PNC
Piano nazionale per gli investimenti complementari al PNRR
Ministero dell'Università e della Ricerca

FIT4MEDROB

D4.8.2

REPORT ON THE ETHICAL AND LEGAL COMPLIANCE OF HEALTHCARE AND PERSONAL CARE ROBOTS

Piano Nazionale Complementare (PNC) – Decreto Direttoriale n. 931 del 6 giugno 2022 – Avviso per la concessione di finanziamenti destinati ad iniziative di ricerca per tecnologie e percorsi innovativi in ambito sanitario e assistenziale
Project identifier: PNC0000007
Start date: 01/12/2022
Duration: 44 months
Website: www.fit4medrob.it

Editor(s): Francesca Gennari (SSSA) with the collaboration of Arianna Rossi (SSSA) Federica Casarosa (SSSA), Pelin Turan (SSSA), Irina Carnat (PhD candidate, SSSA) PIs: Professor Giovanni Comandé (SSSA).

Due date of deliverable: 30/11/2024
Actual submission date: 09/12/2024
Version: 9.1

DISSEMINATION LEVEL OF DELIVERABLE		
PU	Public, fully open, e.g. web	**X**
CO	Confidential, restricted under conditions set out in Partners Agreement	

PNC
Piano nazionale per gli investimenti complementari al PNRR
Ministero dell'Università e della Ricerca

HISTORY OF CHANGES

VERSION	SUBMISSION DATE	CHANGES
1	04/ 09/2023	D4.8.1 First version
2	30 /10/2023	D4.8.1 Full version for finalization
3	30/10/2023	D4.8.1 Full version sent to external referees
4	21/11/2023	D4.8.1 Final version submitted for upload in the platform
5	05/02/2024	D4.8.2 First version - draft
6	06/06/2024	D4.8.2 Second version - draft
7	08/07/2024	D4.8.2 Third version - draft
8	04/10/2024	D4.8.2 Fourth version – draft
9	30/11/2024	D4.8.2 Final version for peer review and final submission
9.1	09/12/2024	Submitted version

TABLE OF CONTENTS

1 EXECUTIVE SUMMARY

This deliverable is the direct continuation of its predecessor, D4.8.1 (it contains, builds on and expands D4.8.1), and it connects with the other two deliverables which are due at M24, meaning D4.2.1 Report on Awareness and Regulatory Gap Analysis with stakeholders #1 and D4.9.1, Web-based platform for open acceleration #1. This executive summary describes how this deliverable connects the past, the present, and the future of the other A4 deliverables within the initiative and its content.

This deliverable's relevance, contents, and outputs are synthetised below as follows.

1. *Deliverables' objective and importance*

This deliverable is the direct continuation of its predecessor, D4.8.1, and has the same objectives. The first one is to disseminate in a clear and succinct form the most important contents of legal frameworks for the Fit4MedRob's initiative participants who are not legal experts. This mapping has also the objective to enable Fit4Medrob Initiative's participants to become more aware and get acquainted with rules that need to be known since the design of rehabilitation and allied technologies. This need is also made apparent by the result of the D4.2.1 summary that demonstrated that there is a scarce awareness even about the MDR, which should be one of the fundamental rules to respect when it comes to put new medical devices into the market. Moreover, this deliverable also completed the legal mapping that served as a basis for the selection of legislative framework for the Web- Based Platform for Open Acceleration (WBPOA). That is its importance for the A4's team. It represents the contents

2. *Connections with the Fit4MedRob Initiative*

One of the Fit4MedRob's objectives is to consolidate the paradigm of the continuum of care. This objective will not be achieved if new rehabilitation robots and technologies are created and cannot be marketed because they do not respect the necessary compliance rules. More concretely, this deliverable is helpful in the context of Mission 1 as clinical trials have started or are about to start and will test the technologies that are developed in the context of Mission 2. Not knowing the rules concerning the MDR clinical investigations or the newly approved AI Act could be detrimental for the successful outcome of the match-making operations. The legal knowledge condensed in these two deliverables (D4.8.1 and D4.8.2) is also the baseline for developing new materials, instruments, and technologies, which is Mission 3's goal, since their early design.

3. *Connections with the previous deliverables*

As far as the past deliverables, in terms of relevant connections with the other two deliverables of A4, D4.1.1 was the start of a legal analysis of what are the main obstacles that impacted the development and successful uptake of rehabilitation robotics and allied technologies. It helped highlighting which needed to be the legal acts to focus on, but it was only with D4.8.1 that it was possible to find a methodology that would translate the most relevant legal acts for the Fit4MedRob Initiative's partners in a form that would be more understandable for non-legal experts. That is why D4.8.1 already used a synthetic approach and used tables to outline both the content of each legal act and what were the obstacles to compliance from a legal and ethical point of view. It is important to point out that D4.8.2 is connected to deliverable D4.2.1 as far as it will give the stakeholders a deeper overview of the subjects that they need to focus on to put into the market safer, legally and ethically compliant products for rehabilitation robotics and allied technologies. The connection with the first draft of open acceleration platform D4.9.1 instead is in the content of this deliverable as it gives provides a first and useful global mapping of the contents for the platform and of the services that it could provide.

4. *Methodology*

D4.8.1 was based on a dual approach: a first mapping of the relevant legal and ethical rules in regulatory documents relevant for the Initiative's partners' everyday practice and a first comment and elaboration of survey results (the survey circulated within the consortium in October 2023) on a wide range of legal rules (more than the ones analysed in the first iteration) that were relevant for the Fit4MedRob actors. The objective of the survey was twofold: to be sure that there were not topics left out of the theoretical analysis and to start thinking about services that are needed by the Fit4MedRob participants and that might integrate the future Web-based platform for open acceleration (D4.9.1 and later D4.9.2). The same methodology used to build the first part of the D4.8.1 was used to create the present iteration D4.8.2. it consisted of mapping new areas that were not covered by the previous deliverable. The main activity of A4 researchers was a theoretical and gap-filling task, hence the main result is the systematic explanation of the main notions and rules underpinning the relevant regulation. Two new sections are part of the

original ToC: Cybersecurity (section 4) and Intellectual Property (section 5). The space devoted to these subjects is a direct consequence of last year's survey results in which it appeared very clear that the Fit4MedRob participants were interested in these two subjects. As these subjects are more technical and difficult to simplify without serious omissions or mistakes, the language they are written is unavoidably richer in technical terms. Nevertheless, whenever possible, A4 reported examples relating to the everyday experience of the Fit4MedRob participants to help understand technical notions that cannot be oversimplified. However, the structure in tables was maintained. This is supposed to help non-legal experts to associate better the main contents and names of the EU legal acts. A second part of this gap-filling work also consisted of the systematic update, in contents and writing style, of the past contents of this deliverable. It was a momentous year in terms of Digital Policy enactment: the Data Act, the Machinery Regulation, and the General Product Safety Regulation (GPSR) are finally law as well as the AI Act. Some proposals were updated and agreed on but are not applicable law yet. Despite this

5. *Main results of the deliverable*

As far as the content is concerned, this deliverable is more restricted in scope than D4.8.1 but not less important. About the first part of the update, it introduced new content altogether: the most relevant EU regulatory relevant concerning copyright (5.1), patents (5.2), trade secrets (5.3), and industrial designs (5.4) were explained. The main results from the analysis of this section are that the EU has progressed rapidly in the harmonization process of copyright, but that it also values industries with the regulations on trade secrets and the upcoming regulation on the standard essential patents (SEPs) which will apply to standards used to build the IoT. This information is essential for people designing technologies, such as the ones in Biorobotics, that use interconnected hardware and standards to implement them. Section 4, devoted to Cybersecurity, showed that both the EU and Italian legislator displayed a high level of activism, with several legislations approved until almost the end of the deadline of M24. Among the most interesting legislations dealt with in the sector, let us remember the Cyber-resilience Act (CRA) -that lays out a framework of general cybersecurity duties and standards that will apply to personal care robots but not to medical devices, and the European Health Data Space proposal, for the cybersecurity aspects of medical devices.
As far as the update of the previously cited legislations, we should remember some of them in particular (which were voted into law since D4.8.1): in fact, since August 1st, 2024, the AI Act is law. It is going to radically influence how software is developed from its design and will make a product that needs to be certified as safe before being put into service or into the market. During the finalization of this deliverable also the final version of the Revised Product liability directive was approved, and it is important in terms of liability as it extends the definition of "product" to digital manufacturing files and software - and will be reanalysed in the prosecution of the A4 activities. It is important also to remember that the Italian code of personal data protection has been amended in May 2024 and new rules are in place to facilitate the secondary use of data for research. This modification is done in anticipation for the enactment of the European Health Data Space which will allow a safe access to a multitude of personal and non-personal electronic data for research purposes.

6. *Timeline with the outcome and 7. Future work and why the deliverable is an enabler.*

The first two iterations of this deliverable (D4.8.1 and D4.8.2) completed the legal mapping and analysis of the strictly necessary sets of legal rules that are indispensable to consider a product compliant by design. This is the necessary framework to start building more on the compliance part. This means a progressive work through this deliverable's following iterations, meaning D4.8.3, D4.8.4 which will contain indications and guidance on what legal rules prioritise and in which order according to the different products that need to be marketed (the main distinction will be between medical and non-medical device). Given that the last iteration is due at M44, A4 team is on time. This will also allow integrating the national implementation of the EU rules that might intervene between M24 and M44. There are no estimated deviations. This work, as explained supra, will enable non-legal experts to get acquainted and to know the minimum level of legislative acts that need to be considered while designing or marketing a rehabilitation robot or an allied technology

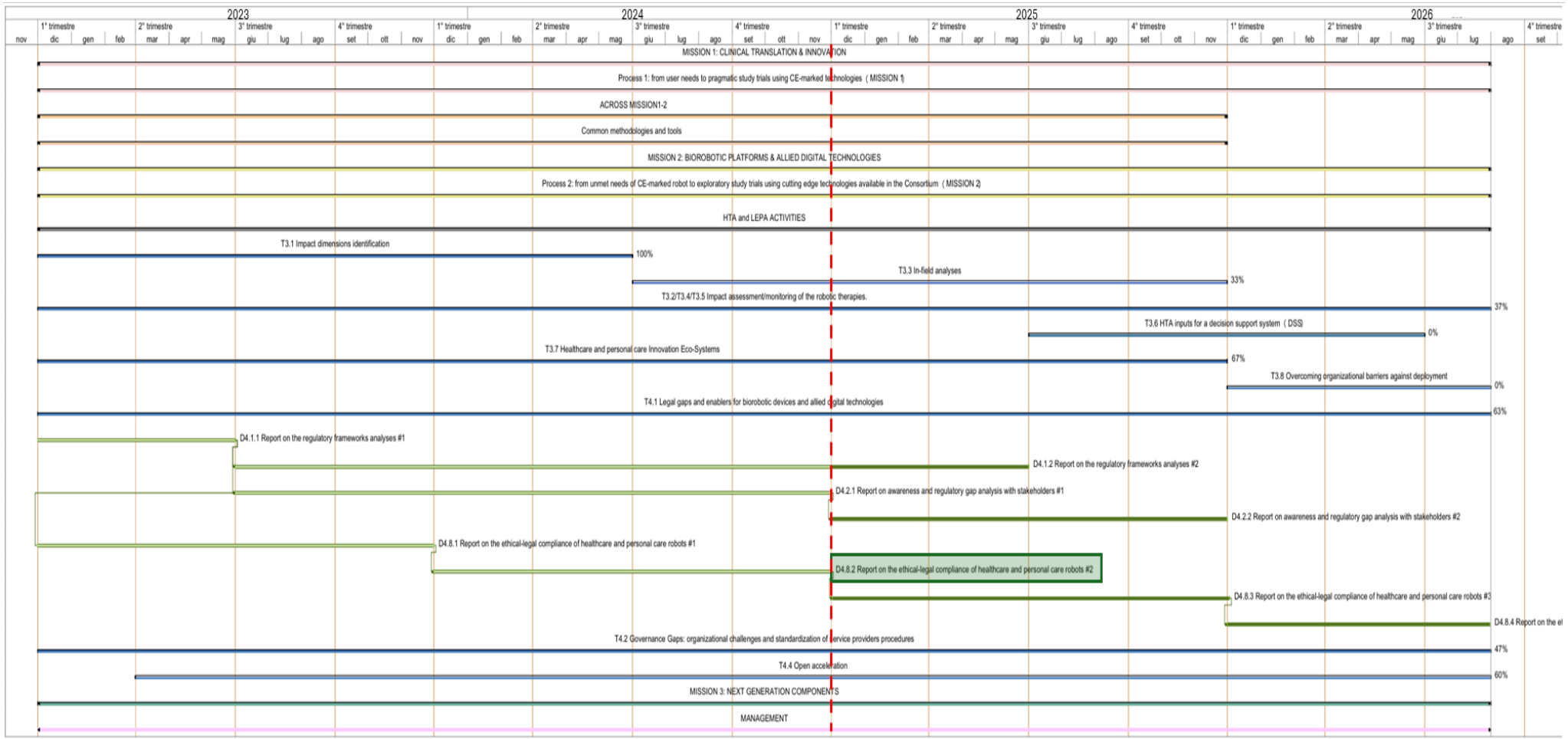
The methodology section (2) explains that the first part aims to map down the main legal and ethical requirements that the Fit4MedRob partners need to consider while developing a new generation of healthcare and personal care robots. The main difference with D4.1.1. is both in the means and in the substance of this deliverable. Mapping down legal and ethical compliance requirements this time was a process mainly addressed to non-lawyers (3). That is why a more concise and synthetic way of displaying information rationale was employed in selecting the most important points to raise in the short and medium run, as far as compliance is concerned. More precise and further

research on this will be done in the further iterations of the deliverable. The reference audience being mainly non-lawyers explains the use of tables which are grouped in theme sections: the safety of products (3.1) (with medical functions or not), AI regulation and ethics (3.2), Liability issues (3.3), and Data Laws (3.4). For each of the legal acts commented there is a focus on the more pressing current legal and ethical compliance problems and open issues for researchers and innovators explained in the clearer way possible.

The methodology also explains the rationale of the second part of the deliverable and coincides with section 4. Activity 4 needed an instrument to check whether their mapping was correct and what were the most pressing ethical and legal compliance issues in researchers' everyday lives. This explains the origin and the development of the survey on ethical and legal compliance (4.1), its questions and their purpose (4.2) and its replies (4.3). After the survey results, Activity 4 decided to start drafting already a draft of the services that will be developed through the next deliverable, D4.9.1 (4.4) which will lay the foundation for the creation of a web-based platform for open acceleration which will then become part of the instruments developed by the future centre of excellence (I)URAT, created thanks to Fit4MedRob funds.

Section 5 is a short part concerning the main findings of the two central sections (sections 3 and 4) of this deliverable.

It is important to highlight this deliverable's relevance for the Fit4MedRob project. Methodologically, the choice of having as reference audience doctors, engineers, and technical experts, which constitute the utter majority of the Fit4MedRob consortium, influenced the language use, correct but clearer, to make the readers understand what the relevant legal and ethical compliance rules are when designing a new generation of personal or healthcare robots and help them put those legal and ethical obligations in practice. The extent of the subjects covered is considerable and will be completed with additions and updates in November 2024 (M24). This is done to give the Fit4MedRob consortium partners a 365° view of the aspects they need to cover to design innovative personal or healthcare robots and other allied technologies - such as AI systems- while at the same time being compliant with the ever-increasing set of legal and ethical obligations. Moreover, the survey that was circulated aimed at focussing and making more granular choices in terms of the needs that the Fit4MedRob consortium partners have to better address their concerns with the upcoming update of this deliverable (D4.8.2) and with the upcoming web-based platform for open acceleration (D4.9.1).


2023
2024
2025
2026
MISSION 1: CLINICAL TRANSLATION & INNOVATION
Process 1: from user needs to pragmatic study trials using CE-marked technologies (MISSION 1)
ACROSS MISSION1-2
Common methodologies and tools
MISSION 2: BIOROBOTIC PLATFORMS & ALLIED DIGITAL TECHNOLOGIES
Process 2: from unmet needs of CE-marked robot to exploratory study trials using cutting edge technologies available in the Consortium (MISSION 2)
HTA and LEPA ACTIVITIES
T3.1 Impact dimensions identification
100%
T3.3 In-field analyses
33%
T3.2/T3.4/T3.5 Impact assessment/monitoring of the robotic therapies.
37%
T3.6 HTA inputs for a decision support system (DSS)
0%
T3.7 Healthcare and personal care Innovation Eco-Systems
67%
T3.8 Overcoming organizational barriers against deployment
0%
T4.1 Legal gaps and enablers for biorobotic devices and allied digital technologies
63%
D4.1.1 Report on the regulatory frameworks analyses #1
D4.1.2 Report on the regulatory frameworks analyses #2
D4.2.1 Report on awareness and regulatory gap analysis with stakeholders #1
D4.2.2 Report on awareness and regulatory gap analysis with stakeholders #2
D4.8.1 Report on the ethical-legal compliance of healthcare and personal care robots #1
D4.8.2 Report on the ethical-legal compliance of healthcare and personal care robots #2
D4.8.3 Report on the ethical-legal compliance of healthcare and personal care robots #3
T4.2 Governance Gaps: organizational challenges and standardization of service providers procedures
47%
T4.4 Open acceleration
60%
MISSION 3: NEXT GENERATION COMPONENTS
MANAGEMENT

2 Methodology

2.1 Theoretical and practical needs

This deliverable is at a crossroads between a concise synthesis concerning the state of regulatory policy and the internal needs of the Fit4Medrob consortium. This deliverable can be divided into two parts. The first one concerns a sum up of the legal framework that applies to personal care and healthcare robots (2.1.1). The second part is an analysis of a voluntary and anonymous survey conducted among the members of the Fit4MedRob consortium to gather their legal blocks and needs concerning the same EU and Italian legal acts and proposals concerning personal and social care robots (2.1.2).

