingly common also in the EU has they can also give relevance to the circumstances of the damage (claims made deeming clause) and have a period of validity beyond the end of the insurance policy (claims made sunset clause). • The specific discipline of private insurance instead can be found at L.D. 7 September 2005, n. 209, Codice delle assicurazioni private and subsequent modifications. It is a code of EU inspiration which sets rules on private insurance policies and sets also up the IVASS (Istituto per la Vigilanza sulle Assicurazioni) the body that must exercise checks on insurance policy intermediaries with the objective to protect the insured clients and to maintain a fairly competitive insurance market. At present, there are not specialised insurance policy contracts for new technologies, but insurance 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[176].
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

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

	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 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[177] 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

[177] 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

	complex and needs to be explained and simplified for the operators of this sector, BioRobotic experts included. • Risk management and insurance • Healthcare services organisation • Medical malpractice

Table 6: Cross-field legal areas that are impacting on BRIEF's ethical legal framework

5. GAPS AND ENABLERS IDENTIFICATION

The following step for providing a cross-field analysis is to identify interpretative gaps and inconsistencies that may arise in the practical application of the illustrated principles and obligations from the interplay of the different legislative initiatives, as well as the legal provisions acting as enablers for certain common purposes that could 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 research and innovation activities in any way. With specific reference to the BRIEF project, innovation corresponds to the scientific and practical output, whether in the form of 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 to the BRIEF ecosystem.

During the three years of the BRIEF project, the European and national legal frameworks have substantially evolved. Most of the legislative proposals in 2023 have been approved or repealed by September 2025, providing greater legal certainty for the research and development activities of BRIEF's stakeholders (and the iterative drafting of this report has outlined such an evolution). Yet, there are many questions concerning the wide range of research activities that BRIEF enables that still go unanswered, as the legal framework is highly complex and presents overlaps that are not always harmonized. In most cases, official guidelines and best practices that clarify legal requirements and obligations are still missing, which may hamper, or at least slow down, the activities of BRIEF's personnel.

All the legislative proposals and acts that were previously outlined may contain both gaps and enablers. In the following sub-paragraphs, an explanation of a possible classification will be provided, synthesizing the main gaps and enablers that emerge from this cross-field analysis. From a methodological viewpoint, identifying gaps and enablers is relevant in shaping interpretations that facilitate compliance. In fact, covering administrative and legal gaps with good practices and taking advantage of enablers will facilitate R&D&I activities.

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

useful not only for scientific dissemination, but also for the development of business ideas which might 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 mainly to achieve the purposes of data sharing and reuse, as listed in Table 5. Enabling safe-by-design secondary uses of (health) data is paramount in the EU Digital Strategy, for example, to advance progress in AI and biorobotic applications across various domains, to contribute to scientific advancements and to deliver better public services, such as healthcare. This is why the analysis primarily focuses on the use of (personal and non-personal) data for scientific and other purposes, but also includes elements related to AI development and deployment, intellectual property rights, cybersecurity, liability, and safety.

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

Table 7: Secondary uses for data. A list.

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

Some gaps exist due to discrepancies in notions and definitions that do not align completely across different regulations. Other ones refer to procedural inconsistencies that may require identifying a harmonized solution that can comply with different sets of obligations in various scenarios. In other cases, gaps may simply be referred to as a lack of a provision establishing a specific term or condition that would have otherwise resolved interpretative issues related to a given step of the R&D&I life cycle.

The current analysis has identified a series of cross-cutting challenges, that are summarized here below and are better detailed in Table 8. Gaps and enablers may emerge both from a theoretical comparison of the sources of law and from their practical application.

The **scope of application** of some regulations and their obligations is not always clear-cut. In the AI Act, for instance, the categorisation of AI systems into high and low risk may not be straightforward in practice. Moreover, what the research exemption excludes is also of difficult interpretation when it comes to settings that are not "pure" research settings, since many AI systems developed within research laboratories may be later commercialized or put into use. Similarly, the Data Act can be applied in theory to several IoT objects, no specifications are reserved for those impacting on the healthcare sector/market.

Across many regulations of the EU Data Strategy there are several alignments, but also some lack of clarity regarding the **technical and organisational measures** required to ensure data protection and cybersecurity. While guidance and case law shed light on how to implement GDPR's context-specific risk assessments and the principle of data protection by design, even

if this does not dissipate all doubts, the EHDS and CRA introduce additional layers of security expectations to certain types of activities and services without providing detailed implementation guidance. The DGA establishes obligations for data intermediaries, data altruism organizations and secure environments for facilitating safe-by-design data sharing, but the opportunities for data re-use risk being undermined by resource constraints and lack of incentives.

Another challenge is related to establishing a **lawful legal basis for data processing**, particularly in scientific research contexts. National interpretations, such as Italy's requirements for *consenso a fasi progressive,* may complicate research activities even more than missing guidance at the EU-level on the derogations on the specificity of consent. Since a valid legal basis is the *conditio sine qua non* for data processing and reuse, there needs to be alignment with the relevant requirements set by the DGA, the EHDS and the DA. For instance, the DGA's provisions on data altruism are promising, but legally ambiguous when it comes to understanding which legal basis would be the most appropriate one. Even though the GDPR, the DGA, and the EHDS aim to encourage data flows to advance science and innovation, among others, these uncertainties complicate compliance, especially for researchers and developers working with sensitive data or digital products, and hinder secondary uses of data and (AI-driven) innovation.

Another important issue concerns **interoperability and standardization** across Member States and sectors which is a common goal of many of the analyzed regulations. However, such goal is difficult to achieve in practice. For example, the EHDS lacks practical guidance on harmonizing national digital health systems, while the CTR struggles with aligning ethical review processes. The CRA proposes horizontal cybersecurity standards but does not fully address how these interact with sector-specific regulations. The AI Act introduces compliance obligations that may overlap with other domains, such as medical devices and data protection, without clear coordination mechanisms. These gaps may hinder the development of integrated infrastructures and scalable research solutions, instead of enabling them.

Many of the analyzed legislative initiatives underscore the complexity of **defining and allocating roles** to various stakeholders that participate in the value chain of digital technologies' research, development, production and use, such as data controllers and data processors, AI developers and AI deployers, data holders and data users. In particular, the GDPR's multilayered ecosystem makes it difficult to standardize data sharing agreements which would expedite innovation tasks. The DA and the CTR require clear contractual frameworks to delineate responsibilities, especially in data-intensive collaborations. The AI Act introduces an additional layer of complexity by requiring risk assessments that intersect with those mandated by other regulations, such as the MDR and the GDPR. 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. This lack of clarity can lead to compliance gaps, delays and legal disputes.

Research workflows can also be affected by **IP-related limitations**, such as those introduced by the Software Directive, Database Directive, InfoSoc Directive, and CDSMD. While these directives offer exceptions for lawful use, interoperability, and text-and-data mining, they also impose constraints through copyright, digital rights management, and technological protection measures. Researchers must navigate complex conditions for decompilation, extraction, and reuse, which may vary across Member States. The CDSMD's TDM exception is a major step

forward, but its effectiveness depends on national implementation and institutional awareness. These IP constraints require careful legal and technical planning to avoid infringement and ensure compliance.

More in general, the legal framework that emerges from this analysis suffers from **unclear interrelations** between legislative instruments. For example, the GDPR's obligations must be reconciled with the DGA and the EHDS provisions, while the DA overlaps with health law and liability. The CRA's scope excludes medical devices but may apply to adjacent technologies that may have some kind of medical functionality, such as social care robots. The MR and the AI Act both regulate AI systems, but they lack harmonized conformity assessment procedures. This regulatory overlap creates confusion and may lead to inconsistent enforcement or duplicated compliance efforts.

The GDPR, ODD, CTR, EHDS, PLDU, and CDSMD all suffer from **fragmented national implementations**, which undermine the coherence of EU-wide frameworks. Italy's stricter consent requirements under the GDPR, the lack of a unified Open Science policy, and the uneven rollout of clinical trial infrastructure illustrate how national divergences can obstruct cross-border collaboration. Similarly, the CDSMD's TDM exception is subject to national interpretation, which may affect its practical utility. Analoguously, despite the CTR's 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. This fragmentation creates legal uncertainty and operational inefficiencies for researchers and institutions navigating multi-jurisdictional projects. A fragmented approach risks undermining the creation of a Digital Single Market and introduces legal barriers that translate into operational ones. There is therefore a strong need to clarify opaque regulatory aspects and, consequently, to streamline researchers' activities concerning legal compliance with applicable regulations.

5.3 Specific gaps

The table below refers more in detail the gaps emerging from the interplay of the legislative initiatives concerning data, AI and public health that might require a systematic interpretation for avoiding being a barrier to innovation.

Legislative act	*Gaps to be interpreted*
General Data Protection Regulation (GDPR) (Sec. 3.1.1)	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 of many emerging technologies. The **translation of responsibilities into a data sharing agreement** could be difficult to standardize. Moreover, the lack of pre-determined **technical and organisational measures and the scarcity of off-the-shelf tools** that can enhance the privacy and security of personal data, especially for anonymizing and pseudonymizing (health) data may constitute a barrier. This challenge is exacerbated by the fact that each data protection impact assessment may result in varying levels of risks for similar data processing activities, since the

	risk estimate is highly contextual. This is why it is impossible to define whether data are effectively anonymized or pseudonymized *a priori*: **the selected techniques must be appropriate to the specific setting** where they are employed, in line with the principle of data protection by design and by default. **National implementations introducing different additional safeguards to process sensitive data** under article 9, especially in case of scientific research and statistical processing purposes, could constitute a barrier to data reuse and data sharing. For example, in Italy, the consent of the data subject is required also when 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 no. 1, 2, 3, 4 and 4 update). The ease of use of "consenso a fasi progressive" in real-world scenarios is also debatable. Lastly, the **interplay of GDPR's obligations with the EHDS's provisions** on secondary use of health data must yet be clearly appraised.
Open Data Directive (ODD) (Sec. 3.1.3)	Even though the ODD sets a favourable framework for the reuse of research data originated in publicly funded projects, **national policies in Italy that would encourage the uptake of open science are still being defined**. The assessment of the current state of Open Science drafted by the dedicated working group in 2024 underscores that there is no national legislation on Open Access and Open Science and that the existing norms are scattered across different websites and documents. This uncertainty, combined with the still imperfect offer of incentives and actions to support researchers and institutions in adopting open science policies and practices, risks hampering the successful implementation of the ODD in the short term.
Data Governance Act (DGA) (Sec. 3.1.4)	The DGA complements the ODD in terms of reusing publicly held data that are protected due to their personal nature, intellectual property rights, or commercial or statistical confidentiality. Public bodies need to ensure that the **privacy and confidentiality of the data they make available to others is guaranteed with appropriate technologies**, which would definitely help scientific progress but may be challenging to implement in practice, due to lack of adequate resources. This is why, **data intermediaries** could play an essential role and provide the necessary technical, legal or other means for data sharing and reuse (for e.g., anonymizing the data). Even research institutions could resort to data intermediation services to facilitate the sharing of the data they hold, especially in the view of fostering open

	science. However, **such services come with a cost** that should be covered by appropriate resources and should be planned in institutional budgets and project funding. Another promising solution is represented by data altruism organizations that would make data available for general interest purposes, including research, and other purposes that are established by national law (note that the notion of general interest is not defined and it could vary from one country to another, which could hinder transnational data flows). However, since they do not operate for profit, their **business model is still unclear,** which could hamper the adoption of the newly established mechanism of data altruism at large. Indeed, at date, only 3 data altruism organizations have been registered in the dedicated national registries. Moreover, the **legal basis** that would enable the reuse of data for broad general interest purposes is still unclear
Data Act (DA) (Sec. 3.1.5)	The aim of the DA is to set a general regulation for **any kind of IoT object**. This proposal's **wide range of application** makes it difficult to foresee how its implementation will unfold. More specifically, the DA spans from cloud providers switching capabilities to data-sharing in 'emergencies' to the access to one's own IoT data to develop another product (read IoT object) or a service on a secondary market. The obligations of all the parties involved (mainly the user, the recipient and data holder) and how the **contracts** among them should be regulated are explained at Articles 3-13 of the proposal. Moreover, at this stage, the DA does not make any difference between IoT with consumer/professional functions and e-health IoTs. This also makes it more **complicated to coordinate this proposal with all the EU health law** as data concerning health needs more protection in general than 'less sensitive' categories of personal data. One of the most interesting but also difficult to implement parts is how to draft **data sharing contracts between users, data holders and third parties**. Moreover, national and EU institutions in exceptional circumstances have the right to access connected product data. Even if this option was imagined during the pandemic, the generality of the word emergency as a justification has raised quite a few concerns. One of the most problematic points concerns the respect of the GDPR. The DA states that personal data other than the users' must be processed according to a **lawful legal basis**. Even using consent as a legal basis as set in Article 6(1)(a) and Article 9(2)(a) GDPR can be difficult in some countries such as Italy where there is a restrictive

	interpretation governing the re-contact of people for biomedical research even with the new rules applicable to secondary use of data for medical research.[178] This is relevant as the DA is applicable in principle to all IoT devices, **including also medical devices which use IoT or AI technology** to perform, which might be tested in their early prototype form in the BRIEF facilities.
European Health Data Space Regulation (EHDS) (Sec. 3.1.6)	The EDHS sets the groundwork for the creation of a new system for the **sharing of digital health records**. 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 regulation does not give practical guidance on this aspect. Most importantly, the EHDS covers the conditions for the **secondary use of health data**. The vision of this regulation is ambitious, and its implementation could be ambitious as well, for example, concerning the information security requirements related to the **secure processing environment** that should guarantee the privacy and confidentiality of health data. The Italian provisions concerning the Electronic Health Record 2.0 (FSE 2.0) and the Ecosistema Dati Sanitari (Health Data Ecosystem, EDS) are **complex and interrelated with other legal provisions** (e.g., those on data protection), and add additional requirements to those set forth by the EHDS, for instance concerning the re-use of health data for research purposes that should be deprived of direct identifiers. Albeit the requirements are meant to strengthen the protections surrounding Italian patients' sensitive data, their complexity may create further disorientation and may hinder data sharing, instead of fostering it, if medical personnel does not have the **necessary resources** to understand and know how to implement the requirements in practice, for example those related to anonymization and pseudonymization (see also the related aspects concerning the GDPR above).
Medical Devices Regulation (MDR) (Sec. 3.2.1)	According to the new framework, medical device producers need to comply with **several novel duties (which also involve post-market surveillance)** in addition to the process involving conformity certification by Notified Bodies. This complex system requires the