2.1.1 Mapping and Commenting the Reference Legal and Ethical Framework

From a methodological point of view, it was not an easy task to map down the legal and ethical requirements concerning personal care and healthcare robots. In fact, since 2017 with the European Parliament resolution on the civil liability of robots[1], these objects have not been regulated directly, but through the general safety of products regulations and the medical devices regulation. Among the different kinds of laws, it was possible to identify three macro-areas: data laws, safety laws, and liability laws. The first one could be called the 'data laws', which include the GDPR, but also the recently implemented Data Governance Act. In addition, one has also to consider as part of the data laws the new proposals on data access such as the Data Act (DA), and the European Health Data Space (EHDS). Then there are the 'safety laws' with their most important subset which are the Medical Devices(MDR) and Clinical trials (CTR) disciplines. Moreover, it is also likely that the AI Act proposal might be approved soon, and the healthcare and personal care robot manufacturers need to understand whether they employ a high-risk AI system that needs to comply with a complex set of obligations. Further, to design and deploy a new series of products it is also essential to think about which kinds of liability regimes might come into play. Among these, we must take into account the Product Liability Directive (PLD) and its proposed update (PLDU), the two directives on certain aspects of the sales of goods (SG) and the directive on the supply of digital content and digital services (DCDS) and, the proposed artificial intelligence civil liability proposal (AILP).

As far as the ethical framework, ethics has always been more difficult to frame and write down but, certainly, some articles of the GDPR or of the AI HLEG guidelines on trustworthy AI do have an ethical significance for innovators.

To differentiate the contents of this deliverable from the ones of D4.1.1 concerning the mapping of the legal blocks concerning new-frontier medical devices research, this part of the deliverable will be mostly made of tables in order to summarise the contents for operators and people who are not lawyers. The main function is the one to highlight what possibilities are offered by proposed and enacted legal acts and what the problems could be for personal care and healthcare robots.

In this iteration of the document, we will exclude cybersecurity issues, intellectual property ones, and also issues connected to insurance as there would not be sufficient time to devote to each of these subjects in detail.

2.1.2 Building a survey for the Fi4MedRob Initiative needs

The second part of the deliverable is of capital importance to understand what the needs of the members of the Initiative are. Activity 4 decided to draft a survey to reply to some simple but essential questions that are preliminary to the drafting of the future deliverable D4.9.1. which is a web-based platform for open acceleration. Despite deliverable D4.9.1 being due only next year, Activity 4 found that doing this kind of survey also highlighted the gaps and requirements concerning legal and ethical compliance which are part of this deliverable as well. The survey in the context of this present deliverable D4.8.1. is comparable to the 'other side of the moon': it is a trustworthy picture of how ethical and legal compliance is dealt by non-legal professionals on a day-to-day basis. That is why it is important not only to explain how it was drafted and circulated but also to take an ideal step back and comment

[1] European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)) OJ C 252, 18.7.2018, p. 239–257.

on the services that could be provided to the Fit4MedRob consortium in order to design a thorough legal and ethical compliance strategy.

3 LEGAL AND ETHICAL COMPLIANCE IN THEORY

3.1 SAFETY LEGISLATION

As an over-arching rule of law, the more specific law applies to the issue at hand. In the case of safety, if the object has a medical function according to its manufacturer, it will be the Medical Device Regulation or Clinical Trial Regulation that will be applicable (3.2.2). Instead, if the object, even if technologically advanced such as a personal care robot, is not marketed as a medical device, then, the general rules concerning the safety of products will apply (3.2.1).

3.1.1 General Safety laws

General safety legislation corresponds to the heterogeneous group of enacted or proposed legal acts that sets up all the requirements and surveillance mechanisms that will apply to products that are not medical devices, even if they will interact with healthcare robots (which could be considered as medical devices, see infra 3.2.1.) both as accessories or part of a connected system of robots with medical devices functions. Moreover, the need to follow up closely this legislation is that the Fit4MedRob consortium also hosts partners which are commercial entities and that might decide to market a personal care robot as an object with no medical functions. Hence, they will be obliged, depending on the characteristics of their personal care robot or device to apply two or more of the following regulations. As far as the machinery legislation, they are applicable if the parts that compose the device are part of the list enclosed in the annexes of the Machinery Directive (MD) or the recently approved Machinery regulation (MR). Nevertheless, there is one point in common among all these different legislative acts: the product conformity to specific EU (harmonized) or, where they are not present, to national standards is a (rebuttable) presumption of conformity of that product or part of the product.

Table 1 General legislation

Name of the Initiative	Legal Compliance and obstacles	Ethical principles
Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 (Text with EEA relevance) OJ L 218, 13.8.2008, p. 30–47 (**CE Marking Regulation**)	It creates a market surveillance system, including conformity obligations as follows. Most notably that happens through the • set-up of **conformity assessment bodies**; a **market surveillance system** and a system for rapid information • set-up of a **Community Rapid Information System** **Obstacles** The CE marking regulation might need an **update** sometime soon as it was drafted and enacted when technology such as the mainstream use of IoT, robotics or AI were in their first days.	Highest level of safety possible. The CE marking conveys an idea of trustworthiness both for the professional subjects that use the object for work but also for the consumer
Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety (Text with EEA relevance) OJ L 11, 15.1.2002, p. 4–17	A product's compliance with EU or national safety requirements is a presumption (rebuttable) of its safety. The requirements concern not only producers but distributors and National states as well. It sets up	Same as above

General Safety of Products Directive (**GSPD**)	an EU fast recall system which is called RAPEX. **Obstacle**: The GSPD will be shortly substituted by the General Safety of Products Regulation (**GPSR**, see infra in this table)	
Regulation (EU) 2023/988 of the European Parliament and of the Council of 10 May 2023 on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council and Directive (EU) 2020/1828 of the European Parliament and the Council, and repealing Directive 2001/95/EC of the European Parliament and of the Council and Council Directive 87/357/EEC (Text with EEA relevance) PE/79/2022/REV/1 OJ L 135, 23.5.2023, p. 1–51General Safety of Products Regulation (**GSPR**)	The **GPSR** is an update of the previous directive **GPSD**. It makes it explicit that a presumption of conformity if the products comply with **harmonized** and/or **national standards** as well as **voluntary certification schemes**. It sets out horizontal requirements (meaning general ones unless there are other more specific that apply to the case) on the safety of products for a series of **economic operators** and not just manufacturers. This list also includes **online platforms** and fulfilment service providers. These last ones are not only traditional consumer objects but also **interconnected ones** (Article 2.2 GPSR), such as IoT and, in principle personal care robots. **Obstacle:** This system partly builds up on the previous general safety one but there are also new **traceability requirements** (Article 18) that will add up to the system of recall such as the Safety Gate Rapid Alert System (for the Member States to share information about product safety) and the Safety Business Gateway (for online market places to provide consumer with information) but also of market surveillance. It might be complex to connect all these requirements that involve not only manufacturers but a much longer list of economic operators. All these rules will become applicable by **2024.**	Same as above
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) (Text with EEA relevance) OJ L 157, 9.6.2006, p. 24–86 Machinery directive (**MD**)	It applies to products that might be part of a personal care robot and that are comprised in the list of **Article 1 MD** (e.g., interchangeable equipment and safety components, chains…). It is a more specific regulation that in the case of personal care robots might be considered apart from the more general **GSPD**. It sets a system of market surveillance and obligations before putting the machinery into the market or into service. **Obstacle**: the MD does not consider new technologies as well as the GSPD. That is why a new Machinery Regulation (MR) has been approved	Highest level of safety possible. The CE marking conveys an idea of trustworthiness both for the professional subjects that use the object for work purposes but also the consumer. Specifically for this case, it is applied to machinery components or their groupings with inherently higher risk for human health and physical integrity.

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 (Text with EEA relevance) PE/6/2023/REV/1 OJ L 165, 29.6.2023, p. 1–102 Machinery regulation (**MR**)	The Machinery Regulation will be applicable from **2024.** It builds on the previously existent MD and relies on the **same presumption concerning conformity** underpinning the previous regulations and directives. However, the MR modifies the list of parts and machinery to which the MR can potentially be applicable. Moreover, the MR comprehends a series of annexes that provide more details concerning conformity procedures which depend on the level of risk and type of object. It can be of particular interest that software has been included in the MR and specifically in annex II concerning the indicative list of safety components.	Same as above

3.1.2 Medical Safety laws

This is a group of special legal acts that still are connected to the area of safety of objects from an administrative point of view. They are relevant as there is not a more specific regulation concerning healthcare robots but the medical devices one. It is also important to highlight the importance of the Clinical Trials Regulation (CTR) of the projects. Activity 4 believed it was relevant also to better outline how the Italian implementation of both the MDR and the CTR given its importance for Activity 1 and 2 of the Fit4MedRob project.

Table 2 Medical Safety Legislation

Name of the Initiative	Legal Compliance and Obstacles	Ethical principles
Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (Text with EEA relevance) OJ L 117, 5.5.2017, Medical Devices Regulation (**MDR**)	MDR sets all the compliance duties a manufacturer must follow to commercialize medical devices in the single EU market. In particular, it is useful to highlight as follows. As in the previous directive, the medical devices are divided into **classes of risk (I, IIa, IIb, III)**. The higher the risk for human health, the more thorough must be the procedure audit/certification for the medical device. In general, the different classification rules are spread between Article 51 MDR and Annex VIII. After having found the appropriate class for the medical device, the manufacturer must choose one certification/conformity procedure following the rules of Article 52 MDR and Annexes from IX to XI. The objective is to obtain the **CE marking for the medical device** to be put into the market or put into service. In order to trace with more precision medical devices in the EU market (which will be used also to know whether there are ongoing clinical	The main ethical principle is to ensure **the highest level of protection of health possible**. *This is not an absolute threshold, as it has to take into account also of the level of technology and the state of medical science*.

	investigations on a medical device), the MDR sets the rule on how to create and how to make operative a EU database for medical devices (**EUDAMED**, Articles 33 and ff. MDR). Moreover, every medical device will be traceable thanks to the inclusion of in a system called **UDI** (Unique Device Identification system), whose functioning is described at Article 27 and in part C of annex VI. **Obstacles** According to the MDR, **software** can also be considered as a medical device according to Article 2(1) MDR. The criteria on how to differentiate software from software as a medical device have been collected at the EU level by the Medical Devices Control Group (MDCG)[2]. However, in practical terms it might be difficult to understand whether a software could be considered a medical device. The **product and value chain** of medical devices has become more complex than it used to be. There are not only manufacturers as subjects which do have requirements and obligations but also authorised representatives, importers, and distributors who also do have requirements (Articles 10, 11, 12,13, 14 MDR). More interestingly the list of manufacturers requirements can be found at Article 10 MDR but must be complemented with the post-market surveillance duties which can be found at Article 83 MDR. Concerning manufacturers duties and requirements, particularly interesting is the mention at Article 10(16) MDR of the necessity to have financial means to face product liability claims. In some specific cases, manufacturers obligations must be carried out by importers or distributors (16 MDR) Moreover, **Notified Bodies** (NB) (Article 35 and ff MDR) are audit/certification bodies selected by the Member State and recognised by the EU Commission as trustworthy enough to certify whether a device can be certified as medical device.	

[2] More on the strategies on how to categorise software as a medical device can be found here: Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR https://ec.europa.eu/docsroom/documents/37581 accessed 27 October 2023.

	Because a NB was involved in a health scandal under the previous regime, the NB have more requirements to respect which concern the acquisition of the status of NB but also their obligations. For instance,they are considered responsible if they use subsidiaries or hire contractors to carry out their duties which was not the case in the past (Article 37.2 MDR) The MDR deadline for national implementation was **26 May 2024** therefore it is extremely important that medical devices producers comply with these rules.	
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) Devices bearing the CE marking*. This implementing decree's contents concern: 1) how to **handle the official communication** for products bearing the CE marking, at least until the EUDAMED database (see MDR supra) is fully operative. In any case, all manufacturer's communications are officially addressed at the **Italian Health Ministry**. 2) the fact that it is the **manufacturer's duty** to send **complete and compliant documents** and files documentation sent must be compliant with the MDR requirements. 3) further, that **preliminary** to the manufacturer's official relevant documents communication to the Health Ministry, the manufacturer submitting the file **must obtain the approval by an Ethical Committee** either at a **local** level from a CET (Comitato Etico Territoriale) or at a **national**, from a CEN (Comitato Etico Nazionale) 4) that manufacturer must give **notice** of the trial(s)'s start **within 30 days to the competent authority** *B) Devices not bearing the CE marking*. This implementing decree's content concerns 1) how to **handle the official communication** for products not bearing the CE marking, at least until the EUDAMED database (see MDR supra) is fully operative. In any case, all manufacturer's communications are officially addressed at the **Italian Health Ministry**.	Same as above

	2) the **clarification** about the **sponsor** being the legal entities/subjects habilitated to **officially communicate information** to the Italian Health Ministry is the sponsor 3) that the **request** for the start of clinical trials must be done **only after obtaining a favourable opinion from either a local Ethical Committee (CET) or national (CEN)**. 4) that the **sponsor** communicates the **beginning of the trial promptly** to the competent authority (Health Ministry). **Obstacles:** The manufacturer's and sponsor's difficulties in this phase is that the implementing acts are ready but they need to be tried in practice and there is always a margin of uncertainty.	
Clinical Trials regulation (and its implementation in Italy): Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC Text with EEA relevance OJ L 158, 27.5.2014 (**CTR**)	The CTR should have both a **digitalisation** and **harmonisation** effect on the clinical trials' discipline. Its founding principles are the following ones: 1) that each clinical trial needs to **pass both a scientific and an ethical review** 2) that the said **ethical review** must be carried out by a **national ethics committee.** 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 CTR** and → in Part II of the assessment report as referred to in **Article 7 CTR** as appropriate for each Member State concerned. 3) that the **procedure will be standardised through a common EU portal** where all the documents must be submitted (CTIS) and the authorisation procedure is led by one Member State (generally the one of the persons submitting the documentation in CTIS). **Obstacles** This regulation was needed but the problem is the **implementation time**. It was firstly adopted in 2014, and it is not fully applicable after 10 years. This is understandable given the level of harmonization required.	Same as above

	Nevertheless, 10 years it is also the time in which there could have been a consolidation of this regulation at the EU level and research could have progressed more rapidly.	
National implementation of Clinical Trials Regulation into the Italian discipline: 26, 27, 30 January 2023 decrees	The Italian framework concerning the implementation of the CTR hugely relies on 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*:** describes the way in which to select the Ethical Committees per region **(there will be only 40 ethical committees).** ***Decree Jan 27, 2023***: The first part of this second decree concerns its field of application (substantial amendments of clinical trials proposals) and postponement of the application of the CTR **until 31 January 2025**. However, one can already start using the new EU portal, Clinical Trial Information System (CTIS) for the presentation of Clinical Trials (CT) proposal; The second part of the decree concerns the implementation of the clinical trials evaluation proposals into 2 parts. The first part concerns (see Article 6 CTR). 1. the clinical trial type (e.g. low-intervention clinical trial); 2. what the therapeutic and the public health benefits of the proposed CT are. 3. what the subject could risk; 4.marketing and labelling requirements compliance and 5. the presented material's fitness for the CT The second part instead concerns (Article 7 CTR): 1) informed consent compliance requirements (chapter V CTR) 2) rewards and compensation requirements for CT participants which need to be compliant with the requirements set out in Chapter V (CTR)and investigators. 3) subjects' recruitment with the compliance requirements set out in Chapter V (CTR)	

	4) compliance with Directive 95/46/EC; 5) compliance with Article 49 CTR (Suitability of individuals involved in conducting the clinical trial) 6) compliance with article 50 CTR (Suitability of clinical trial sites) 7) compliance with article 76 CTR (Damage compensation) 8) 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). **Obstacles** As already observed in the part concerning obstacles and the EU CTR, even these last implementing decrees create some uncertainty, as it is typical in all the transitional periods as it still needs to be fully applied.	

3.2 AI REGULATION AND ETHICS

Artificial Intelligence is a technology which is bound to influence other ones such as robotics and the IoT. The algorithms that power it have become increasingly more complex and efficient in just a few years. Given the possibilities offered by large language models (LLMs) but also Natural Language Processing (NLP) AI systems, it might be tempting for new personal and healthcare robot creators to integrate those into the device's functioning. Since 2018, the AI has been the technology that has received more public and media attention and in a matter of a few months the text of the AI act (now still a proposal) should be voted into law and become effective. One of the main problems is that AI applications such as the LLMs were not considered in the first drafts of the AI proposal (which was presented almost two years ago) and this creates some doubts as if the AI act will be still an applicable legislation in practice when it will become effective. That is why the ALTAI checklist for ethical AI might still be a useful tool for assessing new kinds of AI for which the AI act might be difficult to apply.

Table 3 AI Regulation

Name of the Initiative	Legal Compliance and Obstacles	Ethical compliance
ALTAI checklist for a trustworthy AI [3]		This document is a **checklist** of **ethical/legal principles** that should always be followed and applied

[3] ALTAI, Assessment List Trustworthy Artificial Intelligence. ALTAI Self-Assessment https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment. Accessed 25 October 2023.

		since the early stages of AI systems development, especially the ones that might not be formally considered as high-risk by the combination of Article 6 and annexes II and III of the AI act but that could have impactful effects on society The principles that AI providers should follow from the design phase for their algorithms are the following ones: • **human agency and oversight** • **technical robustness and safety** • **privacy** and **data governance** • **transparency** • **diversity, non-discrimination and fairness** • **environmental and societal well-being** and • **accountability**
Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 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) Text with EEA relevance. PE/24/2024/REV/1OJ L, 2024/1689 **AI Act**	The AI Act regulates the development and deployment of **AI systems** defined as a machine-based system (primarily a **software**), which operates with varying levels of autonomy and adaptiveness, and "infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments". It adopts a **risk-based regulation of AI systems.** The main requirements concern **high-risk** AI systems, defined according to the classification rules in **Article 6(1):** AI used as a **safety component** of a product (or is in itself a product) required to undergo third-party conformity assessment under **Annex I;** and **Article 6(2):** AI systems referred to in **Annex III.** For such high-risk AI systems, a **risk management system** is required, accounting for the intended purpose of use, the reasonably foreseeable risks to health, safety or fundamental rights, and appropriate technical measures for risk mitigation. Compliance requirements for high-risk AI systems include: **data governance** to ensure that datasets	Providers of high-risk AI systems to be deployed in areas listed in Annex III (with some exceptions) are required to perform a **fundamental rights impact assessment** (Article 27), which is basically an ethical compliance document. There is an explicit reference to Article 35 GDPR concerning the **Data Protection Impact Assessment (DPIA**). The AI Office is expected to develop a template to facilitate compliance with this requirement. The assessment shall consist of: a) description of the deployer's processes in which the high-risk AI system will be used in line with its intended purpose; b) description of the period of time within which, and the frequency with which, each high-risk AI system is intended to be used; c) the categories of natural persons and groups likely to be affected by its use in the specific context; (d) the specific risks of harm likely to have an impact on the categories of natural persons or groups of persons identified pursuant to point (c); (e) a description of the implementation of human oversight measures;

	are relevant, sufficiently representative and to the best extent possible error-free; drawing up **technical documentation;** the possibility for **record-keeping** and logging; transparency and **information provisions** for deployers to ensure they are able to interpret the AI system's outputs; **human oversight** measures in accordance with the AI system's risks, level of autonomy and context of use; and finally **accuracy, robustness and cybersecurity** measures. Compliance with these requirements shall be documented in a **quality management system,** which can also be included in other quality management systems subject to relevant sectoral Union legislation (Article 17(4)). High-risk AI systems shall then undergo a process of **certification** with **specialized notified bodies**. Moreover, **an EU database of high-risk AI systems** will be established. Certain specific AI systems, such as those meant to interact directly with natural persons, are subject to additional **transparency** requirements under Article 50, such as marking that the output or content are **AI-generated.** Specific requirements concern **general-purpose AI models (GPAI)**, depending on whether they pose systemic risks or not. Under Article 53, all providers of such models shall provide **technical documentation** and **information** on the model's capabilities and limitations. Finally, all AI systems that do not fall under the high-risk category, are considered as **lower risk**, thus subject to the general requirement of **AI literacy of deployers** under Article 4, and the requirements under the **GPSR** (Recital 166)**.** **Obstacles** **AI practices** listed in Article 5 are **prohibited,** such as those meant to manipulate or specifically exploit certain vulnerabilities of natural persons. Article 40 provides for a presumption of conformity if AI systems or GPAI comply with **harmonised standards**, which have **not yet been developed.**	(f) the measures to be taken in the case of the materialisation of those risks, including the arrangements for internal governance and complaint mechanisms.

	While formally adopted, the AI Act has not entered into force yet. **Obstacles** or certain groups (article 5 Ai Act). Concerning Fit4MedRob partners which create personal and healthcare robots, they will need to combine the AI act to the MDR and the MR compliance. In fact, The Machinery regulation is connected to the AI Act as well the MDR and the In Vitro Fertilization rules because of they appear in Annex II list. Therefore, we can expect that AI systems for medical devices and machines will need to follow the AI act discipline which concerns high risk AI system which will include several obligations concerning transparency and training of this algorithms as well as the drafting of a fundamental rights AI impact assessment. Risk and the certification from a specialised Notified Bodies and the registration. NB: The parts of the AI Act connected to cybersecurity are dealt with in the Cybersecurity section	

3.3 LIABILITY LAWS

Liability rules are essential to design better and safer personal and healthcare robots. Moreover, the characteristics of liability sets might greatly influence the final price of the final product/device. In fact, if the manufacturer needs to invest more in R&D to have a compliant object, this cost will be likely to be absorbed in the final cost of the product. There will be the brief description of the new proposed EU product liability rules, the AI civil liability proposal and the directives concerning goods with digital elements (SG and DC) to conclude with a sum up of the Italian private law responsibility rules.

Table 4 Liability laws

Name of the Initiative	Legal Compliance and Obstacles	Ethical Compliance
Product liability directive proposal (COM/2022/495 final) (**PLDU**) The European Parliament approved a new text of this same proposal on 12 March 2024. It has n been approved officially by the European Council on 11 October 2024, but the last approved text has not been published yet. Therefore, there is not yet an official reference. However, for the discussion the most recent text will be used[4]	The current product liability fundamental rules of the Product Liability Directive (PLD) (which in Italian can be found in Codice Del Consumo) are not different from substantially from the ones of the PLDU. Both in the PLD as well as in the PLDU, the consumer must prove **the damage**, **the defectiveness** of the product and **the causal link** between the two of them. This did	In the official proposal, the ethical (and social) paradigm to check the defectiveness of the product is the **safety that the public at large** can expect of the object (which could or could not be a medical device) whereas in the current regime it is the safety that a person can legitimately expect. This might be a more pro-consumers' choice than the actual regime.

[4] https://www.europarl.europa.eu/doceo/document/TA-9-2024-0132_EN.html

	not change in the newly approved text. However, some of the **old terms** are being **applied more extensively**. One example is the definition of **product** which now comprehends **data** and **software** as well as the word damage, which can also be about data used both for personal purposes. One of the changes of the new version of the PLDU is that it excludes compensation for the loss or damage to data used for professional reasons. Moreover, there is an increasing similarity in the subjects which might be considered liable. In the official PLDU proposal, Article 7 details a long list of economic operators, by using the same terms of the MDR. The consumer must contact the *manufacturer as the first subject to be liable*. If they are not in the EU or are unknown, the consumer will need to follow the list of the subjects that could be considered liable at the place of the manufacturer and that can be found in Article 7 PLDU. In the newly approved text, the same principle is present but has been moved to Article 8. Moreover, it is worth to point out that the complicated cascade system of the previous Article 7 has been simplified. This proposal will be important as it considers software and data used by **connected products** as traditional medical devices as well. It is relevant both for personal robots (because they will be consumer objects according to EU law) but also for medical devices. The MDR is currently directly linked to the actual product liability directive, and this is going to be the case also in the newly approved text, although not stated explicitly be connected to it also in the foreseeable future but not for all healthcare and personal care robots (see *infra-Obstacles*). Moreover, the specific mention of **surrogation** in the position who has been damaged by other subjects makes it clear that to insurance contracts will become of even greater importance in goods with digital elements issues. **Obstacles**: The problematic thing might be that medical devices such as **healthcare robots** might	One must also not forget that the manufacturer can also have exemptions of liability. One that might be interesting in relation to ethics is the so-called **'risk-development' exception**. If the manufacturer proves that they followed the best state of the art at the moment of putting the product into the market they cannot be held liable for damages caused by the same product. However, one must remember that the consumer now has can count on of 15 years for a damage to become apparent (this number was the result of past case-law concerning side-effects with medical products litigation in the past) and three years instead of two to act upon it. Moreover, legal rules that are actually a source of ethical compliance duties are the ones contained in Article 8 and 9 PLDU. The first article states that claimant can ask judges to get access to the functioning of the product to prove one or more of the elements they need to provide evidence for (provided that they justify this request). If the defendant refuses to give access, then they are presumed liable. This responds to a principle of fairness towards the consumer who might not have access to the technical knowledge to prove their point. The same ethical foundation underpins Article 9 PLD sets some ground rules for rebuttable presumptions concerning the defective and/or the causal link elements that the consumer must provide evidence for. Even in case Article 9 PLDU applies the manufacturer can always rebut the presumptions concerning defectiveness.

	integrate high-risk AI systems in situ or in the cloud. This will result in the need to apply the AI act compliance rules but also the AI civil liability proposal rules (infra). This might create confusion in how to apply different set of rules for robots that might be similar but are certified differently. The same thing might happen when **a personal care or healthcare robot** has parts that fall within the MD/MR system. Moreover, it is not clear how the MDR will still be connected to the PLD. The MDR recalls explicitly that it is connected to the currently applicable product liability directive thanks to Article 10.16 MDR. This article states that **the manufacturer must have enough funds** (including insurance) to cover **product liability claims.** There is no reference of the MDR in the new text of the proposal. That makes it clear that the PLDU might be applied to medical devices only when they are not connected devices.	
AI civil liability directive proposal (COM/2022/496 final) (**AILP**)	There are **two new rules** (especially Articles 3 and 4) that are set to harmonize tort liability rules ***whenever an AI system contributes or directly causes technological damage***. More specifically, Article 3 clarifies some rules concerning the disclosure of evidence from a procedure point of view. 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, the court must protect as much as it is possible the AI provider's IP rights. 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 for the judge to presume the presence of a causal link. Three cumulative conditions need to be demonstrated A) The claimant has proved through the use of Article 3	The ethical-legal compliance rule is that the *injured person must be able to prove difficult technical and scientific elements that are relevant for the functioning of AI high-risk systems by using legal presumptions*. This principle is counter-balanced by the fact that ***the causal link presumption is not an absolute one***, hence the defendant always has a chance to rebut the presumption

	AILD (rules on accessing how the AI system works) that the AI system had a role in the damage's causation B) That from the circumstances of the case, it can be inferred that fault also has influenced the output of the AI system C) The claimant has demonstrated that the AI system outcome or lack of caused the damage. The second part of Article 4 AILP is based on the official proposal of the AI act, which was very different from the last approved version. As a consequence, there will most likely be a modification of the content of this part of the article. Nevertheless, it is worthwhile to mention that Article 4(2) AILD lists a series of duties of care concerning the development and fair deployment of an high-risk AI system. If also one of these duties of care (which span from transparency requirements to fairness) is breached than the first of the conditions listed above (letter A) is considered to be proved. **Obstacles**: This proposal is closely **connected to the AI Act** first proposal**.** This might create problems as there is no mention of General-Purpose AI systems (GPAI, see above 3.2) in the AI liability proposal. It is likely then that this proposal will be modified deeply soon. Another problem is that the PLDU has also changed quite substantial. Supra it was mentioned that the PLDU in its first version mentioned that it did not infringe the rights under the AILP, in its Article 1. Now that this mention connecting the two documents has disappeared from the text of the PLDU, it is likely that also the same reference to the PLDU in Article 1(3)(a) AILP will be erased or otherwise modified, It might be difficult to understand in practice when to apply the AILP. This is because the AILP field of application coincides with the one of the PLDU as both these legislative acts regulate partly the same phenomena. In fact, the PLDU deals	

	with software and does not make any distinction between 'simple software and AI systems. Surely the system of presumptions of this proposal is much more difficult for a consumer to enact than the one set in the PLDU but also for a manufacturer it is not easy to understand. Further, this directive is going to heavily influence the **civil procedural rules** of the Member States. Specifically, Article 3- disclosure of evidence and rebuttable presumption of noncompliance- and Article 4 of the proposal – rebuttable presumption of a causal link in the case of fault-provide principles according to which the MS civil procedural laws will need to conform.	
Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services (Text with EEA relevance.) PE/26/2019/REV/1 *OJ L 136, 22.5.2019, p. 1–27* **(DCDS)** Directive (EU) 2019/771 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC (Text with EEA relevance.) PE/27/2019/REV/1 OJ L 136, 22.5.2019, p. 28–50 771(**SG**)	These directives regulate contractual liability aspects of liability. They both are interesting as they are complementary in character, and they do consider both the notions of **good with digital elements** (Article 2.5.a SG, Article 2.3 DCDS). *They are applied both to personal and healthcare robots whenever there is a conformity issue about the interconnected good or the digital service acquired and downloaded and supplied to the good*. Services and goods are judged according to **conformity criteria** which can be **objective** (mainly connected to technical features that were promised to the consumer) but also **subjective** conformity criteria which are mainly connected on the expectations that the seller or trader made the consumer have about the connected object or digital service/content. The seller or trader are always presumed liable (**rebuttable presumption**) for the non-conformity of the good/service. The remedies for both these directives are almost the same and are the 'traditional ones' of EU consumer law. They are almost the same for the two directives: **repair**, **substitution**, **price reduction**, and or **termination of the contract**. As far as the DCDS, there are some more specifications concerning the duty of the trader to ensure, in the event of a termination of a contract (Article 16 DCDS), the respect of some obligations. The trader needs to reimburse the sums paid in carrying out the contract and they will	Contractual liability in this case does not start from the assumption that the contracting parties are equal but that the one buying the good or service is **more vulnerable** as a consumer as they do not have any leverage on the trader or seller. Hence, these rules might appear more favourable to the weakest of the two parties

	comply with the GDPR obligations including Article 20 GDPR on the portability of data. Finally, the trader must not use content other than personal data that was provided or created by the consumer unless such content *'(a) has no utility outside the context of the digital content or digital service supplied by the trader;* *(b)only relates to the consumer's activity when using the digital content or digital service supplied by the trader;* *(c) has been aggregated with other data by the trader and cannot be disaggregated or only with disproportionate efforts; or* *(d)has been generated jointly by the consumer and others, and other consumers are able to continue to make use of the content'* Article 16(3) DCDS.	
General liability issues under Italian law (civil Code)	There are two main kinds of liability in Italian private law: contractual and extracontractual (tort liability). The former (almost) always implies the need of a contract among parties (e.g. a contract of sale). The latter kind of liability does not need a contract to be valid (e.g. a pedestrian is run over by a car). In liability parlance, there are shared concepts among extracontractual and contractual liability but with different declinations. Some examples are • disrespect of a legal obligation •causality link, •fault/ presumption of fault The general rules for both contractual and extra-contractual liability can be found in the **Italian Civil Code** and **special laws** such as the Consumer code and Private Insurances codes. **Obstacle:** Both the SG and DCDS are implemented in Italian law. The implementation of the PLDU and especially the AILP will also **significantly impact** the concept of causality link and the concept of defectiveness in Italian private law together with civil procedural law.	The ethical principle underpinning these rules is that liability must restore *the status quo ante*, meaning that **it must limit itself to compensate for the value or to restore the state of how things were before the damage**.

3.4 DATA LAWS

Data Laws is an unofficial term that Activity 4 used to regroup the enacted and proposed legal acts that concern data protection, data sharing and data access rules. To sum up, data in all its forms. In order for the Fit4MedRob partners to build a new generation of medical devices and allied technologies, they need to know, in a concise and a succinct way what the main legal and compliance requirements they need to abide by. These laws are fundamental for the design and deployment of a new generation of robotic devices as they will mostly rely on data both in situ (within the device) and remotely (in the cloud). Only two of the following documents are enacted[5] and just one of these, the GDPR, almost fully implemented. The Table 5 proposal acts that are listed below will take more time to become effective as they both need to be voted into law and implemented at a national level. In fact, they concern the construction of new infrastructures and regulated data-based economic activities[6]. That is why it is important since now to follow the evolution of these proposals and use their rationales as ethical compliance to integrate in the design and in the deployment of future robotic devices. The table sums up the most important elements that the Fit4MedRob consortium needs to focus on for its activities. The list will become more structured and become definitive in the following iterations of this deliverable.

Table 5 Data Laws

Name of the Initiative	Legal compliance and obstacles	Ethical compliance
Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) OJ L 119, 4.5.2016 (**GDPR**)	It sets the of principle data protection of personal data but also of its safe and as free as possible sharing. **Obstacles**: Article 9 GDPR implementations in the national states can be implemented and – especially for **scientific research** and **statistics purposes** – could constitute a gap for data sharing. For example, in Italy, the consent of the data subject is required also in cases where the GDPR seems to promote another legal basis for data processing, like in the case of use and reuse of health-related data for scientific purpose. Difficulty in the attribution of the different roles of **data controller**, **data processor** and **third party** with connected objects such as personal care robots in connected environments (e.g. hospitals or the home) as in the Fit4MedRob project. This has practical consequences in terms of **liability** and **accountability** allocation	The GDPR is important as it sets for the first time some ethical principles to enhance the data protection and privacy as fundamental rights: • Accountability. • Lawfulness. • Fairness. • Transparency. • Data minimisation. • Accuracy. • Storage limitation. • Integrity and confidentiality • Privacy-by-design and by-default
Italian Code of Privacy D. lgs 193/2003 updated with D.lgs. 101/2018	Code: at articles **100**, **110** and **110bis** the Italian Privacy Code sets the main rules to process personal data for **medical biomedical** and **epidemiological** research and further data-sharing for these activities. According to article 100 public entities such as **universities**	Same as above

[5] The GDPR and the DGA, see Table 1 for the complete legislative reference.

[6] We are referring to the Data Act and the European Health Data Space, see Table 5 for the complete legislative reference.