[178] Aurucci P and Di Tano F, 'Dati Personali e Ricerca Medica: Condizioni, Incoerenze e Prospettive Giuridiche a Fronte Dell'evoluzione Interpretativa e Applicativa Del Garante per La Protezione Dei Dati Personali' (2024) 3 BIOLAW JOURNAL 305; Casarosa F and Gennari F, 'Data Sharing in the Internet of Medical Things: Between the Data Act and the EHDS' [2023] European Journal of Risk Regulation 1

	implementation of a general strategy of compliance (see Policy briefs no. 6, 7, 8). In particular, if we have a SaMD, a **software as medical device**, which uses AI techniques and could be considered an AI system, there might be uncertainty concerning how to harmonise the AI Act and the MDR conformity procedure for software (see Policy briefs no. 9, 10). A future rising problem, as far as SaMD is concerned, is implementing rule 3.1 of Annex VIII. In this rule, the manufacturer's intended purpose for the device plays a significant role. This rule will become increasingly important in the coming years as more medical devices incorporate AI systems, as mandated by the AI Act. More and more apps in fact claim they are not medical devices, but they work with sensitive data concerning health. Hence, the MDR still concedes a leeway to the manufacturer: in case there is a doubt about the fact that it is in fact Software as a Medical Device (SaMD), it is the intended purpose that counts. Moreover, there is also another rising issue, and it is that it is not yet clear how compliance will be carried out in practice between the MDR and the AI Act with a high-risk AI system used for medical purposes (it will be basically all the classes except class I). Article 8 AI Act sets the rule that if the high-risk system is within the list of Annex I section A, then the manufacturer can follow the older conformity procedure (in this case, the MDR), and can add the relevant AI Act rules for high-risk systems. Nevertheless, this rule is brutal to put in place as, for instance, there are several parts of the MDR, such as the Quality Management System, which is general for all medical devices, and there is also the principle of quality management in the AI Act, which does not consider the medical implications of software. That is why the MDCG and the AI Office started coordinating with a set of guidelines[179] in form of Q&A that will be gradually implemented. At a first reading, the document does not give clear indications on how to practically implement the high-risk AI Act principles in a more concrete setting and what to select from the MDR conformity procedures when AI-powered SaMD is involved. As this document is a living document, it is expected that a better level of clarity will be achieved by the joint MDCG and AIB action
Clinical Trials Regulation (CTR) (Sec. 3.2.2)	The legislative decree concerning the implementation of the clinical trials regulation was voted on some years ago,

[179] (AIB 2025-1 MDCG 2025-6 Interplay between the Medical Devices Regulation (MDR) & In Vitro Diagnostic Medical Devices Regulation (IVDR) and the Artificial Intelligence Act (AIA), 2025

	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 regions. This aspect has been addressed by the decrees of January and June 2023. Although the EU CTR aims to foster a more unified and harmonized approach to clinical trials, the implementation of the unified Clinical Trials portal (CTIS) has been a protracted process. Moreover, there are many **differences and discrepancis 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). Determination 424/2024 aims to simplify and decentralize clinical trial operations in Italy, mainly by clarifying the roles and responsibilities of those involved in the trials, also from a data protection point of view. This means that the parties covering the roles of data controllers and data processors are set in a more transparent accountability framework, but need to be able to comply with the relevant legal and technical requirements for adequate protection of personal data, with all the difficulties already identified above (see GDPR) and the need for clear contractual frameworks.
Machinery Regulation (MR) (Sec. 3.3.1)	While in the MR proposal there was an explicit reference to the AI Act, the same cannot be said in the text of the approved MR regulation. However, in the approved AI Act, ~~Annex III~~ Annex I refers to the Machinery Directive (rather than the Regulation) in the list of harmonized EU legislation. **When such legislations cover AI systems, it is presumed that they are categorized as high-risk AI systems,** as explained in Article 6 AI Act. There is also a convergence regarding the term 'safety component' in both the MR and AI Act, as well as in their definitions (Article 3(14)) (see Policy brief no. 16). However, in the MR, the AI Act was not mentioned as it had not been approved yet. **Software is included in the definition of safety components in the MR** (Article 3(3)) and can be a (high-risk) AI system if it is '*fully or partially self-evolving using machine learning approaches ensuring safety functions'* (Recital 19). Nevertheless, in the MR, software is also important for other reasons, such as accessing the technical documents that are necessary for the correct use and conformity of the machinery (Article 10). For the safety component AI software, one has to look in Annex III concerning essential health and safety requirements. Part B of the mentioned Annex III explains

	that it is important to protect the software and data that "*are critical for the compliance of the machinery or related product with the relevant essential health and safety requirements*" (Annex III, Part B, 1.1.9) from corruption or hazardous intentions. Further on, among the different requirements of the control system, it is mentioned that "*the tracing log of the data generated in relation to an intervention and of the versions of safety software uploaded after the machinery or related product has been placed on the market or put into service is enabled for five years after such upload, exclusively to demonstrate the conformity of the machinery or related product with this Annex further to a reasoned request from a competent national authority*" (Annex III, Part B, 1.2.1 (f)). The lack of clarity regarding the connection with the AI Act in the MR's text creates a gap, as it **fails to provide a clear definition for harmonizing conformity procedures**, specifically for high-risk AI systems and software as security components. The introduction of AI for safety components is also an enabler, as it allows machine manufacturers to be more informed about AI and its risks, as enshrined in Article 4 of the AI Act on AI literacy (see Policy brief no. 15). 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 (PLD) and Product Liability Directive Update (PLDU) (Sec. 3.3.2 and 3.3.3)	Until 9 December 2026, when the PLDU will become applicable, the BRIEF infrastructure and researchers must know that the PLD applies to all consumer products, including those still in a prototype phase, regardless of whether they might become medical devices in the future. This new division changes the rules on how to prove damage, fault and the causality link. 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 can also guarantee (under certain conditions) **compensation for data damage**,

	which is considered a product or a good, when it is not used for professional purposes. However, the PLDU application is formally separated from 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)[180]. It is true that the PLDU considers the criticalities of the PLD and adapts it to a world where advanced technologies, such as IoT and AI, are part of a consumer's life. However, the main mechanisms underpinning the PLDU have arguably stayed the same of the PLD's. It is likely that the problems that emerged with the PLD, such as the difficulties in **establishing a causal link in increasingly complex technologies**, will not be solved and will arise again with the PLDU. It is indeed up to the MS to make this directive work in practice.
AI Act (AIA) (Sec. 3.4.1)	Even though dedicated guidelines issued by the AI Office in 2025 have attempted to clarify what falls under the definition of AI system (Article 3(1)), it is **challenging to characterize AI systems according to the elements proposed in such a definition**. Just to name a few, the notion of autonomy looks too vague to be operationalized, while there seems to be a certain degree of terminological confusion between learning, training and inference. The AI Act contains an **exemption for research activities, which should be interpreted in a narrow manner**. The scope of the regulation excludes research activities "prior to [the AI systems] being placed on the market or put into service" (Article 2(8)), which include commercial activities even without a financial compensation but exclude any other non-commercial activity, such as uploading an AI system to an online repository where it can be downloaded in combination with the publication of a paper. The definition also includes the provision of the system to deployers for first use or for own use for the purposes intended by the provider. As a consequence, researchers should be mindful of this narrow application of the research exemption, since in many cases it may not apply. Moreover, any activity carried out by spin-offs does not probably count as "sole purpose of scientific research and

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

	development". Clarifications and guidelines on this aspect are still needed, though. The AI Act forbids some forms of AI systems, such as those that discriminate against a person or certain groups and those that use subliminal techniques to manipulate decision-making (which could be a risk of certain human-brain interfaces). These are only tolerated if they fall under the research exemption. Among the forms of AI systems that are admissible, there is a primary division between high-risk and non-high-risk AI systems (see Policy brief no. 13). Suppose the system is considered **high-risk** based on the combination of the definitions at Article 6 AIA and Annex I-III. In that case, there are **many compliance obligations concerning the design and the implementation** of the AI system (e.g., risk assessment, transparency, documentation, etc) (see Policy briefs 11, 12, 14). This places an additional burden on researchers throughout the entire AI system development lifecycle, when the systems are meant to be commercialized or put in use later on. This means that researchers should **consider the AI Act's obligations and requirements early on**. Otherwise, they may be unable to use the system outside mere research settings. The allocation of responsibilities and obligations set forth by the AI Act depends on yet another **risk assessment**, which, in certain use cases, should be carried out in addition to the risk assessment performed in case of personal data processing and the one performed for medical devices.
Software Directive (Sec. 3.4.1.1)	The Software Directive establishes a harmonized legal framework across EU Member States for the copyright protection of computer programs, defining the **rights of authors and lawful users, and setting out rules for ownership, use, and interoperability**. Its provisions are crucial for BRIEF researchers, especially when they develop or reuse software in their activities. In essence, software is protected as a literary work if it reflects the **author's intellectual creation**. This includes preparatory design materials, which may be relevant during early development stages. Protection covers the expression of the software, not the underlying ideas or principles, allowing researchers to study and build upon conceptual foundations. The author can be an individual, a group, or a legal entity. In employment contexts, **economic rights typically belong to the employer**, unless otherwise agreed. Researchers thus need to check this aspect with their employees.

	The **copyright holder has exclusive rights.** For example, the reproduction, adaptation, and distribution of software require authorization. These rights apply to all forms of use, including loading, running, and storing the software. **Researchers may perform certain acts without prior authorization if they lawfully acquired the software**, such as producing backup copies, and studying and testing the software to understand its underlying principles. Decompilation is allowed to achieve interoperability, but only under strict conditions (e.g. necessity, limited scope, and non-commercial use).
Database Directive (Sec. 3.4.1.2)	The Database Directive provides two layers of legal protection for databases: 1. **Copyright protection** for databases that reflect the author's intellectual creation through **the selection or arrangement of content.** 2. **Sui generis rights** for databases that involve substantial investment in **obtaining, verifying, or presenting their contents.** Researchers should note: • Lawful users may access and use databases for teaching and scientific research, provided the use is **non-commercial and the source is cited**. • Decompilation and interoperability are not covered, but **extraction and re-utilization of insubstantial parts are permitted**. • **Substantial changes** to a database may qualify it for renewed **sui generis protection**. • Protection does not extend to the database contents, which may be **governed by other legal regimes** (e.g. data protection, IP rights).
Information Society Directive (InfoSoc Directive) (Sec. 3.4.1.3)	The InfoSoc Directive establishes a harmonized framework for copyright and related rights in the digital environment, defining **key economic rights and introducing exceptions and limitations to support lawful uses**, including those relevant to research and technological innovation. In particular, there are three main aspects that are relevant for BRIEF's activities: 1. **Mandatory exception for temporary reproduction** (Article 5(1)). This enables AI model training and other technological processes involving copyright-protected works without infringing reproduction rights. It applies to transient or incidental acts of reproduction that are essential to a technological process, such as transmission or lawful use. These acts must have

	no independent economic significance, making them particularly relevant for non-commercial research and experimentation. 2. **Technological protection measures (TPMs) and access rights** (Article 6). TPMs are tools designed to prevent unauthorized use of protected content. While Member States must prevent circumvention of TPMs, they are also required to ensure that exceptions and limitations (E&Ls), like those for research, remain accessible despite TPMs. 3. **Digital rights management (DRM) safeguards** (Article 7). DRM refers to metadata and identifiers that control access and usage of digital content. The Directive obliges Member States to prevent the removal or alteration of DRM information, which is crucial for maintaining lawful access and use in research contexts.
Copyright in the Digital Single Market Directive (CDSMD) (Sec. 3.4.1.4)	The Directive on Copyright in the Digital Single Market (CDSMD) marks a pivotal legislative step in modernizing EU copyright law to support digital innovation, notably by introducing **targeted exceptions and limitations (E&Ls) for text and data mining (TDM) in scientific research**. The TDM exception (Article 3 CDSMD) enables research organizations to **reproduce and extract copyright-protected content for TDM, provided they have lawful access** (e.g., via open access, subscriptions, or freely available online content). TDM is defined as any automated analytical technique used to analyze digital text and data to generate insights such as patterns, trends, or correlations. Research organizations **may store mined content indefinitely, provided it is securely stored and justified by research needs** (e.g., verification, peer review, joint research). Rightsholders may implement proportionate safeguards (e.g., IP validation, user authentication) to protect their content, but these must not obstruct legitimate TDM activities. Member States are encouraged to foster best practices through stakeholder collaboration. Article 7(1) ensures that the TDM exception under Article 3 cannot be contractually waived or overridden. The Italian Implementation (Article 70-ter l.aut) mirrors the EU provision and clarifies that eligible research organizations include **universities, libraries, and research entities operating non-profit or with reinvested profits in research**. Entities under decisive