Italian Data Protection Authority provisions implementing and /or clarifying some aspects of the GDPR	can communicate and share data concerning study ad research activities even to private parties and through electronic means. Articles 110 and 110bis are about the **medical**, **biomedical** and **epidemiologic research** and the **reuse** of data for **scientific research** or for **statistical purposes**. In Article 110, data processing can be carried out when there the application of Article 9 (2) j GDPR conditions (which means that it needs to be carried out for reasons of public interest) are applicable and a Data Protection Impact Assessment (DPIA) has been carried out. Further, consent is not necessary when it implies a disproportionate effort or might the result of the whole research. Article 110 bis instead explains that the national Data Protection Authorities can authorise the reuse for scientific or statistical research when: I) it is not possible to inform the interested data subject or II) the delay risks to bring prejudice to the outcome of the research. It adopts its decision within 45 days. The further treatment of personal data by third parties can be authorised by the national authority through general provisions. In this case the data controller shall submit the research project to the competent ethics committee for approval. Finally, the Data Protection Authority will indicate deontological guarantees to respect according to article 106, paragraph 2, letter d of this code. Under the law 56/2024, the Italian legislator partially modified Articles 110 and 110 bis through which it allowed the secondary use of data also for scientific research. This amendment facilitates the use of data for secondary purposes in view of the approval of the European Health Data Space which will allow health personal data to be shared easily. The new text of Article 110 explains that the National Data Protection authority can authorise the special treatment of personal data based on Article 9 GDPR because of scientific research or statistical targets to third parties that carry out essential research activities when informing the data subjects has become impossible or might entail a	

	disproportionate effort. All of this can be authorised only if appropriate measures to protect the rights of the data subject have been taken, such as the principle of data minimization that is recalled through the reference to Article 89 and 5 GDPR. This Article's amanedment was completed by decision n. 298 issued on 9.5.2024, of the Italian Data Protection Authority which adopted new safeguards under Article 110 of the Italian Code of Privacy, pending the implementation of new ethics rules according to Articles 2-quarter and 106 of the Italian Code of Privacy. It The new safeguards[7] state that it concerns two categories mainly of data subjects i) the data subjects that are deceased 2) and the ones that cannot be easily contacted. If that is the case, the data controllers (which generally are the sponsors of the trial or the research entity) will need to do the following: I. Get a positive opinion from the competent ethical committee concerning the treatment of the personal data of the data subjects. II. Before the ethical committee, they should motivate why it was impossible for data controllers 1) to contact data subjects; 2) to get data subjects' consent because it would lead to a disproportionate effort (this does not prevent data controllers from documenting the reasonable efforts made); 3) that trying to obtain data subjects' consent would entail a significant prejudice for the objectives of the research. All of the above conditions must be justified by ethical and organisational reasons that are explained infra. c. If these conditions are met, data controllers shall **only** conduct a data protection impact assessment according to Article 35 GDPR. This is important because it will exempt researchers from asking a preventive authorization from the National Data Protection Authority. This is extremely important for the Fit4MedRob initiative especially	

[7] 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], https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/10016146 Accessed, 11 October 2024.

	when it comes to design for retrospective clinical studies. To know more about the ethical and organizational reasons that might make impossible or be of prejudice to the research, the Italian National Data Protection Authorisation states the following. As far as ethical reasons are concerned that make it impossible to obtain data subjects' consent, they do occur when the needed information would inform data subjects about research results that may cause material or psychological damage to them (e.g they might not have known that they suffered from a rare and incurable disease but the contact for the research might make it known to them). The organisational reasons for which it might be impossible to re-contact the patient are connected to the fact that, if the re-contact occurs, then the quality of the research would decrease. The factors to look for when evaluating a decrease in the research quality level are the following: the inclusion criteria, the recruitment procedures, the statistical population of the sample and how much time passed since obtaining the personal data for the first time. Article 110bis of the Italian Privacy Code was also amended. The most interesting part of the article also for the Fit4Medrob Initiative is Article 110 bis (4). In fact, the IRCCSs are mentioned and for them there is a big exception as their research activity is not considered as a secondary use of data. In order to apply this part of article 110 bis (its fourth paragraph) the Italian National Data protection authority issued some FAQs[8]. Briefly the FAQs tate the following. • The legal basis that IRCCS should use as a basis for the personal data data processing is consent according to Article 6(1) and 9(2)(a) GDPR • There will be the need of a data protection impact assessment to be published on the websites of the centre that promotes the	

[8] The FAQs on the IRCCS are available at this link https://www.garanteprivacy.it/temi/sanita-e-ricerca-scientifica/irccs Accessed on 11 October 2024.

	trial and on other centres webiste that might participate in the same trial • There is still the need that the IRCSS ask an authorisation to the National Data Protection Authority whenever it cannot avoid serious risks for the data subjects **Data protection authority provision on 5.6.2019**[9] concerns specific categories of data. One of the joint documents deals with data that are used scientific research (Autorizzazione generale 9/2016). Basically, it explains the interaction between Articles 5 and 89 of the GDPR. It is possible to use derogations for scientific research when collecting data subjects' consent for the processing of their health data if the following conditions are met: 1) **ethical reasons** concerning the data subjects' ignorance about their health condition 2) **unsolvable organization problems** which could affect the final results (for instance they are either dead or not reachable) 3) **serious health concerns** (and in that case the research should have a specific result the objective to make the data subjects' health better). In any case, the data controller must put in place the **technical and organizational measures** apt to safeguard the data subjects' right to data protection according to the principle of minimization. **Deontological rules on processing for scientific research**[10] One of the most important rules of this document is to be compliant with Helsinki Declaration on patient's safety. The data subject must express their intention to be informed about possible health-related issues that they might not have been aware about. Moreover, this document mandates the respect	

[9] 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] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9124510 Accessed 25th October 2023.

[10] 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]https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9069637 Accessed 25th October 2023.

	of these deontological rules by universities and research institutes carrying out medical research. **Rules on the use of consent to re-use data concerning health Opinion of 30 June 2022, n. 9791886**[11] The Italian Data Protection Authority (DPA, aka Garante per la Protezione dei Dati Personali) explained that for medical research it is possible to use consent to process data. However, the initial consent clause must not be ultra-general, but it is required that consent must be obtained and must be specific for each kind of processing that will be carried out starting from the health data that the patient had provided the controller originally. **Obstacles:** Following up on the previous point, it can be difficult to create an information policy that is sufficiently granular and specific that can cover all the further research and re-use activities	
Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (Text with EEA relevance) PE/85/2021/REV/1 OJ L 152, 3.6.2022, p. 1–44 (**DGA**)	The DGA sets up quite a complex system of data intermediaries based on the principle that private parties can access certain categories of data of the national public sector bodies which are generally protected 1) by **commercial confidentiality**, 2) **statistical confidentiality**, 3) **protection of intellectual property of third parties** (Article 3 DGA). **Obstacles**: The DGA is creating a complex system of data intermediaries in the 27 EU member states which will give each their own implementation. SMEs and start-ups might not be aware of **how to take advantage of the data that the public administration can let them access according to the DGA**. Moreover, the role of data intermediaries, which can share data for altruistic and non-altruistic purposes (depending on their mission), are still brand-new entities which have never existed in this form. It could constitute a great opportunity, but it still is difficult to	Data re-use: "*the use by natural or legal persons of data held by public sector bodies, for commercial or non-commercial purposes other than the initial purpose within the public task for which the data were produced, except for the exchange of data between public sector bodies purely in pursuit of their public tasks*"; Article 2(2) DGA Data altruism: the ethical and legal principle that allows a person to share their data related to health for research and business implementing research on the basis of consent. Article 2(16) DGA

[11]Parere ai sensi del ai sensi dell'art. 110 del Codice e dell'art. 36 del Regolamento - 30 giugno 2022 [9791886] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9791886 Accessed 25th October 2023.

	visualise how these data intermediaries will work in practice	
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) PE/49/2023/REV/1 OJ L, 2023/2854, 22.12.2023, (**DA**)	The DA is set to be the most general regulation for all kinds of IoT devices in the EU which could also apply both to personal care and healthcare robots. It deals with several issues: • **data access rules** which concern **new business subjects**: a) a **user** (which could be a consumer or a professional) who asks to have access to the IoT device's data to the b) **data holder**, the manufacturer of an IoT product and a 3) **data recipient** which is a subject authorised by the user to receive the data asked from the data holder. Upon reception of the data, the user or the data recipient could develop a product or a service which will not compete with the original one(s) but it will be destined to secondary markets. •**data-holder requirements** about how to make data available and **dispute settlement provisions**; • the **unfair contractual terms** in data access contracts (if a clause is unfair according to Article 13 DA then it is null and void); • data availability for public **sector bodies and union institutions**, agencies or bodies based on exceptional need (e.g. pandemic); •**switching rules** between data processing services; •the **safeguards** for **non- personal data sharing in international context**; •**interoperability** rules. In theory it will be applicable for all IoT object (see the definition of connected product in Article 2 DA) also for e-health purposes. **Obstacles**: the DA has been criticised for its generality (which also extends to medical IoT hence to healthcare robots). Therefore, it will be applicable in theory both **to personal care** and also to **healthcare robots.**	The ethical-legal principle is that **access must be guaranteed by the subjects that are bound by the DA rules (data controllers)** and have to **provide data possibly for free**, if not by using the **F/RAND method** (Fair, Reasonable and Non-Discriminatory) to calculate access fees. Moreover, the users and data recipients of the accessed data must create a *product or a service that is not in competition with the original product/service* and must respect the **trade secrets** they might come across while accessing the relevant data. The enforceability of this aspect will probably be taken care of through non-disclosure agreements
European Health Data Space (EHDS, secondary use of health Data for research, COM/2022/197 final), (**EDHS**). The European Health Data space was finally approved on	EHDS proposal will give rise to a new EU harmonised framework which will eventually: • help EU citizens have **control over their health data** independently from the EU country they are in through the **European Health Records (EHR)**	The secondary use of genetic, biometric and data related to health is encouraged both for research and business purposes (**wellness apps are included in the EDHS**) much more explicitly in the GDPR. This is represented by the model on **data access permit** in the Annexes of the

24 April 2024 but still in the form of an interinstitutional agreements[12].	• **boost the use of health data** for better healthcare delivery, better research, innovation, and policy making • incentivise a secure exchange, use and reuse of health data in centralized infrastructures (the data access bodies) authorised by MS and the EU. **Obstacles**: The EDHS proposal sets the groundwork for the creation of a new system to share health record data and to take advantage of the secondary use of health data. However, to operate efficiently, it requires quite some work in terms of **standardization** and **interoperability** among the systems of the different EU Member States (MS), and the proposal in itself does not give much practical guidance on this aspect. Moreover, the national DPAs will need to revise or *partially change their strict interpretation of data re-use for research*. As for the AI Act, the next session on cybersecurity will deal with the cybersecurity aspects of the EHDS	proposal. Given the sensitivity of these kinds of data, access is streamlined through the evaluation of data access bodies to balance the ease of accessing health data by a larger platform of public and private subjects.

4 CYBERSECURITY LAWS

The survey circulated in October 2023 showed that the Fit4MedRob initiative partners were very interested in Cybersecurity issues related to their work. Cybersecurity is a fast-paced and ever-growing regulatory and legal compliance source that not only public entities, but private ones as well, will need to consider mandatorily. In the following table there is a synthetic explanation of the main cybersecurity legislations, which share their EU origin and their Italian implementation. The language will be more difficult to read as well as in the following section due to the technicality of the issue.

4.1 CYBERSECURITY LAWS: EU AND NATIONAL IMPLEMENTATION LEGISLATIONS

Table 6 cybersecurity laws

Name of the Initiative	Legal compliance and obstacles	Ethical Compliance
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	The NIS Directive aims at improving and **harmonizing** the cybersecurity level across Europe. NIS requires each Member State to adopt a **national cybersecurity strategy** plan that would protect the operators of essential	Not applicable unless we consider that these regulatory blocks protect interests that the State recognizes as essentially important, and health

[12] The interinstitutional agreement on the EHDS is available here https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/CJ43/AG/2024/04-09/1299790EN.pdf Accessed 11 October 2024.

systems across the Union OJ L 194, 19.7.2016, p. 1–30 **NIS Directive**	services (OESs) and digital service providers (DSPs) identified by each Member State. Among the sectors covered for the OES, health is also included (including hospitals and private clinics). OES must adopt adequate and proportionate technical and organisational measures to manage risks and to prevent and minimise the impact of network and information system security incidents in order to ensure service continuity. Such requirements are to be set by the national implementation of the NIS Directive (see below). Moreover, OES have notification obligations only in case of incidents with a substantial impact on the provision of service. ***The notification should be submitted to the national Computer Security Incident Response Team (CSIRT)*** or the national competent authority ***without undue delay***. Once the notification has been made, the national competent authority or CSIRT will support the notifying entity with assistance in handling the incident. Sometimes there is a need to notify the incident to the public; in this situation the competent authority or the CSIRT, after consulting the notifying operator of essential services, may communicate the individual incident to the public to raise awareness of the prevention or management of an ongoing incident. ***Not all the incidents should be notified, only the ones which have a significant impact***, according to the following parameters: (a) the **number of users affected** by the incident, in particular users relying on the service for the provision of their own services; (b) the **duration** of the incident; (c) the **geographical spread** with regard to the area affected by the incident; (d) the **extent of the disruption** of the functioning of the service; (e) the extent of the **impact on economic and societal activities**. **Obstacles:** The NIS Directive includes a distinction between OES and DSP and in case of collaboration between the two (e.g. a hospital relying on cloud computing service for storage of electronic information), in case of security incident occurring to the DSP, the **notification of such incident is allocated on the OES,** based on the information provided by the DSP, pursuant art. 16 (5) NIS.	information is deemed as such.
Legislative Decree N. 65 of May 18, 2018 Decree-Law of September 21, 2019 (Perimeter Decree).	**Leg. decree 65/2018** defines the regulatory framework for network and information security measures to be adopted and identifies the entities responsible for implementing the	

D.P.C.M. No. 131 of July 30, 2020 (DPCM 1) D.P.C.M., No. 81 of April 14, 2021 (DPCM 2) Presidential Decree No. 54 of February 5, 2021 Decree Law 82/2021	obligations under the European legal framework. Note that to reach a higher level of security of networks, information systems and IT services of public administrations, as well as national public and private entities and operators, **the legislation defines a so-called National Cybersecurity Perimeter with so called Perimeter Decrees.** Article 1 (8) Perimeter Decree requires OES and DSP providers to comply with the cybersecurity requirements outlined in Decr. Leg. no. 65/2018, if they are at least equivalent. **DPCM 1** identifies the **public** and **private** entities that fall within the Perimeter and the *criteria for creating lists of relevant networks, information systems and IT services of those entities*. **DPCM 2** defines the **procedure for reporting incidents** and **mandatory technical security measures**. **Presidential Decree 54/2021** establishes a procedural framework for the procurement of ICT assets for use on networks, information systems and IT services by entities within the Perimeter. DPCM 1 establishes the procedural criteria by which the relevant public administration shall identify the entities included in the Perimeter (the list is not subject to publication). **Entities within the Perimeter are obliged to prepare a list, updated annually, of the networks, information systems and IT services that constitute the ICT assets under their control**. The list must be compiled using a **scalable, risk-based approach**. Moreover, a description of the *architecture* and parts of the *previously identified ICT assets* based on a *template provided by the National Information Security Agency should be submitted*. The reporting procedure and risk management measures (defined in DPCM 1) distinguish security incidents according to their impact on ICT assets. The provided taxonomy distinguishes two types of incidents based on their severity: incidents identified in Annex A, Table 2, are to be reported within one hour, while the ones falling in Table 1 should be reported within six hours. DL 82/2021 established the **National Cybersecurity Agency** to assume the role of the National Cybersecurity Authority as the **single point of contact for the NIS Directive** and the **National Cybersecurity Certification Authority for the Cybersecurity Act**.	

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)	The NIS 2 Directive aims to update and solve some of the open issues emerging in the application of the NIS Directive. Main changes are the new criteria for the identification of the operators subject to the legislation: **all private or public entities that are at least qualified as medium enterprises**. Moreover, a new distinction is adopted between essential entities (EE) and important entities (IE). Among the EE the health sector is still included with the extension to EU reference labs, as well as research and manufacturing of pharmaceuticals and medical devices. EE are required to adopt security measures that include incident response, supply chain security, encryption and vulnerability disclosure. However, also in this case, the national implementation measures will be defined in detail such requirements. As regards the incident notification, the procedure is more detailed and encompasses the following steps: (1) the affected entity should inform, with an initial report, the national authority or CSIRT within 24 hours from when they first become aware of an incident (2) the entity will provide a full report within 72 hours from when they first become aware of an incident (3) The entity will submit a final report one month later from the initial report, after the complete restoration of the problem.	
Legislative Decree 4 September 2024, n. 138 Implementing 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	Identification of Essential and important entities: the Italian cybersecurity authority (ACN) will draw up the list of the companies and public administration covered by the scope of application of the legislative decree by April 2025. All entities will have to register from the date of publication on a special platform at ACN Security obligations are not mentioned in the text but to be defined by the ACN on the basis of the degree of exposure to risk; the size of the entity; the probability of incidents occurring; and the severity (including the economic and social impact). The sanctioning treatment is differentiated according to the type of violation - non-compliance with the obligations imposed on the management bodies; failure to implement technical, organisational and operational measures; failure to notify. EEs: up to 10 million or up to 2% of the total annual worldwide turnover for the subject's previous financial year	

	IE: up to 7 million or up to 1.4% of the total worldwide turnover - the failure to register, communicate or update information on the ACN platform; failure to comply with the procedures established by ACN for the registration, communication or updating of data; failure to communicate or update the list of activities and services for the purposes of their categorisation; failure to implement obligations relating to certification schemes; failure to cooperate with the ACN in carrying out its tasks and exercising its powers; failure to cooperate with the CSIRT Italia. EE: up to 0.1 per cent of the annual turnover IE: up to 0.07 per cent of the annual worldwide turnover - In the event of repeated violations, sanctions may be increased up to threefold - In the event of a warning from the ACN requiring the implementation of certain measures being ignored, it is possible to temporarily suspend a certificate or authorisation relating to the services provided by the subject.	
PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL ON HORIZONTAL CYBERSECURITY REQUIREMENTS FOR PRODUCTS WITH DIGITAL ELEMENTS AND AMENDING REGULATION (EU) 2019/1020 COM/2022/454 FINAL The Council of the EU agreed on the final version of this document last 10 October 2024[13]	The CRA regulation provides for the horizontal cybersecurity requirements for products with digital elements throughout their entire life cycle. Products with digital elements are defined as "*any software and hardware product and its related remote data processing solutions, including software or hardware components to be placed on the market separately*". All products with digital elements must be designed, developed and manufactured in such a way as to ensure an appropriate level of cybersecurity. Manufacturers should follow **conformity assessment procedures,** proving that their products comply with the **essential requirements defined in Annex II.** The security requirements address the following issues: *security by default measures, confidentiality protection, integrity and availability of the data and the networks, data minimisation measures, resilience measures (particularly against DoS attacks), safeguards against network effects, records on internal activity, and data portability*. However, these requirements are still general and will have to be defined in detail on the basis of the work of the European Standardisation	

[13] Here is the final version of the CRA available while waiting for the official publication https://data.consilium.europa.eu/doc/document/PE-100-2023-INIT/en/pdf

	organisations upon a request by the Commission. The technical documentation that manufacturers should prepare before the products are put on the market should contain an assessment of cybersecurity risks and describe the means used by the manufacturer to meet the essential cybersecurity requirements and mitigate the risks. The conformity assessment procedures to be followed depend on the class of risk of the product, ranging from an internal control procedure to a conformity assessment based on full quality assurance. Internal control conformity assessment is only available for those products with digital elements that do not perform any of the functions listed in Article 6 (2). In case the manufacturer becomes aware of exploited vulnerabilities or incidents having an impact on the security, he/she is obliged to notify the event within 24 hours to CSIRT or to the competent authority, providing the most relevant information about the event, as well as the corrective and mitigating measures taken. The information about the incident should also reach the product user to request the latter's collaboration in the deployment of corrective measures. **Obstacles:** The scope of application excludes medical devices for human use (EU Regulation 2017/745) and *in vitro* medical diagnostic devices with the same intended use, together with their related accessories (EU Regulation 2017/746); therefore, for these products, only the requirements set by MDR and CTR are applicable. However, if the product is a 'wellness device', it is subject to CRA.	
European Health Data Space (EHDS, secondary use of health Data for research, COM/2022/197 final), (EDHS)	See above. The Electronic Health Records (EHR) that will be available in the EHDS the regulation imposes a set of **security requirements** (Annex II). The security requirements mainly focus 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. The EHR system should enable patients (i.e. data subjects) to restrict access to electronic health data, except for emergencies. Further clarification of these requirements will be provided through 'Common specifications' to be adopted by the Commission, Article 23 EHDS.	

	The security requirements are subject to a **certification process** based on the self-assessment of the EHR system manufacturer. The market surveillance authorities oversee the process set up at the national level, exercising their powers of investigation and enforcement and requiring the EHR system manufacturer to take preventive or corrective measures in case of serious incidents. Serious incidents are defined as any malfunction or deterioration in the characteristics or performance that directly or indirectly leads, might have led or might lead to the death of a natural person or serious damage to a natural person's health; a serious disruption of the management and operation of critical infrastructure in the health sector. In this case, the manufacturer is required to notify to the market surveillance authority no later than 15 days after becoming aware or immediately after he has established a causal link between the application and the event (or the reasonable likelihood of such link). **Obstacles:** (1) *essential requirements dedicated to security are focused only on the **confidentiality perspective**, disregarding the issues of integrity and availability of networks and data* (2) the monitoring activity of market authorities can only be exercised after the products are put on the market, with no ex-ante assessment of compliance with the essential requirements.	
Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 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) Text with EEA relevance. PE/24/2024/REV/1 (**AI Act**)	See above. Art. 15 provides for cybersecurity requirements along with the ones of robustness and accuracy. The detailed definition of the technical and organisational solutions is left to the standardisation provided by the European Standardisation bodies. A presumption of compliance is acknowledged if the AI system is certified according to a cybersecurity scheme adopted in line with the Cybersecurity Act (Regulation 2019/881). Art. 55 provides that GPAI should also ensure an adequate level of cybersecurity. Such **'adequate level' should be defined by codes of practice and, if available, by harmonised standards**. Recital (115) clarifies that in GPAI cybersecurity should take into account the entire model cycle and includes a long list of risks that may emerge, ranging from accidental model leakage to unsanctioned releases to circumvention of safety measures, to defence against cyberattacks, to unauthorised access or model theft.	

	Obstacles: Article 15 (5) focuses only on the first step of AI design, namely the model training, while limited or no attention is addressed to attacks occurring during deployment.	

4.2 CONCLUSIVE REMARKS ON CYBERSECURITY LAWS

The main observation is that the cybersecurity related laws that have been recently approved at the EU level and are being implemented at a national level concern duties that will need to be respected by organizational entities of which the Fit4MedRob initiative partners might be a part of. It will be the task of each of the Initiative's partners to sensibilize their personnel to the cybersecurity threats that they might face and linking their awareness to the specific legislations mapped herein.

In terms of the cybersecurity requirements for the construction of safer connected products, including personal care and healthcare robots, there might be a higher level of cybersecurity protection for the former ones as the CRA will apply to the majority of connected products, with the exception of medical devices. As far as healthcare robots and other allied technologies applied to healthcare, they might have a more diverse and layered legal framework as far as cybersecurity is concerned. Within the MDR there are no explicit references to cybersecurity standards, but the ISO standards applicable to medical devices include cybersecurity standards.

Furthermore, the EHDS and the AIA might give more indications concerning the creation of harmonised standards and common specifications for the creation of health records and ways to give access to health data while protecting them (as they are special categories of personal data under Article 9.2 GDPR). This might be an obstacle in terms of applying all the necessary cybersecurity compliance rules while designing and, subsequently, marketing new healthcare robots and allied technologies.

5 INTELLECTUAL PROPERTY

This section analyses the most relevant forms of Intellectual Property Rights (IPRs) that might be useful for the consortium. These specific topics were selected based on the replies to the 2023 survey about the consortium's internal needs. This overview will be divided into four main categories: copyright protection (5.1), patents (5.2), trade secrets (5.3), industrial design (5.4) and general IPR protection instruments. As these group of IPRs entail very similar obstacles among them, there will be a conclusive subsection (5.6) which sums them up.

5.1 COPYRIGHT

As a preliminary remark, one must state that copyright is a set 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. It could interest literary, scientific, and artistic domains. 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[14]. This rule would apply regardless of the domain, mode, or form of expression, quality or content.

The economic rights encompassed within copyright are:

1) Right for **reproduction right**,
2) **Right to communication to the public,**
3) **Right to making available to the public,**
4) **and right for distribution (including lending and rental**).

14 Ibid. Also see: Directive 96/9/EC, Art. 3(1); Directive 2009/24/EC, Art. 1(3); Directive (EU) 2019/790, Art. 14.

In addition to the abovementioned economic rights, copyright, at least in the EU context, grants several **moral rights to the author/creator of an original work.**[15]

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*.

The author/creator of a work is, in principle, the first copyright owner of the work. Whereas the moral rights remain with the author/creator, the economic rights encompassed within copyright can be transferred or licensed to third parties. The transfer of copyright as such 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*. This would be particularly important for the publications which will be funded by the Fit4MedRob initiative. It would be advisable that all the publications funded by the Fit4MedRob initiative be in Gold Open Access, or at least Green Open Access to enhance the availability of knowledge created within this public- funded project.

The use of copyright-protected work is not restricted to the transfer of copyright or the voluntary licensing of copyright by the copyright owner.

Both the EU and the national copyright legislations have several exceptions and limitations (E&Ls) to copyright. This makes the use of copyright-protected works easier in certain cases (e.g. for research purposes) *without the authorization of and, often, remuneration of the copyright owner.*

Moreover, in the EU and national legislative frameworks, there are other mechanisms to achieve the same result. An example is compulsory licenses. This instrument is thought for certain uses of copyright-protected works. Last but not least, copyright does not confer eternal economic rights to its holder. Generally, copyright lasts during the **lifetime of the author** and **at least an additional fifty-year post-mortem**. Once this term of protection is over, the work in question falls into the **public domain** and can be freely used by anyone.

[15] Complementary to these rights of an economic nature are I) the rights to claim authorship, and II) to object to certain modifications and other derogatory actions.

Table 7 relevant EU laws on copyright

Name of the Initiative	Legal compliance and obstacles	Ethical compliance
Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs (Codified version) (Text with EEA relevance), OJ L 111, 05.05.2009, p. 16-22. (**the Software directive**)	Software Directive applies to computer programs "*in any form, including those which are incorporated into hardware*"[16] as well as the "preparatory design work leading to the development of a computer program" [17]. 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*" – hence, the logic, algorithms, and programming languages – are neither eligible for nor protected by copyright under the Software Directive.	Not applicable
Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, OJ L 77, 27.03.1996, p. 20-28. (**The Database directive**)	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*". This broad definition encompasses databases available in any form, including online and offline databases. However, computer programs involved in the making or operation of such databases are excluded from the scope of the Database Directive. The Database Directive regulates the legal protection of databases by copyright or by *sui generis rights*, and the regime applicable to the databases depends on their defining characteristics. Indeed, databases that are **original** in their structure and arrangement are protected by copyright,[18] whereas databases that required qualitatively or quantitatively substantial investments in the collection, verification and organization of their materials are protected by sui generis rights[19]. Copyright protection	Protection of the effort and resources put in the creation of the database is seen as protection of a creative and literary work.

16 Ibid recital 7
17 Ibid.
18 Ibid, Art. 3(1).
19 Ibid, Art. 7(1).

	consists of 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*"[20] 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*"[21]. Copyright protection applies to databases created before 1 January 1998,[22] while the *sui generis* protection extends to databases completed from 1 January 1983[23]. 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.[24] In other words, 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 DA Regulation also partially changed the Database directive content. It will not be possible to use the *sui generis protection* for when data is obtained from or generated by a connected product or related service falling within the scope of this Regulation, especially when Article 4 or 5 on data access and data sharing contracts[25]	

20 Ibid, Art. 7(2)(a).
21 Ibid, Art. 7(2)(b).
22 Ibid, Art. 14(1).
23 Ibid, Art. 14(3).
24 Ibid, Artt. 1(3), 3(2).
25 Article 43 DA.

Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, OJ L 167, 22.06.2001, p. 10-19 (the Information Society Directive, known, hereinafter **InfoSoc Directive**)	The InfoSoc Directive is one of the main building blocks of the EU copyright framework as it covers a wide spectrum of copyright-related matters, **including the technological protection measures (TPMs) and digital rights management (DRM)** systems. It also containsthe largest set of copyright flexibilities introduced in the EU copyright acquis so far. In this regard, the InfoSoc Directive is essential for Fit4medrob 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 this regard, it is worth noting that the mandatory E&L[26] to facilitate temporary rreproduction inArticle 5(1) of the InfoSoc Directive, still constitutes the lynchpin of researchers' and ROs' time- and cost-efficient endeavours to train AI models by using copyright-protected works, despite the newly introduced text and data mining (TDM) exceptions with the CDSMD. 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,[27] yet without prejudice to acts concluded and rights acquired before this date[28].	As mentioned above.
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. (The Copyright in the Digital Single Market Directive, hereinafter **CDSMD**) The Member States were given time to transpose the Directive into their national laws by 7 June 2021[29].	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** (exceptions and limitations) 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	As mentioned above.

[26] It stands for Exceptions and Limitations (E&L).
27 Ibid, Art. 10(1).
28 Ibid, Art. 10(2).
29 Directive (EU) 2019/790, Art. 29.

Despite the significant delays in the process, the transposition of the CDSMD was finalized in 2023	Fit4MedRob activities due to being the only copyright instrument to introduce mandatory E&Ls to copyright and related rights for TDM.	
Directive 2006/116/EC of the European Parliament and of the Council of 12 December 2006 on the term of protection of copyright and certain related rights (Codified version), OJ L 372, 27.12.2006, p. 12-18 (the **Term Directive**)	The Term Directive is also worth noting in the context of the Fit4MedRob 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 sets the boundaries **of the public domain**, which, in its broadest terms, *refers to the sum of works and other **subject-matter** that are not protected by copyright or related rights or materials as such **whose copyright protection has lapsed***. Therefore, the public domain is a generic term to collectively refer to the materials that can be used, in theory, without authorization and payment of royalties/fees. Second, the Directive crystallizes the rules regarding the duration of the economic and moral rights of the authors and creators of original works. Therefore, this Directive is essential for researchers and research organisations involved in the Fit4MedRob consortium to contemplate the term of their copyright over their prospective scientific output.	As mentioned above.

5.2 PATENTS

Patent refers to a document issued, upon application, by the competent authority (often an industrial property office) which, on the one hand, consists of a detailed description of an invention and, on the other hand, **provides a legal monopoly in favour of the applicant**, or the patent owner or inventor, **to prevent the unauthorized commercial exploitation of the patented invention**. The term "invention", in this context, refers to "a solution to a specific problem in the field of technology", 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 are as follow: (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.

Just like copyright and other IPRs, the legal protection provided by a patent is limited in time to balance the private interests of the patent owner with the public interest. The term of legal protection of 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". After the lapse of the term of protection, the patented invention falls into the public domain and thus can be freely used by anyone.

However, a patent's exclusive rights of the patent holder are not unlimited. 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.

Table 8 Relevant EU Patent Laws

Name of the initiative	Legal compliance and obstacles	Ethical compliance
The Unitary Patent Protection Regulation 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**. UPP**	The main achievement of this legislation was the creation of a **European patent with a unitary effect**. This means that if an inventor gets this kind of protection, it will not only be valid in its own MS but also for all the other MS that have adhered to the European Patent Convention (EPC)- The other main advantage is that a European Unitary patent will be considered as a patent of each of the MS that have adhered to the convention. For example, if an Italian inventor decides to patent an invention through the EPC and gets the patent, the EPC patent will be considered as an Italian national patent and, if it needs protection in another state such as France, as a national French patent. The international organization to refer to is the European Patent Office (EPO).[30] EPO decides that the innovation is not worthy of the European Unitary Patent it provides a board of appeal[31].	Protection of one's invention in the EU while fostering innovation at the same time.
The Directive on the Legal Protection of Biotechnological Inventions 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. **(LPBI)**	This Directive regulates the conditions for the legal protection of biotechnological inventions. It defines biological material as "*any material containing genetic information and capable of reproducing itself or being reproduced in a biological system*"[32] and also microbiological process as "*any process involving or performed upon or resulting in microbiological material*"[33]. It sets some ground principles concerning what can or cannot be patented if we have	In these rules there are ethical concerning about the creation of biological material. One ethical principle which became a rule in this directive is the prohibition to patent techniques to clone humans. This is justified by ethical and moral concerns which in legal terms are identified in public order and morality-

[30] EPO, The EPO at a glance, https://www.epo.org/en/about-us/at-a-glance. Accessed on 11 October 2024.
[31] EPO, Decision of the Boards of Appeal, https://www.epo.org/en/case-law-appeals/decisions. Accessed 11 October 2024.
[32] Article 2(a) LPBI
[33] Article 2(b) LPBI

	biological material or micro-biological processes. **What can be patented**: inventions (hence they must be new, involve an inventive step and can have an industrial application) if they involve a biological material or involve a microbiological process. If the biological material is "*isolated from its natural environment or produced by means of a technical process may be the subject of an invention* ***even if it previously occurred in nature***"[34]. **What cannot be patented (which already exists):** plants and animal varieties and essentially biological processes to produce plants and animals. **What cannot be patented:** • processes for cloning human beings, • processes for modifying the germ line genetic identity of human beings, uses of human embryos for industrial or commercial purposes, processes for modifying the genetic identity of animals which are likely to cause them suffering without any substantial medical benefit to man or animal, and also animals resulting from such processes[35] Another important point of this directive also for the Fit4MedRob initiative is the **compulsory cross licences principle** which might be used whenever breeder cannot acquire or exploit a plant variety right without infringing a prior patent	
Proposed Regulation on Standard Essential Patents 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.	Standard essential patents, in short (**SEPs**), are patents that are essential to create standards. Their main application is with the Internet of Things and 5G connectivity standardisation and application processes. As an example, keep in mind that there might be hundreds of SEPs in a single smartphone[36]. The Commission has been working since 2020 to frame what essential means in this context[37].	

[34] Article 3(2) LPBI.
[35] Article 6 LPBI.
[36] https://www.eesc.europa.eu/sites/default/files/files/factsheet_-_standard_essential_patents_1.pdf
[37] R. Bekkers, Pilot Study for Essentiality Assessment of Standard Essential Patents, 2020, https://op.europa.eu/en/publication-detail/-/publication/1829605f-2d3a-11eb-b27b-01aa75ed71a1/language-en Accessed 11 October 2024.

	They generally involve two kinds of subjects: one is a SEP holder, which creates the standard, and the implementer, which needs this standard to legally create an invention. Given SEPs importance for the IoT sector and to avoid that innovators of these essential standards patent their inventions and then they apply very high fees and to have more transparency on the concept of essentiality[38] the EU Commission decided to publish this regulation proposal which the European parliament approved at the end of February 2024. The main objectives of this regulation are the following. The proposal in itself aims at facilitating SEP licensing negotiations and lowering transaction costs for both SEP holders and implementers by (i) providing **more clarity** on **who owns SEP**s and **which SEPs are truly essential**; (ii) providing **more clarity on FRAND royalty and other terms and conditions**, including awareness raising with regard to licensing in the value chain; and (iii) facilitating **SEP dispute resolution.** As it is not a finally approved text some measures are worth focussing on[39]: For better transparency There will be an Electronic SEP register and a central electronic database to grasp the quantity of SEPs that are available in the EU market[40]. The SEP holders need to set an appropriate aggregate royalty for the use of the entire standard. Then, they need to communicate this royalty to the EUIPO competence centre. After that EUIPO will include that in the ad hoc register and database. If SEP holders fail to do all these actions, there must be the possibility to get an expert to prepare a non-binding proposal for [41]. One of the most important aspects of the SEPs regulation proposal is that it will be	

[38] F. Gennari, "Standard Setting Organisations for the IoT: How To Ensure a Better Degree of Liability?", *Masaryk University Journal of Law and Technology*, 15, 2, 2021, 153-173.

[39] Gleiss- Lutz, « European Parliament Gives Green Light For Regulation on Standard Essential Patents" https://www.gleisslutz.com/en/news-events/know-how/european-parliament-gives-green-light-regulation-standard-essential-patents. Accessed on 11 October 2024.

[40] Ibidem.

[41] Ibidem,

	possible to carry out an independent check about the the essentiality of a patent without having to conduct court proceedings. Moreover, in order to avoid an over-patenting phenomenon, the competence centre will have the possibility to task independent evaluators with carrying out random checks of the patents which are in the central register. This measure is in the interest of the initiative in general, as many activities might want to use SEP patents or, maybe create SEP patents for Biorobotics and allied technologies.	

5.3 TRADE SECRETS

Trade secrets, also known as know-how or undisclosed information, slightly differ from the other conventional forms of IPRs mainly because this form of IPR requires confidentiality whereas the remaining IPRs encourage dissemination of the protected content. Indeed, trade secrets holders' main interest is to avoid them becoming available to the public. Due to the same reasons, the legal protection envisioned for trade secrets do not require registration as opposed to patent or industrial design. In this regard, trade secrets' protection is an alternative to patent and design rights. At the same time, trade secrets can become powerful enablers of the appropriation of research and innovation results. Because of this, the EU legislator considers trade secrets as "the currency of the knowledge economy" as they provide both an economic value and a competitive advantage to their holders, especially in innovative industries and fields, such as the ones of the Fit4MedRob's initiative.

Table 9 EU relevant legislation on trade secrets

Name of the initiative	Legal compliance and obstacles	Ethical compliance
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. (**Trade Secrets Directive)**	The Trade Secrets Directive's main objective is to eliminate the differences between the MS's national laws concerning the definition of "trade secrets". Other examples of definitions that this directive seeks to harmonize are the definitions of "unlawful acquisition", "use" and "disclosure" of trade secrets by third parties. Furthermore, it harmonizes 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	It responds to the principle pacta sunt servanda (agreements must be fulfilled). In this case there is a non-written agreement that people working in the same environment where there is a trade secret must not divulge that to non-authorised personnel

	European standards for the legal framework on trade secrets. The Trade Secrets Directive is yet another legal instrument that is crucial for Fit4MedRob activities as research activities, including the ones without any commercial interest, invest to acquire and develop the know-how to provide a competitive advantage over other competitors, both commercial and non-commercial. Therefore, knowing the trade secrets discipline is important both to access and use third-party trade secrets in the context of R&D and innovation endeavours, and to apply optimal ways to keep confidential the know-how to be developed by the Fit4MedRob researchers and research activities.	