	influence of commercial enterprises are excluded from benefiting.
Term Directive (Sec. 3.4.1.5)	The Term Directive establishes a harmonized framework across the EU for determining the duration of copyright protection, including for software, databases, and works originating outside the EU. Of relevance is the fact that copyright protection for literary and artistic works, including original software and databases, **lasts for the lifetime of the author and 70 years after the death of the last surviving author**.
Trade Secrets Directive (Sec. 3.4.3.1)	The Trade Secrets Directive sets out a harmonized legal framework across the EU for the **protection of confidential business information**, establishing minimum standards while allowing Member States to adopt more protective measures. **Information qualifies as a trade secret if** it meets all three criteria: • It is not generally known or readily accessible within relevant professional circles. • It has commercial value due to its secrecy. • Reasonable steps have been taken to keep it confidential. Trade secrets may be **legally acquire**d through: • Independent discovery or creation. • Reverse engineering of publicly available products. • Exercise of workers' rights under EU or national law. • Any practice aligned with honest commercial conduct. **Acts considered unlawful** include: • Unauthorized access, appropriation, or copying of materials containing trade secrets. • Breach of confidentiality agreements or duties. • Breach of contractual limitations on use or disclosure. Certain uses of trade secrets are **exempt from liability**, including: • Exercising freedom of expression and information. • Whistleblowing to expose misconduct or illegal activity in the public interest. • Communication between workers and their representatives under legal rights.

	• Protection of other legitimate interests recognized by law.
Design Directive (Sec. 3.4.4.1)	While Directive (EU) 2024/2823 marks a significant advancement in the harmonisation and modernisation of design law across the European Union, it does not fully resolve all the challenges faced by researchers and developers, and in some cases, introduces new layers of complexity. One of the most notable limitations is the **partial harmonisation of the so-called "repair clause."** Although the directive acknowledges the importance of enabling the use of design-protected parts for the repair of complex products, it stops short of establishing a fully unified legal framework across Member States. This leaves engineers and product developers operating in cross-border contexts exposed to legal uncertainty when designing for modularity, interoperability, or sustainability—especially in sectors such as automotive, electronics, and consumer goods. Moreover, while the directive introduces general principles for procedural alignment, it allows Member States considerable discretion in implementing specific rules. This results in **continued fragmentation in registration procedures**, evidentiary standards, and enforcement mechanisms, which can be particularly burdensome for researchers and innovators working within EU-funded or multinational projects. Another unresolved issue is the **lack of harmonisation for unregistered design rights.** In fast-paced industries such as fashion, software, or digital media—where registration may not be practical—this gap creates ambiguity and risk, especially for early-stage innovators. Additionally, although the directive expands the scope of protectable designs to include animated and spatial features, it does not fully clarify how dynamic or interactive designs should be assessed for novelty and individual character. This leaves developers of immersive technologies, such as AR/VR environments or adaptive interfaces, without clear guidance on the boundaries of legal protection. The directive also remains **silent on the growing relevance of AI-generated designs.** As generative design tools become more integrated into engineering workflows, the absence of provisions addressing authorship, ownership, and eligibility for protection of AI-generated outputs may lead to disputes and regulatory gaps.
Community Design Regulation (Sec. 3.4.4.2)	Although Regulation (EU) 2024/2822 introduces important updates to the EU design protection system, it

	does not fully resolve several challenges—many of which are also present in the recast Design Directive. One persistent issue is the **limited harmonisation across Member States, particularly in procedural aspects and the treatment of unregistered designs**. This fragmentation continues to create legal uncertainty for researchers and developers working across borders, who must navigate differing national rules despite the Regulation's aim to streamline EU-wide protection. Additionally, while the Regulation expands the scope of protectable designs to include digital and animated features, it **does not provide clear criteria for assessing novelty and individual character in dynamic or interactive formats**. This ambiguity mirrors similar gaps in the Directive and poses difficulties for innovators working in fields such as AR/VR, interface design, and generative technologies. The Regulation also leaves some questions open concerning the **legal status of AI-generated designs**, leaving unresolved questions around authorship and ownership that are increasingly relevant in design and engineering workflows.
Cyber-Resilience Act (CRA) (Sec. 3.5.1)	The CRA fulfils the critical function of laying down horizontal rules for products with digital elements that could allow better interoperability and incentivise the creation of new shared IT standards . The Regulation creates a governance system based on **notified bodies** that should make the operators involved more accountable. However, it needs to be determined how the CRA **interrelates with other EU legislative acts and areas of application**, such as the MR and the AI Act. The Regulation **does not apply to products with digital components that are classified as medical devices**. This distinction allows manufacturers of medical devices to focus on meeting the safety and security requirements set out in the Medical Device Regulation. However, this does not exclude the application of CRA to those **devices that do not qualify as medical, yet ensure a health function**. For instance, a social care robot used by an elderly individual to provide company and social interactions may not qualify as a medical device, though it is able to process data and establish a connection with a cloud computing service that can be accessed by the manufacturer and by a medical expert. Therefore, it may easily fall into the concept of product with digital elements. Annex II contains security considerations and vulnerability management parameters, but the

	requirements are not sufficiently detailed to identify all the technical and organisational measures that should be adopted in each stage of the design and development of the product. However, they establish a preliminary framework that can be further defined through risk management systems that evaluate the cybersecurity readiness of the product in relation to different types of threats.
Directive on Security of Network and Information Systems (NIS 2) (Sec. 3.5.2)	The NIS 2 broadens the scope of application compared to NIS, as it includes many more actors that are subject to its obligations. One of the criteria of inclusion depends on the size of the enterprise, where small and micro enterprises are excluded. That said, there are certain entities to which the NIS 2 applies, regardless of their size. However, **the size criterion is inadequate to address the increasingly prevalent situations that fall outside the scope of the listed exceptions**. This is exemplified by links included in production chains that do not directly fall within the purview of the exceptions. Despite the fact that such links cannot be regarded as the sole provider of an essential service for the maintenance of critical social or economic activities in a member state, they nevertheless represent a bottleneck for the production chain that has the potential to enable the qualification as an essential entity.

Table 8: Regulatory gaps and interpretative barriers, with a focus on issues that are relevant for BRIEF's research activities

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.
A general methodological approach to avoid negative implications is to address the ethical-legal principles outlined in these pages in a responsible and accountable way, fostering compliance by design and by default also with the common principles emerging from the various regulations, even if official guidelines and case law for the newly approved laws are missing. From this perspective, the reference to a trustworthy approach signifies overcoming formal barriers to achieve a higher level of compliance with EU values. If it shall be translated into providing an impact assessment for new AI-based technologies impacting the protection of fundamental rights (like dignity, healthcare, private life, data protection, employment, etc), this could be an interpretative solution to be boosted in terms of legal enabler.
In this uncertain legal framework, the experience of over a few 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[181] 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.

Moreover, the risk-based approach that has been developed in the GDPR drives some of the mentioned initiatives, such as the AI Act and the MDR. 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 the support of domain experts. It 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	Room for national safeguards for data processing activities for research and statistics purposes that might identify further constrains for cross-border data processing (e.g. the role of consent for the reuse of health-related data for research purposes). Unclear differences between private and public nature of the data controllers, as well as between	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.

[181] 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.

	controllers and data protection authorities. Data Protection Officer to drive compliance activities.	research and Research & Development & Innovation purposes.	
ODD	Publication of non-personal data in open, machine-readable formats and according to open standards Charging rules that establish free re-use as the norm Re-use of data from publicly funded research	Ongoing, sometimes slow, uptake of the obligation concerning the publication of open data National policies that would encourage the uptake of open science are still being drafted in Italy	Existing trustworthy open data portals can be leveraged for publication and reuse of data, while incentives are formulated Established international, as well as institutional, standards and good practices concerning open science can be the guiding principles for research activities, while national policies are defined
DGA	Intermediation services as safeguards for data subjects' rights and for helping public sector bodies share data safely. *Favor* for bottom-up mechanisms of data sharing for general interest purposes through data altruism organizations. Collective control, oversight and exercise of the rights of the data subjects through data cooperatives	Complexity and lack of incentives to set up intermediation services, especially data altruism organizations. 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 practices and technologies for consent management and privacy-preserving data sharing through services of intermediation. Privileged collaborations with specific data intermediation service providers established at the level of the research institution. Researchers should inform research participants of benefits of data altruism and adapt their consent processes accordingly.

	pursuing mutualistic scope.		Development of common terms and conditions for platforms offering data, and of incentives for DAOs and cooperatives.
DA	Non-profit research bodies and SMEs can access data at cost, removing financial barriers only if within the B2B and B2G scheme . Public bodies may share privately held data with research entities during emergencies or for public-interest tasks. Harmonized formats and vocabularies support cross-platform data exchange and integrated research infrastructures. Legal clarity on roles and rights in data access fosters secure and fair collaboration.	Data holders may restrict access to protect intellectual property or trade secrets, especially in competitive sectors. Vague criteria for what constitutes a public emergency may delay or complicate B2G data sharing. Implementing interoperability standards and managing multi-party contracts requires significant expertise and resources.	Promotion of the use of secure data processing environments and data anonymization techniques to minimize IP exposure during sharing. Guidelines on balancing data access with IP protection should be developed and/or followed. Pre-approved emergency data access protocols and templates for requests under Article 17 to streamline B2G procedures should be created, while the definition of public emergency is clarified. Development of open-source toolkits and reference implementations for data format conversion, contract templates, and compliance checklists, funded by adequate resources.
EDHS	Safe environment to share electronic health data for their reuse. EU framework for health data flows with common safeguards	Complex structure to guarantee the interoperability of Member States' health records, but also to allow the secondary use of data. Lack of clear standards and	It will be important to follow-up on any relevant standard concerning health, as well as interoperability of data formats.

	and procedures of access and sharing. Possibility to request the health data access body to elaborate data and provide an aggregate result.	resources for secure, privacy-preserving environments. There are fragmented national rules and unclear interoperability hinders harmonization. The level of awareness and training on the matter is still low.	Privacy information shall include the possibility that today a given data flow stored for secondary use purposes could then converge into an EHDS once established. Researchers should privilege privacy-preserving infrastructures for health data processing that are recognized. They should also seek guidance from national authorities on harmonized access procedures and safeguard requirements, once these are made available. All this requires targeted training programs.
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	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.

	surveillance obligations.		
CTR	There will be a functioning unified portal (CTIS) that 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 on 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.
MR	As a regulation, the MR ensures uniform rules across Member States, reducing legal fragmentation. Software is recognized as a safety component. This includes AI systems, aligning MR with the AI Act and clarifying compliance pathways for research involving intelligent machinery. Researchers and developers can use the MR's conformity procedures to understand how to design and test machine prototypes for market readiness.	Despite direct applicability, national ministries may issue divergent clarifications, risking uneven interpretation. Dual compliance with MR and AI Act can be complex to manage, especially for high-risk AI components. CE marking requirements vary by risk level, which may be difficult to navigate for early-stage research prototypes.	Follow national guidance that addresses regulatory interpretations and reduces national divergence. Joint conformity assessment protocols for products subject to both MR and AI Act, with clear compliance pathways, should be developed. Researchers should be aided in understanding how to follow such pathways. It would be useful to obtain simplified CE marking guides and risk classification tools tailored for research

			prototypes and early-stage innovations.
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. That is why the new concept of the manufacturer's control was introduced New rules on how to prove defectiveness and the causality link in objects with digital elements	Adaptation of the products/good legal concept to data which had always been considered as part of software; complex to implement the procedural inputs that have been put in the proposal.	Need to be updated with important national cybersecurity agency updates on what are the risks of malfunctioning; it will be necessary to better design the product (generally an IoT object) in advance.
AI Act	All of the above principles plus a general principle of protection of fundamental rights The research exemption enables researchers to pursue innovation and experimentation, lifting them from regulatory burden.	The classification in high and low risk AI system will often depend also on the concrete features of the AI system and its functions. Thus it is challenging to provide general recommendations. The exemption for scientific research does not apply to start-ups and SMEs, thus it may be challenging in the BRIEF R&D ecosystem to understand which responsibilities apply to whom, since some AI systems may be developed within academic settings but then commercialized within spin-offs. Moreover,	Guidelines are already available to perform the ethical legal assessment (see ALTAI checklist) and for ethical conduct in computer science and engineering research. The AI Office is issuing additional guidelines on important aspects such as the definition of AI system or the notion of prohibited practices. Other regulators, such as the EDPB, clarify further aspects, e.g., those that intersect AI and personal data processing. Following guidelines early-on may help researchers proactively predispose their AI

		transparency, documentation, data governance and human oversight requirements for high-risk systems need to rely on information produced throughout the entire life-cycle, thus also during initial phases of research. This places an additional burden on researchers. Even when the legal provisions do not apply because the AI system is only developed for pure scientific purposes, researchers still need to respect research ethics safeguards.	systems for later commercialization.
Software Directive	The Directive establishes that computer programs are protected as literary works under copyright law, ensuring a clear legal basis for protecting original software creations. It allows reverse engineering for interoperability purposes, enabling developers to study and understand software interfaces to ensure compatibility with independently created programs. The Directive provides exclusive rights to reproduce, adapt, and distribute	The Directive does not clearly define what constitutes originality in software, leaving uncertainty for developers working on modular or generative code. The scope of permitted reverse engineering is narrowly defined, and national implementation varies, creating legal risk for developers engaged in compatibility research. The Directive does not address modern software development practices, such as open-source licensing, collaborative development, or AI-generated code, which	There is the necessity for a harmonised definition of software originality, tailored to contemporary coding practices and modular development. Researchers should follow best practices for awful reverse engineering, especially for interoperability and security research. Researchers should document reverse engineering activities carefully, seek legal advice when working across jurisdictions, and consider using open-source licenses that explicitly define rights and obligations.