5.4 INDUSTRIAL DESIGN

Industrial design is a form of IPR that protects ornamental and non-functional features of an article or product.[42] It shall be emphasized that this right protects the design within a product, and not the product itself.[43] The design that is subject to industrial design rights may be two-dimensional, as well as three-dimensional, including those generated through the use of 3D-printing technology. This can indeed interest Mission 3 activities working with innovative materials. Nevertheless, not every design is eligible for legal protection. In principle, designs which respond to technical or functional considerations"[44] are excluded from the industrial design legal protection. Moreover, also designs that do not meet the novelty threshold set by the applicable law would also not be entitled to industrial design's legal protection[45].

In the EU, the design rights' acquisition ideally requires the design registration to the competent intellectual/industrial property office of the State in which one seeks legal protection for their industrial design. However, the Community Design Regulation also acknowledges legal protection, with a more restricted term of protection, to unregistered designs. Indeed, the EU's IP framework envisions a five-year legal protection for registered design. This five-year long protection for registered designs is renewable for up to 25 years[46]. For unregistered designs, instead it lasts only three years.[47]

Throughout the legal protection term, the rightsholder holds the exclusive right to use and prevent third parties from using their own design.[48] As far as the extent of the design rightsholder's rights, they 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. After the legal protection ceases, the design will become part of the public domain, and anyone can freely use it.

[42] WIPO Intellectual Property Handbook. Available at https://www.wipo.int/standards/en/handbook.html , accessed on 11 October 2024.
[43] Ibid.
[44] Agreement on the Trade-Related Aspects of Intellectual Property Rights, Art. 25(1).
[45] Ibid, Art. 25(1); Directive 98/71/EC, Art. 4.
[46] Council Regulation (EC) No 6/2002, Art. 12.
[47] Ibid, Art. 11.
[48] Agreement on the Trade-Related Aspects of Intellectual Property Rights, Art. 26(1).

Table 10 relevant EU legislation on industrial design

Name of the initiative	Legal compliance and obstacles	Ethical compliance
Directive 98/71/EC of the European Parliament and of the Council of 13 October 1998 on the legal protection of designs L 289, 28.10.1998, p. 28–35 Design directive	The Design Directive is one of the two EU legislations that sets the legal framework for industrial designs at the Union level. It harmonizes the design protection legislation of the Member States by setting the Union standards. In this context,, it provides a **unitary definition** for the term **"industrial design**" and clarifies the legal consequences of the registration of industrial designs, uniforms the eligibility criteria to grant legal protection to industrial designs, and lays down the scope and terms 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.	
Council Regulation (EC) No 6/2002 of 12 December 2001 on Community designs OJ L 3, 5.1.2002, p. 1–24 **Community Design Regulation**	The Community Design Regulation[49] sets the rules concerning the registration of an industrial design to the European Union Intellectual Property Office (EUIPO). [50] By doing so, the creator of the industrial design will secure legal protection within the borders of the EU. The Regulation lists all the procedural aspects of the legal framework revolving around industrial designs as well as all the steps to register a design to the EUIPO and the legal consequences of the acceptance or rejection of such an application. Moreover, it sets the Union rules on the legal protection of unregistered industrial designs. The Regulation provides the procedural details for EU-wide legal protection which co-exists with the national legal protection that stems from the registration of the design to a national intellectual/industrial property office. Whereas the legal protection envisioned in the latter case remains within the borders of the State in which the design is registered, registration of the design to the EUIPO secures the protection	

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

[50] EUIPO was previously known as the Office for Harmonization in the Internal Market (OHIM). For more information see the site https://www.euipo.europa.eu/it Accessed on 11 October 2024.

	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.	

5.5 GENERAL EU IPR PROTECTION INSTRUMENTS

There is just one EU legislation left, and it is defined as an umbrella regulation called IPRED as it can be used as a general form of protection for all IPRs. It sets a minimum threshold of measures, procedures, and remedies that will provide for effective civil enforcement of IPRs [51]. For a Fit4MedRob initiative participant, this means that when it comes to litigation for the protection of IPRs it will find the rules that will have the same effects and many common characteristics in different places in the EU. For example, let us take the case that an Italian inventor finds out that their invention is being used illegally in France. According to a general principle of the law, if your rights have been infringed, you have to start a trial where the defendant lives. This means that the French procedural law in this case will follow a similar/standardized litigation procedure, as in all the EU Member States. Its content is described in the following table

Table 11: General EU IPR legislation

Name of the legislation	Legal compliance	Ethical compliance
Intellectual Property Rights Enforcement Directive (IPRED) 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	Its **field of application** is any infringement of IPRs provided for by EU law and/or by the national law of the EU country concerned. This directive does not affect: 1) copyright, 2) EU rules governing the substantive law on intellectual property (that is, law defining rights and obligations in relation to intellectual property); 3) EU countries' international obligations and notably the Agreement on Trade-Related Aspects of Intellectual Property	N/A

[51] EUR-Lex, *Enforcement of intellectual property rights*, https://eur-lex.europa.eu/EN/legal-content/summary/enforcement-of-intellectual-property-rights.html Accessed 11 October 2024.

	Rights (known as the 'TRIPS Agreement'); 4) any national rules in EU countries relating to criminal procedures or penalties for infringing IPRs. What this directive does is trying also to set a **minimum common threshold for several aspects connected to IPRs litigation,** meaning a) how to apply for having the IPR protected b) how to protect evidence c) the minimum precautionary measures and some effective measures such as the recall or removal of the infringing goods from the market or their destruction; permanent injunctions or payment of damages[52]	

5.6 MAIN OBSTACLES AND CONCLUSIONS AS FAR AS IPRS

All the forms of IPRs protection that have been dealt with have one thing in common. The EU harmonisation came after the same form or similar forms of IPR had been present in the Member States. With the technological progress, the EU took the occasion to harmonise even more frequently many IP rights during the last years. For instance, think about the new Copyright in the Digital Single Market Directive (CDSMD), but also the harmonisation of trade secrets through the Trade Secrets Directive, and the modification of the Database directive because of the approval of the Data Act. As the last piece of this harmonisation of IPRs pushed by digital innovation is the proposal concerning SEPs.

As far as the main legal obstacles, they are similar for each of the IPRs groups highlighted in the previous tables. For instance, as far as the copyright protection legislations, one of the main difficulties for the Fit4MedRob initiative participants is to negotiate and transfer licences. It might be difficult for Fit4MedRob's participants to exercise a strong contractual power, and this might be detrimental, especially when their know-how is involved in the contract. Moreover, copyright is the IPR through which all software is protected. In principle, then, also AI programs and the databases on which AI systems (algorithms) are trained are protected by software protection. The extent of E&L to the copyright of proprietary AI system might be considerable also in terms of ownership of the final product, which might enrich a third party that is not part of the Fit4MedRob consortium (e.g. commercial chatbots which can be used as well to rapidly create license and transfer contracts). The issue of the connections between AI, and in particular generative AI, will be dealt with in detail in the next iterations.

As far as patents are concerned, they are an effective form of protection. Still, the main difficulty might be the length of the procedures to obtain this protection. At least, in the EU it is possible to apply for a European patent with a unitary effect. In this way, the legal expenses to get an invention patented and the time spent can be partially recovered by the width of the protection of the patent itself (that extends to all the parties which have adhered to the European Patent Convention). The patent protection is also conferred to the protection of the biotechnological inventions. Especially for the Mission 3 activities dealing with new materials and technologies, it is important to be aware of the ethical rationale of these EU legal acts. Not doing that could lead to the marketing of forbidden inventions.

[52] Ibidem.

In terms of industrial designs, the directives analysed do not have perceived obstacles, as they both grant a EU form of protection for these IPRs. The main obstacle could be that operators such as Fit4MedRob Initiative participants might not be aware of the existence of this form of IP legal protection.

6 Legal and Ethical compliance in Action

This second part of the deliverable will give a more precise overview concerning the development of the Survey from its design (4.1), its questions (4.2), the replies given (4.3) and a first attempt to create ad hoc services for the Fit4MedRob consortium (4.4).

6.1 The Survey Design

As already outlined in Section 2 (Methodology), Activity 4 decided that it was important to look for the input of the Fit4MedRob partners to check whether the mapping of the compliance requirements was exact but also to pave the way forward to deliverable D4.9.1. concerning the web-based platform for open acceleration and the services that the future (I)URAT centre of excellence will need to provide.

It was decided that an anonymous survey was the best way to let the different members of the Fit4MedRob consortium be free to express their ideas. However, both in the survey and in the e-mail introducing the survey, Activity 4 made it clear that it did not want survey participants to disclose important or sensitive information concerning their organisation.

That is why it was created a Microsoft forms survey which is accessible at this link

https://forms.office.com/e/038YSBxPNj.

The survey was circulated on Monday 9 October 2023 through the Fit4MedRob mailing list with a reminder on 13 October 2023 through the same channels. In the first email, the deadline to fill in the survey was 16th October 2023. In the reminder email, a new deadline was set for 20th October 2023. The text of both the emails can be found in Annex 1 (6.1.1, 6.1.2).

Activity 4 received in total 59 answers.

The text of questions is added as an Annex 2 (6.2) at the end of this deliverable. The complete series of visualisations starting from the replies to the survey is included in Annex 3 of this deliverable (6.3.).

6.2 The Survey Questions

There is a total of 19 questions divided into three main parts.

The first three questions aimed at identifying the educational background and the role within the Fit4MedRob consortium. The fourth question inquired what the participant's strategy was to answer an ethical question. They were all multiple-choice questions all of which were mandatory to reply but that allowed to select more options.

Questions from 5, 7, 9, 11, 13 and 15 instead aim at understanding what services the Fit4MedRob practitioners need. The questions were divided in themes: regulation of medical devices, intellectual property, data management, ethical compliance of research and product development, contract drafting and cybersecurity. These questions were structured as likert charts. For each of the issues connected to the main theme, the survey participant needed to express their opinion. The alternatives from which to choose from where the following:

1) Slightly important
2) Somewhat important
3) Highly important
4) Not Applicable

Questions 6, 8, 10, 12 and 14 instead are open questions that asked what services they considered important if they had not found a match in the previous question, for each of the themes previously mentioned (e.g. regulation of medical devices et cetera).

Questions 17 to 19 objective was to make the analysis more granular and let the Fit4MedRob participant express themselves and to understand

1) which activities would best serve the survey participant organization in terms of legal-ethical support
2) the most appropriate form to respond to the training needs (if present)
3) if, in the survey participants' opinion, their organization needs specific training in one or more of the topics presented earlier.

6.3 THE SURVEY REPLIES. A SYNTHESIS.

The survey's questions and complete answers are available in Annexes I, II and III but it can be useful to give a synthesis here and to comment on some of the open questions replies.

As far as the background, the majority of respondents were bioengineers (26 replies) and doctors (20)

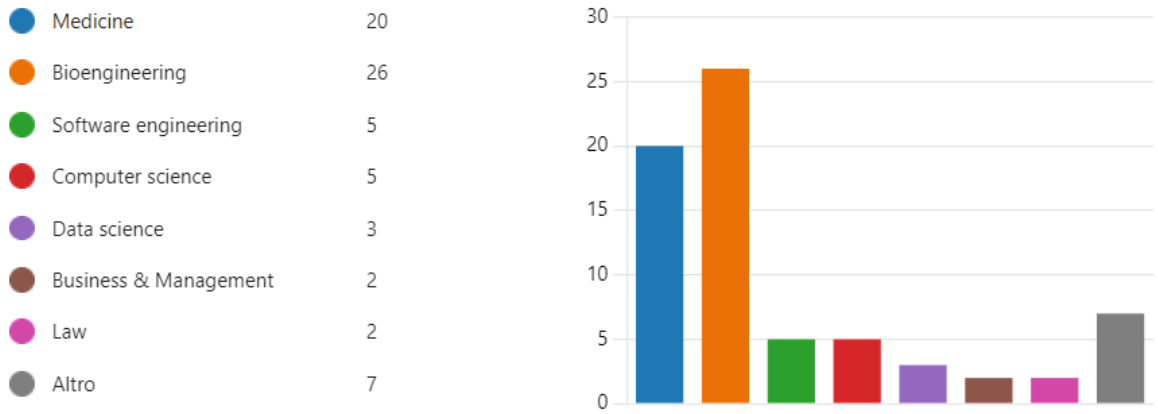


Fig. 1 Replies Question 1

Then, as far as the working place, it appears that 42% of the survey participants works for an academic institution. However, one must remember that in this case the replies were mandatory but there was freedom to choose multiple options. Therefore, it might not be surprising that some or all the people who chose 'academic institution' also selected 'public institution' and/or 'healthcare facility'.

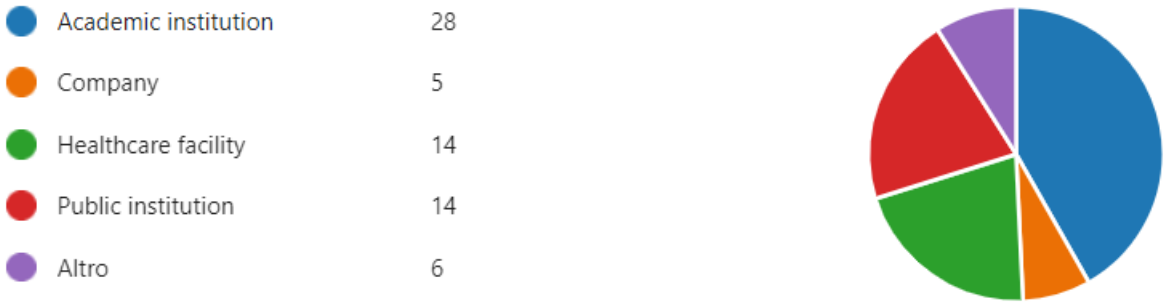


Fig.2 Replies Question 2

As far as the role within Fit4MedRob, 31 respondents chose theoretical and clinical research; this group is followed by people who have selected the option 'clinical practice' (21) and then data analysis (20) and data collection (19). It is also interesting to point out that there are also several people dealing with product development (13). The least represented categories concern ethical compliance (3), legal compliance (2) and administration (1).

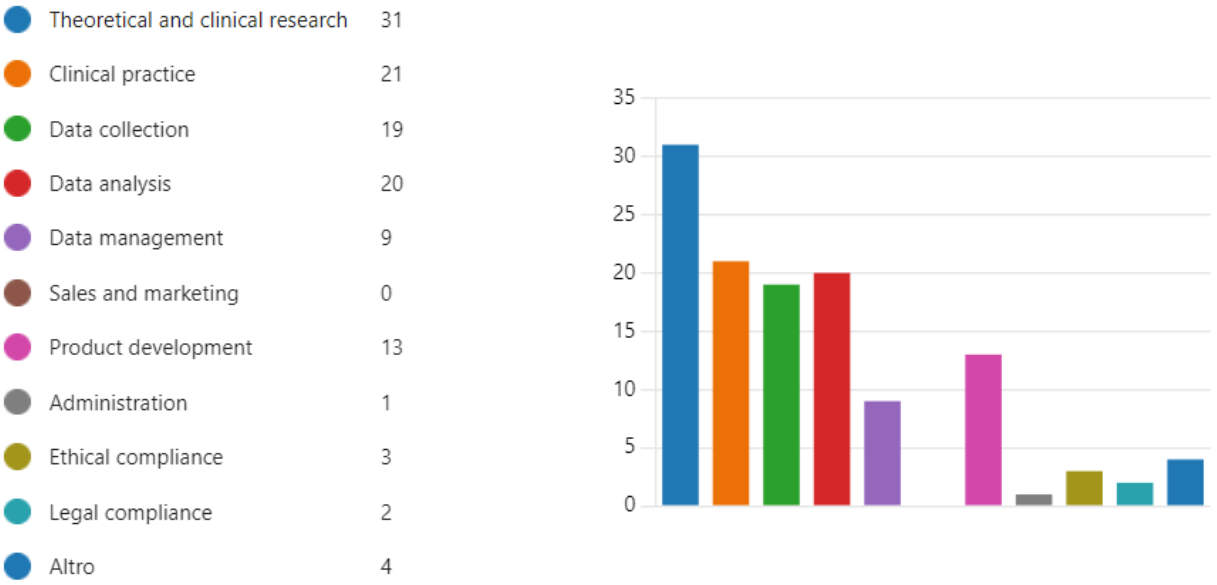


Fig. 3 Replies Question 3

It was also interesting to observe the trends concerning how to solve a legal or ethical question. 42 people responded that they would ask a legal-ethical expert(s) within their organisation, or the organisations' Data Protection office (30). A non-negligible group of respondents also selected the option 'you browse the internet (e.g. specialised forums)' (21 people). It is true that also in this case the reply was mandatory but there was the possibility to select more options. Hence it is possible that more strategies (e.g. Internet browsing and asking the DPO) might have been selected together.

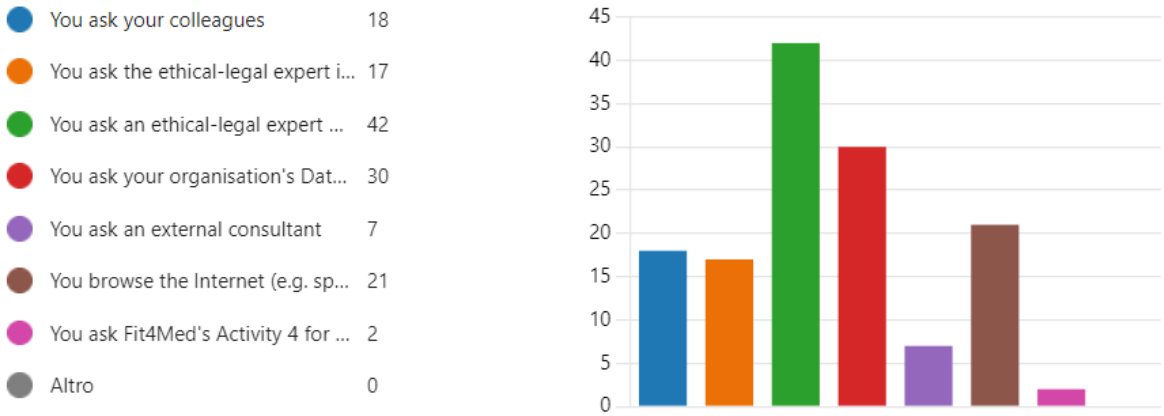


Fig. 4 Replies Question 4

The results of the group of questions which were structured as likert diagrams gave interesting results.