	software, giving developers control over the commercial use of their creations.	were not foreseen in 1991.	
Database Directive	The Directive provides dual protection: copyright for original selection/arrangement of contents, and sui generis rights for substantial investment in obtaining, verifying, or presenting data, supporting both creative and data-intensive research. It allows lawful users to extract and reuse insubstantial parts of a database for any purpose, and permits extraction for teaching and scientific research, provided the source is indicated and the use is non-commercial. The Directive applies to electronic and non-electronic databases, ensuring broad coverage for research outputs across formats and disciplines.	The threshold for sui generis protection ("substantial investment") is vague and inconsistently interpreted, creating uncertainty for researchers compiling or curating datasets. The Directive does not clearly address machine-generated databases or automated data aggregation, which are increasingly common in engineering and AI research. Exceptions for research use are limited and vary across Member States, especially for reuse of substantial parts, which may hinder data-driven innovation and reproducibility.	Researchers should document the origin and structure of databases, use licensing tools (e.g. Creative Commons licenses), and consult institutional and national IP offices to navigate reuse rights and exceptions. They should also follow best practices in their domain to address known challenges.
InfoSoc Directive	The Directive allows reverse engineering (decompilation) when necessary to achieve interoperability between independently created	The Directive protects only the expression of a program, not its underlying ideas or principles, which may leave functional	Legal clarification would better define the boundary between protected expression and unprotected ideas, especially for functional elements

	programs, enabling engineers to build compatible systems. It grants lawful users the right to observe, study, or test the functioning of a program to understand the ideas and principles behind it, supporting research and debugging. It protects computer programs as literary works under copyright, ensuring legal certainty and exclusive rights for developers over their original creations.	innovations without IP protection. The scope of reverse engineering is narrowly defined and subject to strict conditions, which may discourage interoperability research or lead to legal uncertainty. The Directive does not address AI-generated code or collaborative development models, which are increasingly relevant in modern software engineering.	like interfaces or algorithms. Official guidelines should be issued on lawful reverse engineering, including best practices for documenting and limiting such activities to avoid infringement. Researchers should track authorship and contribution in collaborative or AI-assisted development and consider complementary licensing strategies to clarify rights and usage.
CDSMD	The Directive introduces a mandatory exception for text and data mining (TDM) for research organisations and cultural heritage institutions, enabling large-scale computational analysis of digital content for scientific purposes. It clarifies that lawful access to content (e.g. via subscriptions or open access) is sufficient to benefit from the TDM exception, reducing licensing barriers for researchers.	The TDM exception is limited to non-commercial research organisations, excluding private-sector R&D teams and independent developers from its scope. The Directive does not fully resolve legal uncertainty around automated data processing, especially when copyright and database rights overlap in large datasets. Technological protection measures (TPMs) may still restrict access to content, even where exceptions apply, unless rightholders voluntarily enable	The scope of the TDM exception should be further clarified, possibly to include commercial research under specific conditions, such as transparency and non-infringement safeguards. There is the need for usable EU-level guidance on the interaction between copyright, database rights, and TDM, especially for hybrid datasets used in AI and engineering. Researchers should negotiate licensing terms carefully, seek clarification on TPMs, and document lawful access to content to

	It supports cross-border digital uses for teaching and research, helping developers and engineers collaborate across Member States without conflicting national copyright rules.	access or Member States intervene.	ensure compliance with the Directive.
Term Directive	The Directive harmonises the duration of copyright protection across the EU, providing legal certainty for the use and licensing of protected works in research and development contexts. It establishes a clear calculation method for protection terms (e.g. 70 years after the death of the author), which helps researchers assess when works enter the public domain and become freely usable. It includes provisions for related rights, such as protection for performers and producers of phonograms, which are relevant for multimedia engineering and digital content development.	The Directive does not address reuse of orphan works (works whose rights holders cannot be identified or located), which limits access to valuable historical or technical content for research. It lacks provisions for automated or AI-assisted identification of expired rights, making it difficult for developers to systematically determine the legal status of large datasets or archives. The Directive does not harmonise moral rights or national exceptions, which may affect cross-border research involving adaptation or transformation of protected works.	Clarification and possibly the introduction of complementary legislation or soft law instruments to facilitate the lawful use of orphan works for research and innovation purposes. The development of EU-wide registries or tools to automate the identification of works whose protection has expired should be supported, supporting data-driven research and digital archiving. Researchers should consult national copyright offices and institutional teams, and use public domain databases to verify the status of works, especially when engaging in cross-border or collaborative projects.

Trade Secrets Directive	The Directive provides a harmonised definition of trade secrets and legal protection against their unlawful acquisition, use, or disclosure, offering a clear framework for safeguarding confidential technical and commercial information. It explicitly allows lawful acquisition through independent discovery, reverse engineering, and observation, which supports legitimate research and innovation activities. It strengthens civil law remedies (e.g. injunctions, damages, destruction of infringing goods), giving researchers and developers legal tools to defend their proprietary knowledge.	The Directive does not address how to protect trade secrets in collaborative or open innovation environments, where confidentiality may be harder to maintain. It lacks provisions for automated or AI-assisted generation and handling of trade secrets, which are increasingly relevant in engineering and software development. Despite harmonisation, national procedural differences remain in enforcement, especially regarding confidentiality during litigation and calculation of damages.	There is the need for guidelines for managing trade secrets in collaborative R&D, including model clauses for confidentiality and data sharing. The EU could issue interpretative guidance on trade secrets generated or processed by AI systems, clarifying ownership and protection strategies. Researchers should adopt robust internal protocols for documenting, securing, and contractually managing trade secrets, especially in cross-border or multi-partner projects.
Design Directive	Includes digital, animated, and spatial designs, enabling protection of UI/UX, AR/VR, and other non-physical innovations. Unified definitions and minimum procedural standards reduce uncertainty in cross-border design protection.	Legal uncertainty persists for spare parts and modular design across Member States. Lack of clear criteria for assessing novelty and individual character in non-static or user-responsive designs. Absence of rules on authorship, ownership, and eligibility for	Full harmonisation of the repair clause should be achieved to ensure consistent rules for interoperability and circular design across the EU. Researchers should follow sectorial guidance to understand how protection standards for dynamic

	Requirement to indicate product categories improves searchability and supports prior art and FTO (freedom to operate) analyses.	protection of machine-generated outputs.	and interactive digital designs apply. When using AI tools in design, researchers should document human input and creative decisions to strengthen claims of authorship and eligibility.
EU Design Directive	Expanded definitions of "design" and "product" now include digital, animated, and spatial features, supporting innovation in software, AR/VR, and interface design. Design protection now applies to features shown visibly in the application, regardless of when or how they are visible in use—except for component parts of complex products, which must remain visible during normal use. Rightsholders can now prevent the import of infringing goods in transit, strengthening protection against counterfeiting and unauthorised replication, including via 3D printing.	Despite broader definitions, the Regulation does not fully clarify how novelty and individual character are assessed for designs that change over time or respond to user interaction. The Regulation does not address authorship, ownership, or eligibility for protection of designs created with or by artificial intelligence tools. While the Regulation improves EU-level protection, procedural differences across Member States persist, complicating cross-border design strategies.	There is a need to clarify criteria for assessing novelty and individual character in dynamic or interactive designs, possibly through implementing acts or EUIPO guidelines. EUIPO guidelines or case law development should clarify how AI-generated designs are evaluated. Engineers and developers should consult institutional and national IP offices and EUIPO early in the design process to ensure procedural alignment and consider parallel filings where fragmentation may affect protection.
CRA	Ensuring the highest possible level of cybersecurity, that is combined with the	It might take a long time to have an approved, coherent and concrete set of	Refer to standards and safeguards developed by ENISA in order to carry out a *by design*

	robustness and cybersecurity pillar under the AI Act. Annex II outlines essential security measures (e.g. encryption, data minimization, resilience), that can help guide researchers in secure digital product development. Since the conformity assessment procedures are defined, researchers can anticipate regulatory expectations for high-risk digital products, including wearable health tech. The established post-market surveillance framework enables researchers to study real-world performance and vulnerabilities, contributing to continuous improvement.	common and interoperable standards at the European level. In addition, it may be costly to implement secure-by-default features and vulnerability management in early-stage research products and to follow the post-market surveillance framework. High-risk classification limits the use of simplified internal controls, increasing regulatory burden for prototypes.	assessment under the cybersecurity ground of analysis. Reuse modular, open-source cybersecurity components and collaborate with institutional IT security teams. Participate in sandboxed conformity procedures for research prototypes, allowing testing under controlled conditions.
NIS	The inclusion of public administration and health-related services brings certain public research bodies under the protection and governance of NIS 2. Enforcement mechanisms such as fines encourage such research institutions to strengthen internal	Research institutions may face increased compliance obligations without sufficient resources or tailored guidance. The risk of sanctions penalties may pressure research institutions to adopt cybersecurity measures rapidly, even if internal capacity is limited.	Follow official guidance and participate in standardization efforts to develop appropriate solutions. Leverage networks to alleviate regulatory burden.

	cybersecurity policies and infrastructure.		

Table 10: Enablers, barriers and operational solutions

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. This sections does not aim to exemplify and cover every single gap identified in the previous analysis. It rather aims to suggest and illustrate concrete applications of legal principles and obligations to realistic scenarios that are relevant for BRIEF's research activities.

6.1. Scenario A) Reuse of health data

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

6.1.1. 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 patients to renew their 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's approach[182].
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 states that the MS must ensure that the personal data processing is subjected to appropriate safeguards when they process personal data for archiving purposes in the public interest and for research purposes, among the others. Safeguards consist in organizational or technical measures aimed at data minimization (Article 5(1) GDPR), such as pseudonymization. However, MS 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 scientific research purposes is possible, it must be done in a way that complies with the GDPR's requirements. That is, on the one hand, to ensure

[182] Source cited in Table 1.

respect for the fundamental right to data protection, and, on the other hand, to facilitate the circulation of personal data by adopting a risk management approach. This means evaluating contextual risks and adopting technical and organizational measures that are deemed essential to ensure the protection of the rights of the data subjects. Derogations are allowed but just for some specific articles and only when the GDPR obligations seriously hinder the achievement of one of the listed purposes. Thus they can be applied 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 category of personal data that Article 9(1) GDPR protects and that, according to 9(2), can be processed only under certain conditions. In an opinion of 2019 [183], the Italian Data Protection Authority considers the main legal bases to process data concerning health:

- 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 provided by the same Article 9(2) whenever they are best suited for the treatment. This is for instance the case of consent at Article 9(2)(a).

With its opinion of 2022,[184] The Italian Data Protection Authority also introduced the concept of "consenso a fasi progressive" (progressive consent) concerning health data, based on Recital 33 of the GDPR that hints at a possible derogation from the consent's requirement of specificity. This entails that the purposes of processing should be defined as specifically as possible, otherwise consent is not valid. However, in some instances, it is not possible to specifically define all the processing purposes from the onset of the research study due to the open-ended nature of scientific research. Thus, whereas a broad consent may be acceptable at the moment of data collection, the purposes need to be progressively specified as the research studies continues, so that the patients can re-consent to specific stages of the study, once these are better defined.

In the case under analysis, whenever a kind of processing was not specifically mentioned in the privacy policy, the clinical centre must also specify that data could be processed by processors or third parties for research purposes (see policy brief n. 4). This means that patients should be contacted again in case the initial consent form was unclear on whether their data could be re-used for medical research by third parties, such as the researchers in this case.
The best-case scenario would be to modify the privacy policy accordingly. However, sometimes, waiting 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 the legal basis depends on whether the clinical center is private or public. 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

[183] 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.
[184] 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

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 that govern research activities carried out by a university/research centre.