The first theme was medical devices regulation and the areas that were considered highly important were

1) Pre-trial research and clinical evaluation (72,9% of the respondents)
2) Device classification (45,8% of the respondents)
3) Product conformity and quality management (each 44,1% of the respondents)

Post market surveillance duties instead was not considered highly important (only 18,6% of respondents considered that as highly important) and yet, as showed in subsection 3.2.2. post market surveillance is one of the new features for the application of the MDR and it will be important to prepare for that set of requirements as well.

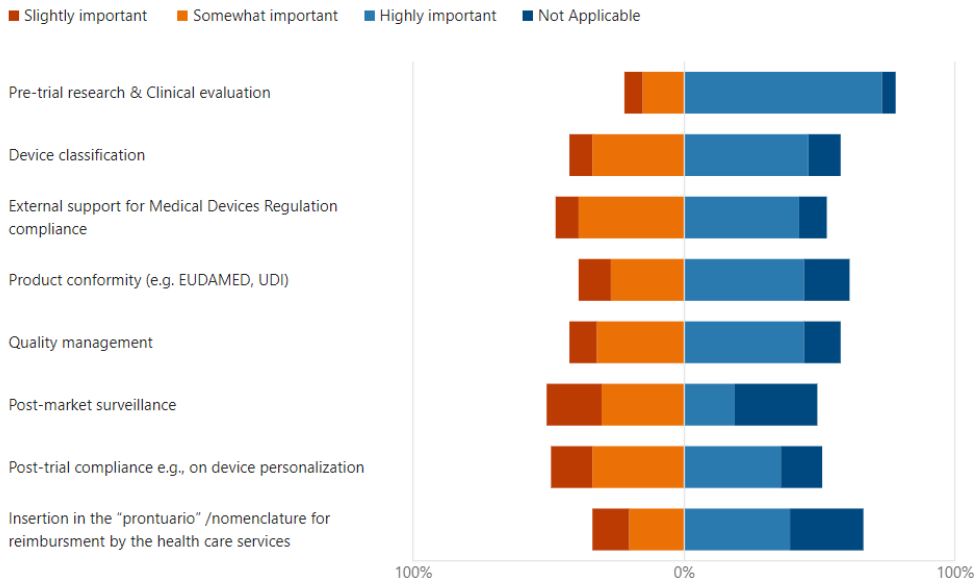


Figure 5 Replies to Question 5

Nobody replied to question 6, which intended to understand whether if none of the options fitted with the survey participant's situation to specify the services which could be considered as highly important. As far as intellectual property, the item that was considered most as highly important was licences (61%), followed closely by Non-Disclosure Agreements (NDAs) and patents and standards (57,6%).

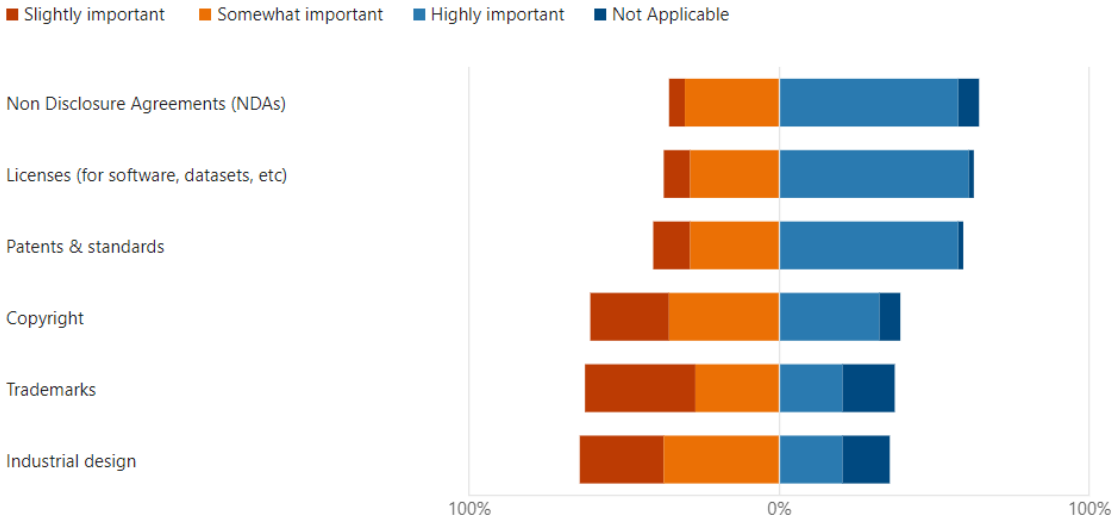


Fig.6 Replies to Question 7

Question 8 was the same of question 6 but applied to intellectual property. Unlike question 6, in this case there was just one answer. The only respondent asked to care more for and "Data protection agreement and IPR management."

Question 9 instead tried to understand which services were more suitable to participants in the field of data management. 62,7% of respondents considered the data management plan and compliance services highly important. Data sharing agreements are the second choice (59,3%) and standardized policies and processes are the third choice (55,9%) more than secondary use of data (50,8%). It will be important to focus on the fact that the DGA and the future DA and EDHS are instruments that can help innovators extract value from the data they have gathered from their devices to build innovative products and services maybe on secondary markets. It is also interesting to notice that the data management services that could be used to evaluate the possible market entrance of a product are considered not applicable to this scenario by at least 25,4% of the respondents.

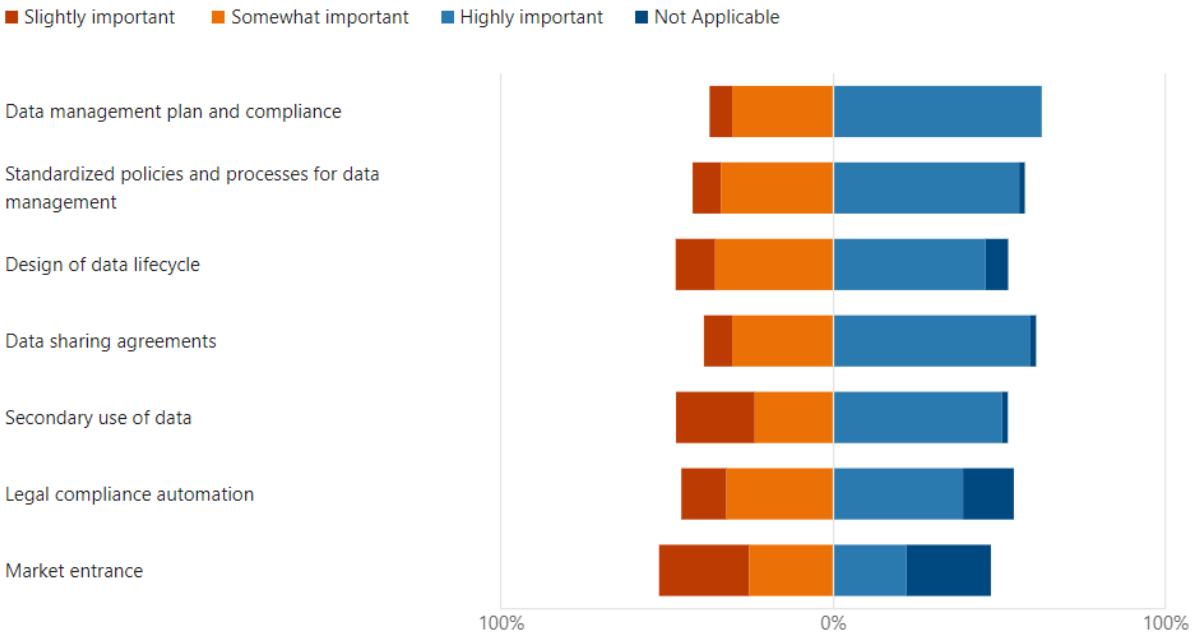


Fig. 7 Reply to Question 9

Also question 10 as well as number 6 did not have any reply.

Question 11 instead inquired on which services were more useful in the field of ethical compliance of research and product development. In this case, it was very clear what was considered highly important. In the first place, there are the services to have a correct application to submit for the ethical committee's authorization (86,4%); this item was closely followed by the issue of obtaining consent, especially from vulnerable groups (76,3%) and ethical risk assessment (74,6%) as a third choice. It is interesting to notice that the item about services concerning 'open science was considered 'somewhat important' with the highest percentage (39%), followed by the option concerning trustworthy AI self-evaluation (33.9%). It might be important to make the Fit4MedRob consortium partners that, especially in the near future, the trustworthy AI self-evaluation is going to become highly important in the near future because of the AI act enactment and its connection with liability rules as well as with the MDR and the MR.

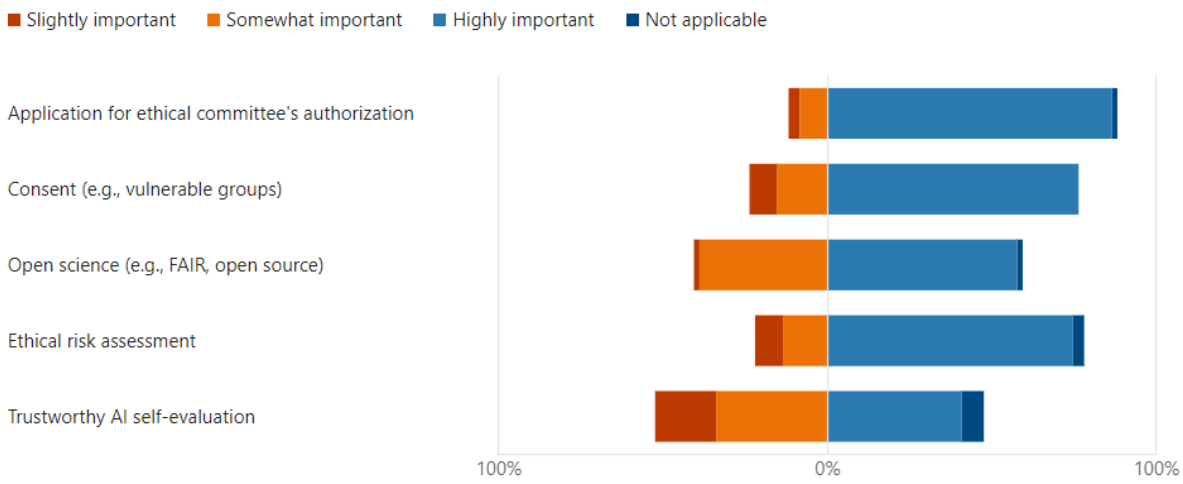


Fig. 8 Replies to Question 11

Question 12 like question 6 got no answers.

Question 13 concerned contract drafting. In this case the services concerning insurance or financial coverage things were considered highly important by most of the respondents (55,9%). What is interesting is thatconsultancy agreements were considered 'somewhat important' with the highest percentage (50,8%).

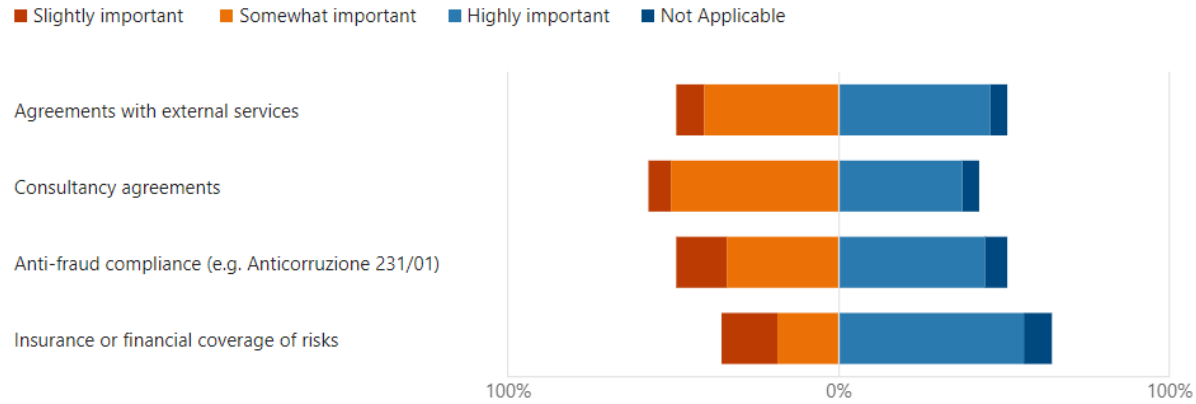


Fig. 9 Replies to Question 13

Question 14 inquired which contract-drafting-related services were considered important and, as question 8, got only one reply. This last reply specified that they did not know what their organization's views were on the topic.

Question 15 concluded the series with likert charts by asking preferences concerning the theme of cybersecurity. The distribution of the 'highly important' evaluation is quite homogeneous and high for most of the options presented:

1) Cyber-risk analysis (57,6%)
2) Data breach crisis management (55,9%)
3) (Cyber) security policy (54, 2%)
4) Conformity with cybersecurity certifications (52,5%)

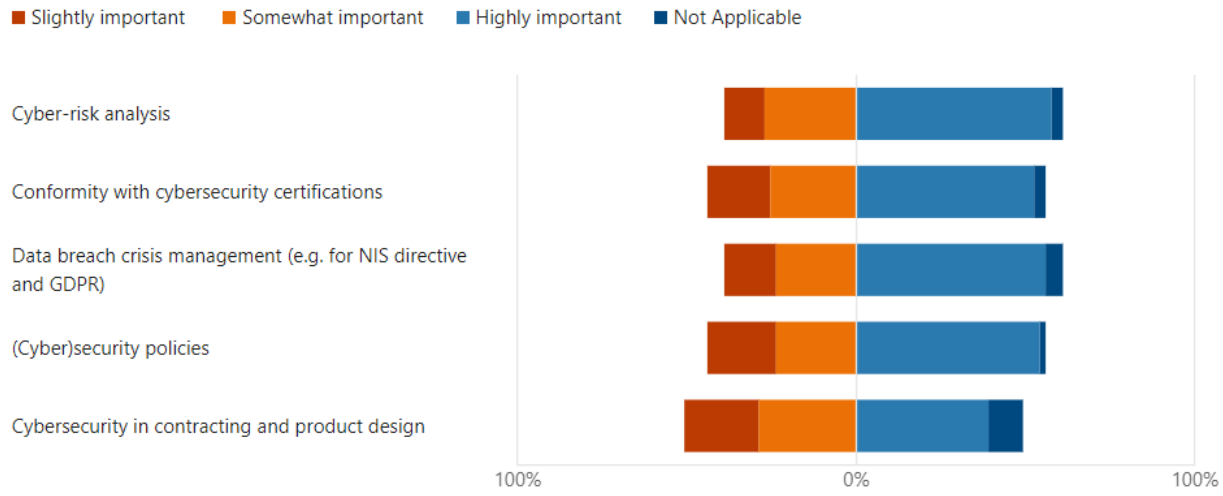


Fig. 10 Replies to Question 15

Question 16 which inquired if there were other services concerning cybersecurity that might have been left out was without reply too.

Question 17 was an open question asking what service would best serve the participant's organization to provide legal-ethical support. 40% of the respondents replied that a dedicated role in their company should fit their organization's need best.

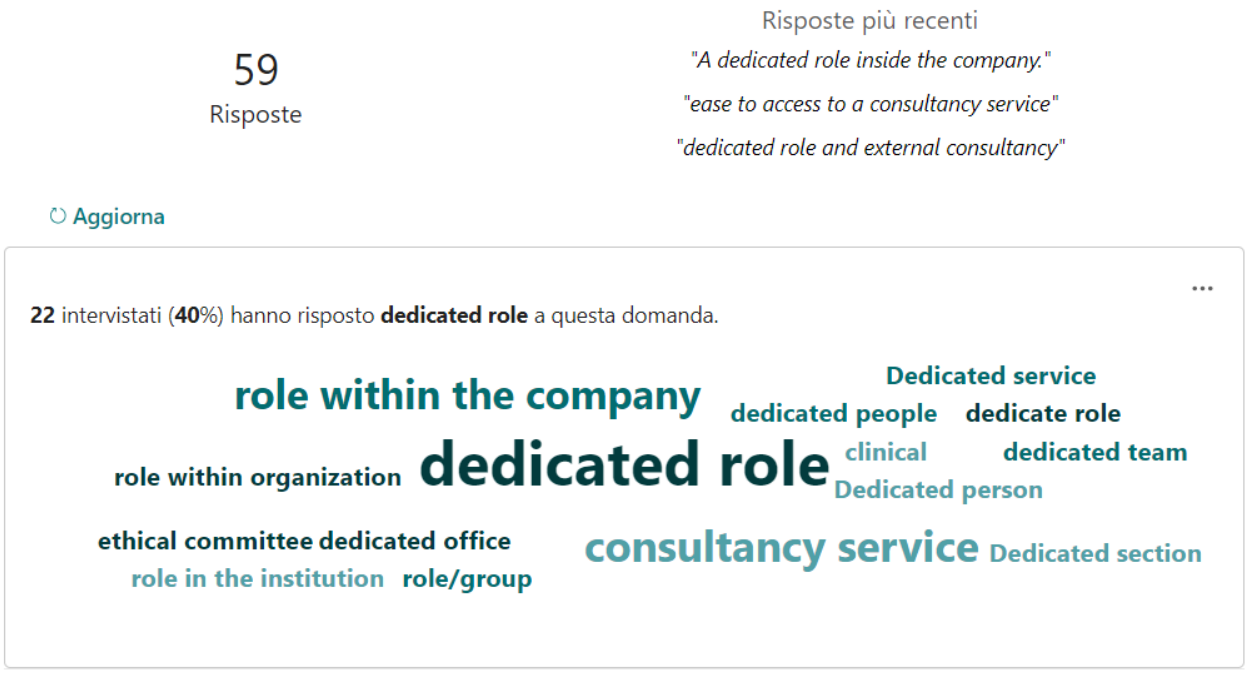


Figure 11 Replies to Question 17

Question 18 on the preferred options for the participants' training needs the replies were also interesting. The most popular options were seminars (40 respondents) and hands-on workshops (36 respondents). Both these choices could be carried out online or in person.

Fig. 12 Replies to Question 18

The last question was an open-ended question as well. It was asked whether respondents thought that their organization needed training on one or more of the topics previously mentioned. The word cloud visualization tool showed that 13% of the survey participants wrote clinical trials as a response but also cybersecurity, data, patents and ethical issues were considered important (9% each).