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

As far as the data governance is concerned, the data flows from the hospital to the research centre shall be governed under an agreement of joint-controllership, if the two centres are both deciding means and purposes of the re-use of the data previously collected for healthcare purposes by the hospital; or through appointing the research institute as a data processor if the hospital outsources the research activities 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 activity that aims to develop a new diagnosis system, whose outcome could benefit the hospital, even though not directly, the research group could be considered autonomous, therefore a data controller. This line of interpretation is the one proposed by the EDPB[185]. Once the platform has been developed and used to create research results, the new dataset could:

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

An agreement between the two centres shall state the governance, ownership, and access rights to such data. 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 information security 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)

6.1.3. The third issue concerns determining if AI models trained on the health data can be considered anonymous

The third issue concerns the possibility of anonymizing the AI models that could be trained on the health data collected on the platform to draw conclusions on other people. This conundrum

[185] European Data Protection Board, "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

has been addressed by the European Data Protection Board in a 2024's Opinion dedicated to the use of personal data to train machine learning models.[186] Generally speaking, it cannot be excluded that the personal data used to train the model can still be extracted or somehow obtained from the model, either intentionally or unintentionally. In such cases, the model cannot be defined anonymous, thus researchers should not consider it as such. However, determining whether the model is anonymous cannot be done *ex ante* because it depends on a case-by-case analysis. Two aspects must be carefully considered in this analysis: 1) if personal data contained in the training data cannot be extracted from the model; and 2) if the output of a query to the model does not relate to the individuals to whom the data used for training refers. The EDPB refers to three conditions that must be met to carry out the analysis. First, the model should undergo a thorough evaluation of the risks of identification. Second, this assessment should be carried out by considering all the means for re-identification that may be reasonably likely to be used by the data controller or any other party. Third, any other party should also include unintended third parties.

6.1.4. The fourth issue concerns the foundational ethical duties of researchers that train algorithms on health data

From an ethical point of view, it is helpful to use the ALTAI checklist for the part of data processing undertaken by the algorithms, in order to make the AI-based solution (in the example, the platform) ethically compliant even before the full applicability of the AI Act. The checklist addresses the 7 grounds of analysis through 63 open questions that could drive the ethical compliance activities by design and by default. If the requests of the check-list cases are met, the AI system shall be considered compliant.

In addition, academic researchers have an ethical duty under the principles of reliability, honesty, respect and accountability of the European Code of Research Integrity.[187] For example, reliability concerns the verification of the produced content and avoiding equality and non-discrimination issues. This means that scientists need to address potential sources of bias in their training datasets and the outputs that their models produce. Honesty may mean disclosing whether certain tools of AI, including generative AI, have been used for supporting the analysis of data. Respect is related not only to research participants, but also to society and environment at large. Researchers need to consider the limitations, environmental impacts, and societal effects of the AI model they develop, with an eye on privacy, confidentiality and intellectual property. This means, among the others, that the lawful and fair use of personal and non-personal data is always paramount. Accountability refers to the responsibility of researchers who must be able to justify their conduct from idea to publication, as well as provide means to other parties to oversee their conduct and assess the possible risks and misuse of the AI models they create (see also Policy Brief 1 on Accountability).

[186] European Data Protection Board, 'Opinion 28/2024 on Certain Data Protection Aspects Related to the Processing of Personal Data in the Context of AI Models' (EDPB 2024) <https://www.edpb.europa.eu/news/news/2024/edpb-opinion-ai-models-gdpr-principles-support-responsible-ai_en> accessed 22 July 2025

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

6.1.5. The fifth issue concerns the role of universities as data holders and data users within the EHDS and the FSE

In relation to electronic health data (see Section 3.1.6), universities can play a two-fold role: on one hand, they can collect such data; on the other hand, they may be interested in accessing and using health data collected by others.
Regarding the first aspect, university healthcare facilities (e.g., polyclinics, university hospitals) can play a role within the current national Fascicolo Sanitario Elettronico (FSE) system insofar as they are data controllers for healthcare purposes. In this case, such facilities contribute to feeding the FSE (Article 12, FSE 2.0 Decree). As data controller for healthcare purposes, the relevant facility must feed the FSE within 5 days of service provision (being liable for non-feeding, untimely or inaccurate feeding) and implement the required security measures (Article 25 and Annex B, FSE 2.0 Decree). In this capacity, the facility also contributes to feeding the EDS.

Universities with healthcare facilities may also be health data holders under the EHDS Regulation. Based on the definition in Article 2(2)(t), EHDS Regulation, health data holders include any legal person in the health sector who has the right or obligation to process personal electronic health data for healthcare provision, research, innovation, policy making, official statistics or patient safety or for regulatory purposes. Universities with, for example, polyclinics or university hospitals fall within this definition as controllers or joint controllers of personal data generated by the activities listed above, under the GDPR. Consequently, from 26 March 2029 or 2031 (depending on the relevant category of electronic health data for secondary use), universities may be required to make electronic health data available in the presence of a data permit issued by a health data access body. Importantly, the EHDS Regulation specifically excludes individual researchers and micro-enterprises from the category of data holders.
On the other hand, universities will be able to play the role of users of health data held by others, both within the EDS and under the EHDS. In particular, under the national system, the EDS will enable universities, as entities that institutionally pursue research activities, to access anonymized data through a request to AGENAS. Regarding access to personal data, until a subsequent decree with specific provisions is issued (as per Article 17, paragraph 4, of the EDS Decree), the provisions of the GDPR and Legislative Decree 196/2003 (also known as the Privacy Code) apply.

In particular, Article 110-bis of the Privacy Code allows the Italian Data Protection Authority to authorise further processing of personal data for scientific or statistical research by third parties when informing the data subjects is impossible or would require disproportionate efforts or could seriously compromise research objectives (see Section 3.1.1). This does not apply to Scientific Institutes for Research, Hospitalisation and Healthcare (IRCCS), public and private, for which the processing of personal data collected for clinical activity for research purposes does not constitute further processing by third parties (Article 110-bis, paragraph 4, Privacy Code). Thus, they fall under the remit of Article 110 of the Privacy Code, which does not require authorisation from the Data Protection Authority.

As data users under the EHDS Regulation, from 26 March 2029 or 2031 (depending on the relevant category of electronic health data for secondary use), universities will be able to request access to personal electronic health data held by others for scientific research purposes by obtaining a data permit from a health data access body. They will also be able to access anonymised electronic health data through an approved access request.

6.1.6. Once these issues are addressed by design, which steps must be followed for putting the platform on the market? And in the healthcare system?

Once the design part is completed, it would be interesting to discuss which following steps there could be in terms of a commercialisation of the future robotic platform. Regardless of the final user's type (private or public), if the robotic platform has a medical function, the route to take is the certification according to the MDR. The length of this process also depends on the level of risk that that will be assigned to the medical device. Moreover, there should be checks concerning the compatibility with the requirements set forth by the AI Act, especially how to categorise the AI systems (high *v.* low risk) that could be used on the platform (see Scenario B below). 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.

6.2. Scenario B) Robotic prostheses as AI systems

Within the BRIEF's research activities, robotic prostheses such as robotic knees and robotic ankles are developed with the view of distributing them as medical devices.

6.2.1. The first issue concerns the applicability of the AI Act to scientific research activities

If the robotic prosthesis is developed for pure research purposes, a superficial analysis could conclude that the AI Act does not apply (see Article 2(6)). However, it is not entirely the case, especially when the algorithm leaves the research settings to be employed in the real-world and can be classified as a medical device. Robotic prostheses integrate mechanical components and intelligent control systems and may thus be subject to the requirements imposed by the AI Act on high-risk AI systems. This means that researchers need to carefully reflect on the foreseeable uses of the AI-based artefacts that they develop, because most obligations that apply to AI systems have far-reaching repercussions and must be considered early on, namely from the first stages of research rather than at the moment of commercialization.

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

on to ensure compliance by design and by default. Ignoring this recommendation implies that it is going to be impossible to commercialize or use the system outside of research settings.

6.2.2. The second issue concerns the applicability of the definition of AI system

After having determined that scientific exceptions are narrower than they seem, another relevant question concerns the definition of an AI system. In other words, when is a certain research output considered an AI system under the AI Act (and thus, to which research outputs the AI Act applies)? This question is crucial because the answer determines whether developers and deployers should align with the applicable obligations and requirements for high-risk AI systems. At date, there is little guidance and much uncertainty on what is comprised under the definition of AI system which reads: "machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, contents, recommendations, or decisions that can influence physical or virtual environments" (Article 3(1)) (see Section 3.3.1.2). Among these components, certain ones appear more cryptical than others when it comes to mapping legal formulations to technical terms and applying them to real-world robotic prostheses.

First, autonomy refers to a system's ability to act independently of human input, either directly or indirectly. However, the concept is context-dependent: for instance, robotic prostheses respond to user intent but may require manual setup for high-level tasks that identify the specific locomotion task. Once configured, they can perform lower-level functions related to movement autonomously. Thus, different components of an AI system may exhibit varying degrees of autonomy, all of which must be considered in its assessment.

Second, according to the AI Act's Recital 12, adaptiveness refers to a system's ability to change during use, often linked to self-learning. However, adaptiveness does not always imply self-learning, especially post-deployment. In powered prostheses, adaptiveness typically refers to adjusting behavior in response to user or environmental changes without requiring the generation of new knowledge. True self-learning systems, by contrast, continuously update internal models based on real-time feedback, making all self-learning systems adaptive, but not vice versa.

Third, the notion of inference is key. The guidelines dedicated to the definition of AI systems[188] clarify that AI systems not only generate outputs but also infer how to generate them, a process tied to the pre-deployment phase. In this respect, Recital 12 distinguishes between machine learning, which learns from data, and logic- or knowledge-based systems, which reason from encoded rules. While machine learning adapts through exposure to data, knowledge-based systems apply predefined logic. However, hybrid systems increasingly combine both approaches, especially in assistive technologies like powered prostheses.

[188] European Commission. (2025, February 6). ANNEX to the Communication to the Commission Approval of the content of the draft Communication from the Commission. Commission Guidelines on the definition of an artificial intelligence system established by Regulation (EU) 2024/1689 (AI Act). https://ec.europa.eu/newsroom/dae/redirection/document/112455

There are also other interpretative issues that arise from the "legalistic" definition of AI system, when it is applied to real-world systems. These are summarized in Table 5.[189]

[189] Rossi, A., Gennari, F., Fagioli, I., Mazzarini, A., Moncelli, F., Amram, D., Crea, S., & Parziale, A. (In press). The AI system definition under the AI Act, a new nomen rosae? Proceedings of 2nd Workshop on Law, Society and Artificial Intelligence: Interdisciplinary Perspectives on AI Safety, June 10, 2025. Co-Located with HHAI: The 4th International Conference Series on Hybrid Human-Artificial Intelligence.

Table 5. An overview of the terminological and interpretative issues arising from the combined analysis of Article 3(1), Recital 12, the Guidelines on the definition of AI system and the technical definitions coming from the computer science and engineering domains, reported from Rossi et al., 2025

Art. 3(1)	Recital 12	Guidelines	Issue
"Varying levels of autonomy"	"some degree of independence of action"	Ability to generate an output "on its own"	Each component may have its own level of autonomy
"May exhibit adaptiveness"	adaptiveness "refers to self-learning capabilities"	"a system may possess adaptiveness, but not necessarily, *or* self-learning capabilities after deployment"	Not all adaptive systems have self-learning abilities
"infer [...] *how* to generate output"	"The techniques that enable inference while building an AI system include machine learning [...] and logic- and knowledge-based approaches"	ML approaches encompass "a large variety of approaches enabling a system to 'learn' " whereas logic- and knowledge-based approaches "[i]nstead of learning from data, [...] learn from knowledge including rules, facts and relationships encoded by human experts"	Increasingly blurred distinction between the two approaches
"infer [...] *how* to generate output"	"This capability to infer refers to [...] a capability of AI systems to derive models or algorithms, or both, from inputs or data"	which "underlines the relevance of the techniques used for building a system"	In ML it would be more appropriate to use terms such as learning or training, rather than inference.
[AI systems that do not infer (exception no. 3)]	"simpler traditional software systems or programming approaches and [...] systems that are based on the rules defined solely by natural persons"	e.g., classical heuristics "typically involve rule-based approaches, pattern recognition, or trial-and-error strategies rather than data-driven learning"	Pattern recognition may also be data-driven
[AI systems that do not infer (exception no. 4)]	see above	"simple prediction systems [...] whose performance can be achieved via a basic statistical learning rule, [...] fall outside the scope of the AI system definition, due to [their] performance"	Performance is not defined and may indicate either the results or the behavior of the system
-	-	"simpler traditional software systems or programming approaches", "basic data processing systems", "simple prediction systems", "reasonable degree"	These terms are not commonly used within the engineering / computer science community

6.3. Scenario C) Research on children

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

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

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

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

From a data protection perspective, Article 8 GDPR sets at 16 years old the age from which the minor could validly express their consent for services of the information society. However, this disposition leaves leeway to the Member States to set a lower age threshold which, in any case, cannot go below 13 years. In Italy, article 2 *quinquies* of the Italian Privacy Code refers to 14 years old. In any case, it is the controller, who sets the means and purposes of the data processing (Articles 4(7) and 24 GDPR), must make sure that, "*in those cases, the consent is given or authorised by the holder of the parental responsibility over the child,* ***taking into consideration available technology***[190]" (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 on the privacy information). It is also necessary to consider: i) that whenever there is a

[190] Emphasis added.

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*"[191]. 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[192]. 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 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:

[191] 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.

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

through simple language, including icons in a way to have a clear outline of the privacy risks and consequences for them. Specific legal design techniques are applicable. Information sheet, privacy policy, and informed consent shall be signed by the child and the parents shall provide an authorisation to proceed.

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

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

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

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

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

Under article 35 paragraph 1 "*where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data*". According to article 35 paragraph 3, the DPIA is surely required when "*a systematic monitoring of a publicly accessible area on a large scale*" occurs, and this is the case described here.
As data processor, you will be asked to assist the data controller (the municipality in this scenario) during the preparation of the DPIA.

In particular, combining Article 35 GDPR and the opinion of the Article 29 Data Protection Working Party (01/2015) on Privacy and Data Protection Issues relating to the Utilisation of drones, you shall assess the impact by providing:

- A) "a systematic description of the envisaged processing operations and the purposes of the processing…";

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

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

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

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

As data processors, as long as you process personal data, you will be asked to implement appropriate technical and organisational measures to ensure level of security according to Article 28 GDPR.
On the other hand, according to recital 26 GDPR, if data processed are not classifiable as personal data, you will be not obliged to respect the GDPR provisions. Given that, if the original processing involves personal data, the only way to convert them in non-personal data is the anonymisation.

The Article 29 Working Party, in the opinion 05/2014 on anonymisation techniques, clarified as the anonymisation of personal data is *per se* a personal data processing. Only after it, GDPR will not apply; before it, it will apply. Recently, the Italian Data Protection Authority affirmed that also temporary collecting of personal data, such as the people's faces before the anonymisation, constitutes data processing, therefore all the measures prescribed by Article 32 shall be respected before the anonymisation.

Still, the Italian Data Protection Authority explained how to make anonymisation techniques adequate to the scenario here described. In particular, the Authority stated that personal data collected by microphones are not adequately anonymised if the technique consists in the substitution of the inhabitants' voices with a fake voice, keeping unaltered the characteristics of the audio signal, including the content of the conversation. The Authority highlighted that the voice substitution was not adequate because from the conversation's content personal information related to the speaker and to third persons may be derived. So, this specific technique will not be considered proper anonymisation. The microphones will need to be designed in order to keep conversations not audible for data controllers and data processors, especially if the intended purpose of the microphone is to detect just loud sounds, otherwise it would be possible to identify the data subjects.

Concerning the visual contents recorded by drones, the Italian Data Protection Authority stated that a proper anonymisation technique cannot be limited to the obfuscation of faces or vehicle number plates. In facts, data subjects are still identifiable through other characteristics such as the body type, clothing, place of the recording etc. Moreover, this information may be combined with data collected by the microphones and with other data collected by thirds, so resulting in personal data after the combination.
Furthermore, the fact the video resolution is not high is not enough to prove a correct anonymisation, even more if video data are combined with audio data.
To conclude, the anonymisation must guarantee the result of the impossible identification of the data subjects.

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

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

In case of the development and placement on the market of a posture support for work-time equipped with an AI system as a safety component, there are two relevant pieces of legislation: the Machinery Regulation (MR) and the Artificial Intelligence Act (AIA). The reason why the Medical Device Regulation (MDR) is not involved is because the described posture support does not fulfil the requirements set by the MDR to classify it as a medical device[193]. In fact, it is not intended to heal the worker (i.e., it does not have an intended medical purpose), but just to enhance his/her work conditions.

If the manufacturer aims to place the product on the market, specific procedures must be followed. Once these are observed, the manufacturer will obtain the CE marking, which certifies the conformity of the support with the EU standards for health and safety. Both MR and AIA procedures must be followed (AIA works as a horizontal regulation, thus its rules will be added to the MR ones).

In this case, the manufacturer of the support is also the developer of the AI system.

6.4.2. Conformity under Machinery Regulation.

Firstly, the manufacturer shall identify the correct conformity assessment module provided by the MR. It lays down four different modules[194]. When artificial intelligence (referred to by the regulation as fully or partially self-evolving behaviour using machine learning approaches ensuring safety functions) is involved, according to annex I[195], the manufacturer shall undergo the conformity assessment indicated by Article 25 paragraph 2. In case of AI, the latter prescribes, alternatively, 3 types of procedures on manufacturer's choice: 1) EU type-examination (module B), followed by conformity to type based on internal production control

---

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

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

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

(module C); 2) conformity based on full quality assurance (module H); 3) conformity based on unit verification (module G).

Once the module is selected, then several obligations are set.
The combination of modules B and C requires the manufacturer to undergo two different assessments. Firstly, module B describes the EU-type examination, which entails an EU-notified body examination; if at its end the support is compliant with the regulation, the examination will result in a certificate of conformity. This procedure must be combined with the one described under module C (conformity to type based on internal production control), which requires the manufacturer to ensure that the support is compliant with the type described in the EU type-examination certificate. Later, the regulation prescribes the affixation of the CE marking on the support in conformity with the type described in the EU type-examination certificate. The procedure ends once the manufacturer draws up an EU declaration of conformity for the support and keeps it at the disposal of the national authorities for at least 10 years after the support has been placed on the market or put into service.

Moving forward, module H (conformity based on full quality assurance) prescribes the manufacturer to operate an approved quality system for design, manufacture and final product inspection and testing.
The manufacturer shall apply for an assessment of its quality system to the notified body of its choice. The quality system shall ensure compliance of the support with the requirements of this Regulation. All the elements, requirements and provisions adopted by the manufacturer shall be documented in a systematic and orderly manner in the form of written policies, procedures, and instructions.
The notified body shall assess the quality system to determine whether it satisfies the prescribed requirements. The notified body's decision shall contain the conclusions of the audit and the reasoned assessment decision. Once received the decision, the manufacturer shall undertake to fulfil the obligations arising out of the quality system as approved and to maintain it so that it remains adequate and efficient.

Still, the manufacturer shall keep the notified body that has approved the quality system informed of any intended change to the quality system and the latter shall evaluate any proposed changes. Successively, the manufacturer shall affix the required CE marking and draw up a written EU declaration of conformity for the support and keep it at the disposal of the national authorities for at least 10 years.
The last possible choice is the module G (conformity based on unit verification). Under it, the manufacturer will make available proper technical documentation, to let the notified body be able to assess the support's conformity with the relevant essential health and safety requirements set out in Annex III and shall include an adequate analysis and assessment of the risks.

A notified body chosen by the manufacturer shall carry out appropriate examinations and tests, to check the conformity of the support with the applicable essential health and safety requirements set out in Annex III or have them carried out. The notified body shall issue a certificate in respect of the examinations and tests carried out. The manufacturer shall keep the

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

6.4.3. Conformity under Artificial Intelligence Act.

The framework previously explained applies to support with AI safety components. These types of supports are regulated also by the Artificial Intelligence Act, once into force. According to article 6 AIA, all the systems covered by the legislation indicated in Annex I are considered high-risk systems under the AIA, therefore several obligations are mandated upon the manufacturer. Annex I explicitly refers to the Machinery Regulation, thus, AI systems working as safety component in machineries (as described by Article 3 MR) are considered high-risk systems under the AIA.
Manufacturers of such high-risk AI systems shall run a conformity assessment procedure before their products can be sold and used in the EU. They will need to comply with a range of requirements including testing, data training and cybersecurity.
The risk management obligations (art 9 AIA) first require identification of the reasonably foreseeable risks that the support can pose to health, safety or fundamental rights when it is used in accordance with its intended purpose. Consequently, it is prescribed the adoption of appropriate and targeted risk management measures designed to eliminate or reduce the risks identified. The measures shall be such that the relevant residual risk associated with each hazard, as well as the overall residual risk of the high-risk AI systems, is judged to be acceptable.

Moreover, high-risk AI systems which make use of techniques involving the training of AI models with data shall be developed on the basis of training, validation and testing data sets that meet the quality criteria provided by Article 10 AIA. Training, validation and testing data sets shall be relevant, sufficiently representative, and to the best extent possible, free of errors and complete in view of the intended purpose. They shall have the appropriate statistical properties, including, where applicable, as regards the persons or groups of persons in relation to whom the high-risk AI system is intended to be used.
Moreover, according to Article 13, the support shall be designed and developed in such a way as to ensure that their operation is sufficiently transparent to enable deployers to interpret a system's output and use it appropriately.
Among the several duties set for, some of them may overlap with the ones provided by the machinery regulation. For example, there is no clear definition of how to harmonise the conformity procedures set for by the MR and the AIA. Or, the log recording is prescribed both by AIA (art. 12) and MR (Annex III, part B, 1.2.1, f). Technical documentation described by article 11 AIA may overlap with the one set for by module G, Annex I, MR.
Furthermore, AIA and MR lack harmonised standards. It is still possible to apply the ones designed under the machinery directive (EN ISO 14121-1 – Safety of machinery – Risk assessment – Part 1: Principles), still in force until 2027, but they should be updated to face AI challenges.

7. MAIN PRINCIPLES

As a result of the cross-fields analysis above-introduced and the possible applications within research settings, we provide 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 many of the previously cited legal acts, in particular the GDPR and the AI Act, given their crucial relevance for the BRIEF research activities.

The principle of accountability refers to the possibility, for both controllers and processors, of always being able to justify their data processing activities. It is the motor of data protection governance, explicitly stated in general terms in Article 5(2) GDPR and concretely developed in Chapter IV, which outlines the duties and obligations of both processors and controllers. Examples include the obligation to keep records of processing activities (Article 30), conduct Data Protection Impact Assessments (Article 35), and ensure the security of processing (Article 32). Accountability is also intrinsically linked to the principle of data protection by design and by default (Article 25 GDPR), which requires that products, services, and methodologies be developed in a way that prioritizes privacy and data protection from the outset. This obligation means that data controllers "should be able to demonstrate that they [implement] the appropriate measures and safeguards in the processing to ensure that the data protection principles and the rights and freedoms of data subjects are effective".[196]

In the framework of BRIEF, accountability warrants particular attention as it is a cornerstone of responsible research and other regulatory domains, such as data use and AI development. Under the GDPR, it shifts the burden of data protection from data subjects to data controllers, who must not only comply with legal requirements but also adopt a proactive attitude—constantly seeking ways to improve data processing and reduce its invasiveness. This proactive stance involves documenting the motivations behind technological, organizational, and economic choices, ideally in written form, making tools like data management plans essential. As the Article 29 Working Party defines it, accountability means "showing how responsibility is exercised and making this verifiable",[197] through concrete and demonstrably effective measures that foster trust. It is double-faced: it protects data subjects while shielding organizations from legal, economic, and reputational risks.[198] The GDPR's accountability framework is thus composed of various components, including a risk-based assessment that identifies specific risks and devises proportional technical and organizational mitigation measures. In the context of scientific research, respecting legal and ethical duties through accountability can ultimately enhance the quality and integrity of research itself.[199]

[196] European Data Protection Board, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default (2019), p. 5
[197] Article 29 Working Party, 'Opinion 3/2010 on the Principle of Accountability' (2010), p.7
[198] Ibid.
[199] 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.

Similarly, the principle of accountability in the AI Act reflects a foundational commitment to ensuring that AI systems are developed, deployed, and monitored in a manner that is transparent, justifiable, and aligned with Union values. Much like Article 5(2) of the GDPR, which establishes accountability as a cornerstone of data protection governance, the AI Act embeds accountability through concrete obligations for providers and users of high-risk AI systems (for example, those that develop or use AI-based medical devices). As mentioned earlier, these include requirements for maintaining documentation, conducting risk assessments, and devising transparency measures – all of these obligations need to be considered and implemented early on by AI developers in view of putting the system on the market. Furthermore, in line with the principles of trustworthy AI elaborated by the HLEG, the AI Act promotes a culture of ethical and legal diligence, encouraging actors to justify technological and organizational choices, with the explicit aim of fostering trust in the use of AI technologies while safeguarding fundamental rights. This proactive stance on accountability not only aligns with the GDPR's ethos but also supports innovation and responsible research, demonstrating that legal compliance and ethical integrity are not obstacles but enablers of scientific and technological progress.

Accountability is closely linked to the principle of **transparency**, which refers to the obligation the controller has to inform the data subjects (e.g. patients, research participants, or more generally users) about the ways in which their data is being processed[200]. 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 principles of transparency and explainability are increasingly emphasized in the AI Act as well. These principles require that AI systems be designed and deployed in ways that allow for traceability, user awareness, and meaningful human oversight. Transparency involves informing users when they interact with AI, clarifying system capabilities and limitations, and documenting system behavior—paralleling GDPR obligations. Explainability, particularly for high-risk AI systems, ensures that outputs are interpretable and justifiable, echoing the GDPR's Article 22 on automated decision-making.

Another foundational principle is **fairness**, but it has not always been easy to define, as it clearly interacts with those principles mentioned above that we can read at article 5(1)(a) GDPR[201]. 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*"[202]. 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

[200] Council of Europe and EU Fundamental Rights Agency (FRA), *Handbook on European data protection law* (Luxembourg: 2018), 119-122.
[201] 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.
[202] Ibid.

could be important for the accuracy of data processing results. Analogously, the principle of fairness in the AI Act is rooted in the broader commitment to human-centric and trustworthy artificial intelligence, aligned with the values enshrined in the Charter of Fundamental Rights of the European Union. Fairness is operationalized through requirements that aim to prevent discrimination and bias, particularly in the development and deployment of high-risk AI systems. The regulation requires that AI systems be designed and used in a manner that respects individuals' fundamental rights, including non-discrimination, equality, and justice. This includes the implementation of privacy-preserving measures and safeguards when processing sensitive data to detect and mitigate algorithmic bias. The AI Act also draws on the Ethics Guidelines for Trustworthy AI, which identify fairness as one of the seven key requirements, emphasizing the need to address power asymmetries and protect vulnerable groups such as children, persons with disabilities, and historically disadvantaged communities, similarly to the GDPR. Both regulations emphasize the need for a fair balance between technological innovation and the protection of fundamental rights, recognizing that fairness is not a static rule but a dynamic principle that must adapt to specific contexts and societal impacts. Ultimately, fairness in both frameworks serves as a safeguard against systemic bias and a foundation for trustworthy technology development and use.

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 data are pseudonymised, no attempts at individual re-identification shall be undertaken.
Accountability	To define information to be selected in a survey regarding the	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	profiling of participants	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 for the data governance purposes	Roles and responsibilities shall be allocated considering the concrete activities and life-cycle of the research more than possible formal constrains.
Transparency		The information sheet and the privacy policy shall include details on the governance of the study and on the data governance, especially to facilitate the exercise of participants' rights.
Fairness		The roles and responsibilities allocation shall avoid any discriminatory conditions.

Table 11: Main guiding principles of the GDPR and how they can help solve practical hurdles to research activities

Principle	*Practical need*	*Interpretative solution*
Accountability	Commercialize AI-powered medical devices	Ensure design choices are traceable through appropriate documentations, carry out risk assessments following established frameworks and put in place mechanisms to ensure that all obligations are met along the research and development chain, by including all relevant personnel members, even when the IA system is developed within research settings. Ensure compliance with other applicable regulations and obtain CE marking.
Transparency		Document system design choices early in an understandable manner on as information will need to be included in the instructions for deployers.
Fairness		Keep in mind that users of the device may be vulnerable people (patients), thus design for and with them, anticipating possible risks
Accountability	Define roles and responsibilities along the R&D value chain	Assign tasks and responsibilities to anybody who may be directly and indirectly involved in the development phases, trace where components come from (e.g., when online libraries are re-used) and how they are

		licensed, and involve ethics and legal team early on.
Transparency		Document the task assignments in a preservable fashion
Fairness		Assign appropriate responsibilities to fitting roles, with a critical eye on the sustainability of the assignments (e.g., fixed term vs permanent jobs, seniority, etc.)
Accountability	Carry our risk assessment for high-risk systems	Conduct the R&D activities with a risk-based approach from the onset. Avoid development when risks are too high and ensure the countermeasures that are implemented are effective. When personal data are processed, the risk assessment can build on top of the data protection risk assessment.
Transparency		Document identified risks, their evaluations, measures taken and justifications for those, and their effectiveness.
Fairness		Consider vulnerable individuals and groups who may be impacted by the use of the system.

8. PRELIMINARY POLICIES AND RECOMMENDATIONS

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

To this end, we addressed the following policies and recommendations impacting on two different aspects of the life-cycle of the research. The first one refers to a checklist for developers, innovators, and researchers aiming to address the main pillars of the ethical-legal compliance during the different steps of the life-cycle of the research.

Preparatory activities	*Comments*
Develop an ethical-legal compliance strategy	If you are unfamiliar with the concepts of impact assessment, accountability, pseudonymisation, data management plan, open data, open science, take time to extend your skills and competence.

Check whether the development you your idea implies either personal data processing, or non-personal data processing, or volunteers' engagement, or algorithms and their training, etc.	Calls for funding may include tailored templates for self-assessing these profiles.
Check skills and competence in your team: if you are not covering the ethical-legal implications of your idea, ask for advice.	Some issues may be addressed directly from the institutional roles (*e.g.* the Intellectual Property Office, Data Protection Officer, etc.), other tasks might require further specialistic advice.
Research Management	*Comments*
Allocate time and resources to develop the applicable ethical-legal framework to the life-cycle of the research, considering: a. The EU strategy on Data, Public Health, and AI, where relevant for your life-cycle. b. Possible specific safeguards implemented at national, or local level for a given sector.	Take into account possible initiatives entering into force in the near future/during the research life-cycle. If a conflict of application arises, you will take the decision considering the principles of accountability, transparency, and fairness.
Develop a data management plan in order to: a. Define datasets that the life-cycle of the research will generate b. Identify organisational and technical safeguards to collect, process, store, share, and reuse datasets according to the characteristics of data.	If one(more) protocol(s) shall be submitted to the competent ethical committee(s), allocate proper time and resource to develop it (them). If one(more) data sharing agreements shall be developed, allocate proper time and resources. If a data protection impact assessment / fundamental rights impact assessments shall be developed, allocate proper time and resources.
Research development	*Comments*

Identify monitoring measures to ensure the proper development of the compliance strategy.	Allocate roles and responsibilities either among partners or in your team.
Identify proper measures to ensure fundamental rights exercise from individuals and reporting activities.	If you are developing AI-based solutions, apply the ALTAI checklist by default. In addition, be mindful of the requirements of the AI Act that apply if the AI system is meant to, or could potentially, be put in use outside research settings or commercialized, especially when it comes to AI systems that can be categorized as medical devices, and thus would be classified as high-risk AI systems under the AI Act. If you are dealing with the digital data, services, platforms, software and other digital assets dimension, check the ENISA standards for cybersecurity and robustness. If you involve vulnerable individuals / groups (*eg* children, patients, refugees) check whether institutional, local, international standards are required.
Identify assessment checks to balance different principles and rights.	Compliance activities may require the interplay of different soft skills to take the more appropriate decision that may change over the life-cycle of the research.
Dissemination and Exploitation	*Comments*
Develop a dissemination and exploitation plan aligned with the adopted strategy of data	*e.g.,* in case of Open Science, the Data Management Plan shall be coherent with the dissemination and exploitation strategy.
Adopt a procedure for making information public: the use of website, online platforms, social media, contacts processing for communication and dissemination purposes, pictures and reports publications, newsletters, surveys etc	Keep in mind the principle of minimisation and what you have declared in the privacy information / information sheet.

Table 12: Preliminary best practices part 1, issued from D7.3 Cross-field regulatory analysis

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 13: Preliminary policy recommendations part II, issued from D7.3 Cross-field regulatory analysis

Following these general best practices and policy recommendations produced as outcomes of the first iteration of the cross-field regulatory analysis (D7.3), the Law and Polic Hub has elaborated a number of specific best practices and policy recommendations that span across disciplinary domains. Below, we summarize the main contributions that we detail in D7.6 "Policy Design and Advice", where we also provide a plan for future work.

Final proposed policy recommendations:

- the definition of specific requirements for data portability that are meant to solve the terminological confusion adopted by many legislations and legislative proposals within the European Digital Strategy (Policy Recommendation 1 – PR1);

- a scientificaly grounded multi-layered solution that integrates personalized dynamic consent, user-centric interface design, and semantic interoperability that should inform the work of the Commission on the rulebook for data altruism consent (PR2);
- a redefinition of anonymization as a contextual, ethically grounded, and spectrum-based governance practice to guide harmonized and transparent implementation under the EHDS (PR3);
- a proposal for legislative and procedural alignment between Italy's FSE 2.0 and EDS systems and the EHDS, through opt-out provisions, institutional consolidation, and phased implementation (PR4);
- a clarification of the roles and responsibilities of the actors that are involved in the accountability measures established for AI (PR5);
- the redefinition of the concept of justice that underlies that of fairness in machine learning so that it the metrics and techniques that are employed in this regard are compliant with EU anti-discrimination laws (PR6);
- a proposal for increasing the terminological clarity about subliminal, manipulative and deceptive techniques of the AI Act to overcome potential under- or over-encompassing definitions (PR7);
- a solution to the issues of uncertainty and slowdown that is caused by the Medical Device Regulation's regulatory process and the lack of notified bodies (PR8);
- a multifaceted strategy for integrating personalized medicine into healthcare, combining humanistic clinical practice with updated regulatory frameworks for equitable and secure implementation (PR9);
- a proposal for extending the liability of manufacturers of defective components to importers and authorized representatives to ease the process of consumers' compensation (PR10);
- a proposal for risk-based decision-making in software development for AI-powered products, supported by contractual safeguards and cybersecurity certification standards (PR11);
- a revisitation of the concept of personal injury compensation within the robotic context (PR12);
- a recommendation for harmonizing liability standards and clarifying legal concepts under the revised Product Liability Directive, while promoting insurer involvement and regulatory coordination (PR13);
- a recommendation for a clearer involvement of the ENISA (European Union Agency for Cybersecurity) in the official definition of emerging cybersecurity issues in AI (PR14);
- the introduction in the AI Act proposal of a deadline for the reconsideration of the adopted standards and common specifications to account for technical developments and emerging cybersecurity threats (PR15).

Final proposed best practices:

- a recommendation to adopt reusable, transparency-enhancing design patterns for privacy communication in research, supported by authoritative resources like CNIL's library (BP1);

- a redesign of privacy and consent policies using user-centered transparency, contextual integrity, and tailored communication to support ethical data sharing in digital health (BP2);
- a recommendation to design multimedia consent forms using strategic reading cues, layered content, and ethical co-design to support informed and context-sensitive decision-making (BP3);
- a recommendation for developers to adopt human-centered privacy engineering practices aligned with ISO standards (BP4).
- a best practice for implementing personalized dynamic consent platforms for data altruism to ensure ethical, adaptable, and legally compliant health data sharing (BP5).
- a recommendation to implement layered, GDPR-compliant consent mechanisms for data altruism in healthcare, supported by transparency, harmonized interpretation, and anonymization safeguards (BP6);
- a structured approach for public research actors to support responsible innovation in personalized medicine through FAIR data, accountability, proactive governance, and coordinated stewardship (BP7);
- a recommendation to apply GDPR principles to AI-based medical systems by ensuring transparency, human oversight, and non-discrimination through proactive, risk-based governance (BP8);
- a structured framework for AI developers to enhance MM-LLM reliability through expert validation, explainability techniques, and safeguards against automation bias (BP9);
- a recommendation for developers to design modular AI control systems for medical devices, integrating human-in-the-loop optimization, clinical validation, and early regulatory engagement (BP10);
- a recommendation for AI developers to standardize terminology and interpretation methods under the AI Act, enabling interoperable, accountable, and future-proof innovation (BP11);
- a recommendation to strengthen personalized medicine through inclusive research, stakeholder engagement, and the preservation of the therapeutic alliance in AI-supported care (BP12);
- a recommendation for dynamic evaluation models, risk-based assessment, real-world evidence integration, and participatory design to support safe and patient-centered adoption of digital health technologies (BP13);
- a proposal for multidimensional evaluation, stakeholder-specific indicators, simulation-based methods, and participatory frameworks to ensure sustainable and system-aligned HTA in personalized medicine (BP14);
- a strategy for structural digital health literacy, inclusive training, patient involvement, personalized support services, and outcome-based evaluation for participatory, equitable, and user-centered healthcare systems (BP15);
- an approach to economic, organizational, educational, regulatory, and ethical barriers through evidence-based models, interdisciplinary teams, participatory training, equitable access, and privacy-compliant integration of robotics in rehabilitation (BP16).
- a framework for reinforced safety expectations, post-market accountability, transparent liability rules, narrow interpretation of exemptions, and harmonized strict liability models for AI-powered medical devices (BP17);

- a guideline for transparent design, interdisciplinary collaboration, AI literacy, lifecycle accountability, and bias-aware data governance to ensure compliant and trustworthy deployment of AI systems in healthcare (BP18);
- a recommendation for proactive risk management, jurisdiction-sensitive deployment, compliance documentation, multimedia instructions, and litigation preparedness to ensure defensible and safe active prostheses under evolving liability regimes (BP19);
- a strategy for liability assessment through objective state-of-the-art evidence, mitigation documentation, and narrow interpretation of exemptions for software vulnerabilities in AI-powered medical devices (BP20).

CONCLUSIONS

This report summarises the main ethical and legal challenges that arise in a R&D&I life-cycle and seeks to provide methodological solutions to deal with the balance between different rights and obligations. By adopting a comparative perspective (Section 2), the LaPoH has provided an overview of the legal frameworks that are applicable to the BRIEF's research activities, with a focus on the European Data Strategy on personal and non-personal data, health law, machinery regulation, artificial intelligence, intellectual property and cybersecurity. The cross-field analysis (Section 4) has underlined the elements that may enable research, as well as the many gaps that need to be bridged (Section 5). A case study methodology applied to five practical scenarios (Section 6) has contributed to the further examination of some of the most relevant issues and the development of reusable solutions that can be applied to similar contexts. Lastly, overarching principles for compliance by design have been outlined (Section 7). Policy recommendations and best practices have been elaborated (see "D7.6 Policy Design and Advice") as a further result of the iterative cross-field analysis described in these pages. Other results have been published in scholarly publications and policy briefs, and disseminated through awareness panels and conferences, as detailed in "D7.7 Research dissemination and awareness".

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

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

COUNCIL DIRECTIVE of 25 July 1985 on the Approximation of the Laws, Regulations and Administrative Provisions of the Member States Concerning Liability for Defective Products (85/374/EEC), OJ L 210 29

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

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Published: OJ L 281, 23.11.1995, p. 31–50).

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016, pp. 1–30.

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), OJ L 333, 27.12.2022, pp. 80–152.

Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (recast) PE/28/2019/REV/1, OJ L 172, 26.6.2019, pp. 56–83

Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on Liability for Defective Products and Repealing Council Directive 85/374/EEC (Text with EEA Relevance) OJ L, 2024/2853, 18.11.2024

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

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

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

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

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

Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights (Text with EEA relevance), OJ L 157, 30.04.2004, p.45-86.
Directive 98/44/EC of the European Parliament and of the Council of 6 July 1998 on the legal protection of biotechnological inventions, OJ L 213, 30.07.1998, p. 13-21.
Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful, use and disclosure (Text with EEA relevance), OJ L 157, 15.06.2016, p. 1-18.
Directive 98/71/EC of the European Parliament and of the Council of 13 October 1998 on the legal protection of designs, OJ L 289, 28.10.1998, p. 28-35.
Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use or disclosure [2016] OJ L 157/1
Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016, pp. 1–30.
Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), OJ L 333, 27.12.2022, pp. 80–152.
Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery and amending Directive 95/16/EC (recast) *OJ L 157, 9.6.2006, p. 24–86.*
Proposal for a Regulation of the European Parliament and of the Council on standard essential patents and amending Regulation (EU) 2017/1001 (Text with EEA relevance), 27.04.2023, COM(2023) 232 final.
Regulation (EU) No 1257/2012 of the European Parliament and of the Council of 17 December 2012 implementing enhanced cooperation in the area of the creation of unitary patent protection, OJ L 361, 31.12.2012.
Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) OJ L 277, 27.10.2022, pp. 1–102.
Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union PE/53/2018/REV/1 OJ L 303, 28.11.2018, pp. 59–68.
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) OJ L 152, 3.6.2022, pp. 1–44
Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) OJ L, 2023/2854, 22.12.2023.
Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA relevance) PE/17/2022/REV/1 OJ L 265, 12.10.2022, p. 1–66
Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847.
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) 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.

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

Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC *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 *OJ L 117, 5.5.2017, p. 176–332.*

Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act), OJ L, 2024/2847, 20.11.2024.

Regulation (EU) 2023/1230 of the European Parliament and of the Council of 14 June 2023 on machinery and repealing Directive 2006/42/EC of the European Parliament and of the Council and Council Directive 73/361/EEC PE/6/2023/REV/1 OJ L 165, 29.6.2023.
COMMISSION IMPLEMENTING REGULATION (EU) /... laying down a list of specific high-value datasets and the arrangements for their publication and re-use. C/2022/9562 final

European Commission. (2020). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A European Strategy for Data. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0066

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

European Commission, 'ANNEX to the Communication to the Commission. Approval of the Content of the Draft Communication from the Commission - Commission Guidelines on the Definition of an Artificial Intelligence System Established by Regulation (EU) 2024/1689 (AI Act)' <https://ec.europa.eu/newsroom/dae/redirection/document/112455> accessed 10 April 2025

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

DECRETO LEGISLATIVO 18 maggio 2018, n. 65. Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.

DECRETO LEGISLATIVO 30 giugno 2003, n. 196 Codice in materia di protezione dei dati personali ((, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonchè alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE)).

Legge 25 settembre 2025, n. 223. Disposizioni e deleghe al Governo in materia di intelligenza artificiale.
Legge 29 aprile 2024, n. 56. Conversione in legge, con modificazioni, del decreto-legge 2 marzo 2024, n. 19, recante ulteriori disposizioni urgenti per l'attuazione del Piano nazionale di ripresa e resilienza (PNRR).
Garante per la Protezione dei Dati Personali, "Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica pubblicate ai sensi dell'art. 20, comma 4, del d.lgs. 10 agosto 2018, n. 101 - 19 dicembre 2018 [9069637]." Dec. 19, 2018.

Garante per la Protezione dei Dati Personali, "Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica ai sensi degli artt. 2-quater e 106 del Codice - 9 maggio 2024 [10016146]." maggio 2024. Accessed: Jul. 14, 2025. [Online]. Available: https://www.garanteprivacy.it:443/home/docweb/-/docweb-display/docweb/10016146

Garante per la Protezione dei Dati Personali, "Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 del d.lgs. 10 agosto 2018, n. 101 [9124510]." 2019.

Garante per la Protezione dei Dati Personali, "Parere ai sensi del ai sensi dell'art. 110 del Codice e dell'art. 36 del Regolamento - 30 giugno 2022 [9791886]." giugno 2022. Accessed: Jul. 14, 2025. [Online]. Available: https://www.garanteprivacy.it:443/home/docweb/-/docweb-display/docweb/9791886
Decreto del Presidente del Consiglio dei ministri, 29 settembre 2015, n. 178, Regolamento in materia di fascicolo sanitario elettronico (15G00192).
Ministero della Salute, Decreto 7 settembre 2023, Fascicolo sanitario elettronico 2.0 (23A05829), in GU, Serie Generale n. 249 del 24-10-2023

Ministero della Salute e Ministero dell'Economia e delle Finanze, circolare 17 febbraio 2021, Fascicolo sanitario elettronico (FSE): indicazioni per eliminazione consenso all'alimentazione del FSE (art. 11 DL 34/2020), 0002031-17/02/2021-DGSISS-MDS-P.
Ministero della Salute, Decreto, 31 dicembre 2024 Istituzione dell'Ecosistema dati sanitari (25A01321), in GU Serie Generale n. 53 del 05-03-2025.
Ministero della salute, Decreto 26 gennaio 2023, Individuazione di quaranta comitati etici territoriali

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.

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

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

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

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
SkovÆgvBilka LavprisvarehusA v Jette Mikkelsen and Michael Due Nielsen EU:C:2005:46

C-621/15 N.W. and Others v. Sanofi Pasteur MSD SNC and Others

González Sánchez. Case C- 402/03
Judgment of the Court (First Chamber) of 4 September 2025. European Data Protection Supervisor v Single Resolution Board. Case C-413/23 P

International Legal Instruments

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

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

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

Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS No. 108) (1980).

ANNEX

As mentioned multiple times, the legal framework has evolved during the iterative drafting of this report. Hence, the Design Directive (Directive 98/71/EC)[203] and the Community Design Regulation (Council Regulation No 6/2002) (D7.3 and D7.4) were amended by the Design Directive and the EU Design Regulation. Moreover, the AI Liability Directive proposal[204] was withdrawn in 2025. For the sake of transparency, we report here below the content that was included in the two previous versions and that was erased or replaced in the drafting of this last iteration of the report.

[203] Directive 98/71/EC of the European Parliament and of the Council of 13 October 1998 on the legal protection of designs. OJ L 289, 28.10.1998, pp. 28–35
[204] 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. The legislative draft was retracted in 2025.

Previous draft on the The AI Liability Directive proposal, Section 3.4:

The purpose of the AI liability directive proposal is to improve the functioning of the internal market by laying down **uniform requirements for non-contractual civil liability for damage caused with the involvement of AI systems**. The overall objective of the proposal is to promote the rollout of trustworthy AI, to harvest its full benefits for the internal market by ensuring victims of damage caused by obtain **equivalent protection to victims of damage caused by products** in general. The proposal also aims to **reduce legal uncertainty** for businesses developing or using AI regarding their possible exposure to liability and prevent the emergence of fragmented AI-specific adaptations of national civil liability rules.
The AI Liability Proposal (AILP) revolves around two main articles, Article 3 which sets some rules concerning the **disclosure of evidence procedural rule.** In sum, the claimant can ask the judge to compel the AI provider to show how the AI system works if it is not easily understandable for the claimant. During this procedure IP rights should be safeguarded. If the AI provider refuses to comply with the court order, the judge can presume a causal link between the damage sustained by the claimant and the AI system way of working.
Article 4 instead gives a set of detailed rules on **how the claimant can build their case in order for the judge to presume the presence of a causal link**. The article is divided into two parts: Article 4(1) concerns all the AI systems that are not high risk, for which the claimant needs to prove all of the following conditions: *"*

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

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

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

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

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

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

Previous draft on the AI Liability Directive Proposal in Section 4, Table 5:

AI civil liability directive proposal (COM/2022/496 final)	*It involves new rules (especially Articles 3 and 4) concerning the harmonization of tort liability rules whenever an AI system contributes or directly causes a damage. However, the AILP*

	will most probably be modified at length as it was closely connected to the AI Act official proposal of 2021 when GPAIs where not yet present. It might take a long time before there will be an agreed text on this issue.

Previous draft on the AI Liability Directive Proposal in Section 5.3, Table 10:

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.*

Previous draft on the Design Directive in Section 4 Table 5:

The Design Directive, while harmonising the national legislations of the Member States, creates a common ground for the legal protection of industrial designs by introducing precise definitions for the key terminology, clarifying **the eligibility criteria for legal protection, the scope and term of the legal protection** conferred upon designs, as well as the **limitations to the exclusive rights** of the registered design holder.

The key take-aways of the Design Directive are, especially with respect to the BRIEF activities, as follows:

- Article 1 of the Directive defines the key terminology as follows:
  - The **term "design"** refers to "the appearance of the whole or a part of a product resulting from the features of, in particular, the lines, contours, colours, shape, texture and/or materials of the product itself or its ornamentation".
  - The **term "product"** which is essential to the definition of "design" is articulated as "any industrial or handicraft item, including inter alia parts intended to be assembled into a complex product, packaging, get-up, graphic symbols and typographic typefaces". Whereas computer programs are explicitly excluded from the scope of the definition of "product", the broadly articulated description of the term as such applies to 3D printed products or parts thereof.
- Articles 2 and 3(1) of the Directive crystalize that the legal protection envisioned for industrial design requires the **registration of the design at the competent intellectual/industrial property office in the country** in which legal protection is sought.

- Article 3(2) of the Directive sets the **eligibility criteria** for legal protection. According to this provision, a design would be protected by a design right only if it is **new and has individual character**. In light of the regulation within Article 4, a design would be deemed new only if "no identical design has been made available to the public" before. As to the other criteria, Article 5 holds that a design would be considered to have an individual character if "the overall impression it produces on the informed user differs from the overall impression produced on such a user by any design which has been made available to the public before (...)".
- Article 7 contours the eligibility criteria for legal protection by clarifying that designs that are **dictated by the technical function of the product or by the standards** to enable the compatibility of a product with others would **not be deemed new or individual character.**
- Likewise, Article 8 of the Directive excludes designs that are **contrary to public policy or morality** from the scope of the Directive.
- A registered design, as per Article 12 of the Directive, would **entitle the rightsholder to the exclusive rights to use the design and to prevent third parties from using the design**. The use of the design encompasses acts such as launching a product to the market which bears the design; and importing, exporting or stocking a product as such.
- As regulated by Article 10, the term of legal protection conferred to the rightsholder starts from the date of the filing of the registration application and lasts **for 5 years**. The term of protection can be renewed for 5-year periods multiple times, however up to a maximum of 25 years.
- Article 13(1) of the Directive provides a regulation that is of pivotal importance for BRIEF activities, as it identifies the **limitations to the exclusive rights** of the design rightsholder. According to this provision, the performance of the following acts does not conflict with the exclusive rights of the design rightsholder:
    - Acts done in privately and for non-commercial purposes,
    - Acts done for experimental purposes,
    - Acts of reproduction for making citations or for teaching.

  However, these acts shall be compatible with fair-trade practices and shall not unduly prejudice the normal exploitation of the design. Additionally, these acts shall be accompanied by the indication of the source of the design in use.

Previous draft on the Community Design Directive in Section 4 Table 5:

The Community Design Regulation sets the norms for the EU-wide protection of industrial designs. Therefore, the content of the Regulation is largely procedural as the vast majority of the legal provisions encompassed within the Regulation are concerned with the **application to be submitted to the EUIPO for the registration of an industrial design**, the examination of such an application, the possible consequences of the examination process, the establishment of the design courts to resolve legal disputes concerning Community designs and the like.

Whereas the substantial provisions of the Regulation closely follow the letter of the Design Directive, the legal provisions on the protection of unregistered designs constitute a novel aspect of the Regulation, as this aspect has not been covered within the Design Directive. Therefore, it is worth briefly reflecting on the legal protection of unregistered designs.

The Regulation adopts the same definitions for "design" and "product" as well as the eligibility criteria required for acquiring design rights. Nevertheless, the novelty and individual character criteria are slightly adapted to the features of unregistered designs, as it is no longer possible to take the date of application for the registration as a reference point. In this regard, Article 5(1)(a) of the Regulation holds that the **benchmark for novelty and individual character would be determined by considering the designs that have existed before the design** in question has been made available to the public.

Similarly, Article 11(1) stipulates that the term of protection envisioned for unregistered designs would start **from the date on which the design has been made available to the public for the first time** within the EU. The design will be under legal protection for a three-year period starting from this date. As opposed to the term of protection envisaged for registered designs, the term of protection for registered designs is not subject to renewal.

Finally, Article 19(2) introduces an important regulation which impacts the exclusive rights of the design rightsholder. According to this provision, the rightsholder of an unregistered design can prevent the use of the design by third parties only if such use "results from copying the protected design".