Fig.13 Replies to Question 19

6.4 From the Survey to the Services. A draft of plan for the future of Fit4MedRob consortium

This last table is an experiment on which the Fit4MedRob partners can give feedback. Section 3 revealed the main legal and ethical compliance requirements for whoever wants to build healthcare or personal care robots. Section 4 explains the origin of the survey both as a means to understand how much Fit4MedRob partners were aware about the said legal and compliance requirements, and as a means to check what Activity 4 might have been postponing in terms of legal and ethical mapping and analysis. The survey also offered an opportunity to already start the work concerning deliverable D4.9.1. concerning the creation of an Open Web Acceleration platform, which in itself will become a structured system within the (I)URAT centre of excellence. The survey replies gave Activity 4 ideas already in terms of the services that could be needed in the medium and long term to Fit4MedRob partners and that are succinctly explained in table 6 below.

Table 6 Future services for Fit4MedRob

Area of expertise	Service(s) suggested	Brief description
Safety legislation: Medical Safety laws	Pre-trial research & Clinical evaluation Device classification External MDR responsible person Product confromity (e.g. EUDAMED UDI certification) Approval from Notified body:help with documents and compliance Quality management system establishment Post-market surveillance Post-trial e.g., on service personalization	The MDR is the legislation that has prompted quite a lot of interest in the survey that is why it is treated as the first one. The services that could be developed by the Open Web Platform Acceleration in the following years and iterations is the possibility to streamline and make it apparent the services listed (in forms of checklist and other forms of easy-to-do compliance forms). Moreover, give the future centre of excellence URAT could help provide tailored care for the specific needs of researchers and provide MDR continuous compliance services as requested by Article 15 MDR
AI Regulation and Ethics will translate into Research and product development ethical compliance	Preparing and manage application to the ethics committees Legal design of consent experience for specific groups (e.g., vulnerable populations, etc) or settings (e.g., internet research) Codes of conduct Open science training Ethics assessment Risk assessment Fundamental rights impact assessment Product\service reimbursement from Health care systems	This part of ethical regulation is partly connected also with the discipline of the clinical trials, both for medical devices and for medicines in general. Ethical committee procedures prompted quite a lot of reactions in the comments also because the discipline has been deeply reformed recently and is in a transitional application phase. However, given the more and more widespread use of AI systems it is important to integrate the traditional ethics requirements with the ones which are more tailored with the AI development
Liability laws which will translate mainly into contract drafting at the moment.	External services agreements Consultancy agreements Anti-fraud d. lgs 231/01 compliance ICT contracting	There can be support in the drafting of these kinds of contracts Concerning other kinds of liability such as product and extra-contractual one with reference to new technologies (AILP and PLDU) things are more complex as far as coordination with other thematic law areas is concerned. Product liability issues, despite their importance, need more time for implementation as they need also to be put into relation with insurance issues and harmonized with the upcoming discipline on the Levels of Essential Assistance which are not yet fully clear and drafted at this moment in time.

Data laws. In this case we need to divide the services provided in *Data management* (concerning both personal and non-personal data)	Data management plan and compliance Information policies Data Protection Impact Assessments for personal data treatments (if needed) Standardized policies and processes for data management (whole cycle) Data sharing agreements Secondary uses design Legal compliance automation	It is necessary to plan the resources and set out the policies that are needed for the management of research data within a research group/project / consortium / etc. And to draft, update and routinely revise the data management.
And *Data Flow design* (which also includes management for the whole data life cycle	Oversee whether behaviours and decisions are in line with the established data management policies (DA, DGA, GDPR, EDHA) and plan courses of actions to correct deviations and to find solutions to obstacles. Support with data sharing and data processing agreements for private businesses. Support providers of secure processing environments for health data. Analysis of existing or developing information systems and consultancy or co-development service (with help from software engineers).	The Data Flow design is not as focussed on compliance as data management as it is also directed on how to improve a product or service and will help researchers figure in advance what obstacles (legal or ethical) their research might encounter and develop strategies to solve them.
Intellectual property	NDAs Licenses Patents & standards Copyright Trademarks Industrial design	It is true that in Section 3 there was not time to map down the several relevant IP EU and Italian legislative acts. However, from the survey, it was apparent that all these issues connected to legal compliance do have considerable weight for the everyday work of the Fit4MedRob consortium. That is why support with the previous cell themes could be also the start for a more intelligent IP mapping and the starting point to create more tailored IP services.
Cybersecurity	Risk analysis Compliance with existing certification Data breach crisis management (e.g. for NIS directive and GDPR) Security policies Cybersecurity relevance in contracting and in product design	The Cybersecurity Act, the Cyber-resilience Act and the NIS II directive requirements and their application will be dealt with in depth in the next iteration of this deliverable

7 PRELIMINARY CONCLUSIONS

The deliverable's focus was more theoretical this year. Not only did it expand into two brand new sections, Cybersecurity (section 4) and Intellectual Property (section 5), but it updated all the legal acts that were dealt with already in D4.8.1, from data protection to the new AI act. This iteration's preliminary conclusions are focussed on the IP and cybersecurity aspects of the update, as well as on the most important updates of the legal acts already dealt with in D4.8.1 and that were voted into law or modified or implemented during this year.

In the cybersecurity section, several legislations are relevant to the stakeholders of the Fit4MedRob consortium. For instance, the NIS 2 concerns, among other things, the national cybersecurity strategy on which the Fit4MedRob participants need to be informed. Then, the CRA proposal lays out general cyber security and duty requirements for all interconnected objects, medical devices excepted. In the intellectual property section instead, as it was a larger field to cover, there was a specific subdivision into several subsections, and each of them focussed on a particular IPR which is relevant to the construction of rehabilitation robots and allied technologies. Overall, the EU harmonization of IPRs is still ongoing and has received a boost as a complementary regulation to the digital policy. This is because IPR regulation is an essential enabler for new technologies which will be applied to both personal care and health-care robots to protect the creativity of the creations and the competitiveness of the inventions in the EU. One of the main difficulties, especially for copyright protection, is for Fit4MedRob's initiative partners to be counselled correctly especially when they need to negotiate and transfer of licences contracts. Moreover, an emerging field of contrast is the interaction of AI instruments, in particular generative AI ones, with the rightful copyright protection of the Fit4MedRob initiative's discoveries and research results. The issues underlying this aspect will be dealt with in the following iterations.

As far as the part concerning the update of the already mentioned legislations, there has been approval into laws of official EU proposals, and modifications to already applicable implementing laws. Here will follow a synthetic list mentioning the most important legal changes happened in a year and what they mean for the Fit4MedRob initiative.

- The AI Act. It is a comprehensive regulation which deals with all the possible applications of the AI technology. It is especially important for software that works with medical devices or as a medical device on its own (Software as Medical Device) but not only. It is important to remember that the AI act introduces principles that need to be considered since the design of the algorithm (or, better, AI system) and that introduces a logic of product safety and quality management especially for the AI systems that are considered high-risk at Article 6 of this regulation (and AI systems working in or as medical devices are comprised in this list); moreover, it will be important for Fit4MedRob initiative's partners to get acquainted with Article 5's prohibited AI practices. The compliance rules that will be most important for the Fit4MedRob's initiative's partners will be dealt with in the next iterations of the deliverable and in the iterations of D4.9.1. Web Based Platform for Open Acceleration (WBPOA)
- The revised rules on secondary use of personal data in the Italian Code of Privacy. The revision of Articles 110 and 110bis have in part facilitated the secondary use of data and have made it easier for IRCCS institutions. This is helpful and will prepare for the enactment of the new regulation called EHDS (European Health Data Space) which will establish rules to access not only personal health data, but also other kinds of data which are connected to health but might come from wellness devices.
- The revised rules on the Product Liability Directive Update. The most important change compared to the old regime is that software (included AI) if defective is considered a product. Hence, the claimant must prove the defectiveness of the product, the damage and the causal link. The manufacturer is the main contact person to which the liability claim is addressed but other economic operators might be involved if the manufacturer is not known or is located outside of the EU. It is important to highlight that this directive introduces presumptions concerning the defective and/or the causal link which might be considered by the judge if there are too many technical difficulties for the complainant to prove these two elements. It must be remembered that these presumptions are always rebuttable by the manufacturer.

The mapping action is now complete and the next phase concerning compliance rules will be implemented in the two next iterations and concretised through the creation of the implementation of the WBPOA in the D4.9.1 and D4.9.2.

The deliverable's two-fold structure allowed to reach some interesting preliminary conclusions. Section 3 in particular made it possible to focus on the current legal and ethical compliance problems and open issues for researchers and innovators for each of the legal acts commented. What appears is that although the Medical Safety laws are approved, they need to be implemented. Moreover, although they are not so old, Medical Safety Laws do not consider all the issues concerning the EU digital policy and, most notably, the AI Act proposal and the Data laws, meaning all the regulations concerning data ranging from the GDPR to the DA, from the EDHS to the DGA. Moreover, new regulations which concern the general safety of products have just been voted into law such as the GSPR and the MR. It will be necessary to understand how their compliance will adapt to the requirements of the data laws and the AI Act. Further, two new proposals have appeared as far as civil and product liability (AILP and the PLDU) which will need to interact with the contractual liability directives (SG and DCDS). The first two proposals need to be voted into law, but they are likely to influence the civil procedural laws of the EU member states as well.

The second part of the deliverable coincides with section 4 which explains the origin and the development of the survey on ethical and legal compliance (4.1), its questions and their purpose (4.2) and the replies received (4.3). After the survey results, Activity 4 decided to sketch a draft of the services that will be developed through the next deliverable, D4.9.1 which will lay the foundation for the creation of an Open Web Platform Acceleration which will then become part of the instruments developed by the future center of excellence (I)URAT, created thanks to Fit4MedRob funds.

The conclusions can be summed up as follows: the survey showed some preferred areas of interest concerning legal and ethical compliance themes that were mostly also mapped down in the first part of the deliverable, especially issues related to compliance with the MDR and CTR issues. Other topics, such as the issues concerning the secondary use of data to extract value from it were not felt as important as they are not yet recurring issues in the everyday work of the Fit4MedRob partners. However, these overlooked topics are essential for the development of new healthcare and personal care robots. Knowing more about how to harvest value from data in compliance with new and future data regulations will enable researchers and innovators to really change the paradigms of contemporary robotics and allied technologies as they will be compliant by design. Consequently, the survey outlined a need to train and inform the Fit4MedRob partners on the upcoming changes that will especially invest the area called Data Laws and the one concerning AI. There is also the willingness of Fit4MedRob partners to have seminars and hands-on workshops on the themes they need to be acquainted with, both the most pressing and the least pressing. Data Laws and AI regulation as thematic areas will be extremely important as they will interact with one another and one of the tasks of the next iterations of this deliverable and of the D4.9 ones will be to highlight a precise order on how to carry out different kinds of compliance for the same device and make it understandable for Fit4MedRob partners who do not have a law background.

The results of this first survey are promising as they showed that Fit4MedRob partners care about creating a new generation of personal and healthcare robots that are legally and ethically compliant. However, Fit4MedRob partners who are not lawyers might focus only on a few legal elements they know and do not keep updated with other relevant innovations in the field. That is why Activity 4's work is precious also in terms of continuous education through workshops and seminars and, in general, as a reference for the legal and ethical compliance of the whole consortium. Through the future dissemination within the consortium of these results, there are chances to make other activities and missions' research legally and ethically compliant. This would also be one of the expected targets of the Fit4MedRob mission, which is to build the next generation of medical robots and allied technologies.

8 ANNEXES

8.1 ANNEX 1: CONTENT OF THE EMAILS SENT

As anticipated in section 4, there were0 two emails being sent. The first one was sent on the 9th October 2023 and the second one as a reminder on 13th October 2023. Their texts will be displayed in the following subsections.

8.1.1 9th October e-mail addressed to the Fit4MedRob consortium

survey anonima per D4.8.1 dell' Activity 4

Francesca Gennari <Francesca.Gennari@santannapisa.it>
Mon 09/10/2023 10:57

To:fit4medrob-mission1@googlegroups.com <fit4medrob-mission1@googlegroups.com>;fit4medrob-mission2@googlegroups.com <fit4medrob-mission2@googlegroups.com>;fit4medrob-mission3@googlegroups.com <fit4medrob-mission3@googlegroups.com>

Gentili membri del consorzio Fit4MedRob,

Il team dell'Activity 4 avrebbe bisogno di una decina di minuti del vostro tempo per aiutarci a comprendere le **questioni etico-legali** che incontrate nelle vostre attività, ad esempio sull'uso dei dati, la conformità dei prodotti, la gestione della proprietà intellettuale, eccetera.

Abbiamo preparato un questionario le cui risposte sono **anonime proprio perché ci serve avere la vostra valutazione oggettiva e libera da qualsiasi vincolo (si prega di non condividere però informazioni riservate).** Le vostre **risposte** e i **vostri suggerimenti** ci sono necessari per elaborare dei servizi, degli strumenti e delle eventuali attività di **training** che vi forniscano il supporto necessario.

https://forms.office.com/e/038YSBxPNj

Sarebbe importante che persone con ruoli diversi all'interno di ogni organizzazione rispondessero: quindi **invitiamo tutti a partecipare anche più persone per ciascuna organizzazione e con ruoli diversi!** Presenteremo i risultati in modo aggregato nel Deliverable "D4.8.1 Report on ethical and legal compliance of healthcare and personal healthcare robots #1 "

Vi chiediamo di compilare il questionario entro il prossimo **16 ottobre 2023**

Resto a disposizione per eventuali dubbi o chiarimenti

Francesca Gennari

per conto del coordinatore Prof Giovanni Comandé (LIDER Lab, Scuola Superiore Sant'Anna)

8.1.2 13th October e-mail addressed to the Fit4MedRob consortium

survey anonima per D4.8.1 dell' Activity 4 - Reminder

fit4medrob-activity3-4@googlegroups.com <fit4medrob-activity3-4@googlegroups.com>
on behalf of
Francesca Gennari <Francesca.Gennari@santannapisa.it>
Fri 13/10/2023 15:56

To:fit4medrob-activity1-2@googlegroups.com <fit4medrob-activity1-2@googlegroups.com>;fit4medrob-activity5@googlegroups.com <fit4medrob-activity5@googlegroups.com>;fit4medrob-activity3-4@googlegroups.com <fit4medrob-activity3-4@googlegroups.com>;fit4medrob-activity6@googlegroups.com <fit4medrob-activity6@googlegroups.com>;fit4medrob-activity7@googlegroups.com <fit4medrob-activity7@googlegroups.com>; fit4medrob-activity8-9@googlegroups.com <fit4medrob-activity8-9@googlegroups.com>;fit4medrob-activity10@googlegroups.com <fit4medrob-activity10@googlegroups.com>
Cc:fit4medrob-mission1@googlegroups.com <fit4medrob-mission1@googlegroups.com>;fit4medrob-mission2@googlegroups.com <fit4medrob-mission2@googlegroups.com>;fit4medrob-mission3@googlegroups.com <fit4medrob-mission3@googlegroups.com>;fit4medrob-sc@googlegroups.com <fit4medrob-sc@googlegroups.com>

Gentili membri del consorzio Fit4MedRob,

Il team dell'Activity 4 avrebbe bisogno di una decina di minuti del vostro tempo per aiutarci a comprendere le **questioni etico-legali** che incontrate nelle vostre attività, ad esempio sull'uso dei dati, la conformità dei prodotti, la gestione della proprietà intellettuale, eccetera.

Abbiamo preparato un questionario le cui risposte sono **anonime proprio perché ci serve avere la vostra valutazione oggettiva e libera da qualsiasi vincolo (si prega di non condividere però informazioni riservate).** Le vostre **risposte** e i **vostri suggerimenti** ci sono necessari per elaborare dei servizi, degli strumenti e delle eventuali attività di **training** che vi forniscano il supporto necessario.

https://forms.office.com/e/038YSBxPNj

Sarebbe importante che persone con ruoli diversi all'interno di ogni organizzazione rispondessero: quindi **invitiamo tutti a partecipare anche più persone per ciascuna organizzazione e con ruoli diversi**! Presenteremo i risultati in modo aggregato nel Deliverable "D4.8.1 Report on ethical and legal compliance of healthcare and personal healthcare robots #1 "

Vi chiediamo di compilare il questionario entro il prossimo **20 ottobre 2023**

Resto a disposizione per eventuali dubbi o chiarimenti

Francesca Gennari

per conto del coordinatore Prof Giovanni Comandé (LIDER Lab, Scuola Superiore Sant'Anna)

8.2 Annex 2: The Survey Questions

Here follows the complete list of questions that the participants needed to answer. Please apologise for the jpeg format of the following pages. The transformation from the original pdf to a word document risked making the template for this deliverable not usable. Hence this shortcut was preferred.

Fit4MedRob
Survey on ethical and legal compliance

Responsabile Prof. Giovanni Comandé
Grant. n. PNC0000007

* Obbligatoria

Objectives of the survey

We would like to better understand your needs and plan our legal-ethical activities accordingly, such as the provision of services, tools and trainings.
Please answer the following questions carefully. Your answers will be anonymous: do not share any confidential information.

Who are you?

1. What is your educational background? You can choose more than one option. *

- [ ] Medicine
- [ ] Bioengineering
- [ ] Software engineering
- [ ] Computer science
- [ ] Data science
- [ ] Business & Management
- [ ] Law
- [ ] Altro

2. Where do you work? You can choose more than one option. *

- [ ] Academic institution
- [ ] Company
- [ ] Healthcare facility
- [ ] Public institution
- [ ] Altro

3. What is your role within the Fit4MedRob project ? You can choose more than one option. *

- [ ] Theoretical and clinical research
- [ ] Clinical practice
- [ ] Data collection
- [ ] Data analysis
- [ ] Data management
- [ ] Sales and marketing
- [ ] Product development
- [ ] Administration
- [ ] Ethical compliance
- [ ] Legal compliance
- [ ] Altro

5. Regulation of medical devices - Please rank the importance of the following services for your organization *

	Slightly important	Somewhat important	Highly important	Not Applicable
Pre-trial research & Clinical evaluation	○	○	○	○
Device classification	○	○	○	○
External support for Medical Devices Regulation compliance	○	○	○	○
Product conformity (e.g. EUDAMED, UDI)	○	○	○	○
Quality management	○	○	○	○
Post-market surveillance	○	○	○	○
Post-trial compliance e.g., on device personalization	○	○	○	○
Insertion in the "prontuario" /nomenclature for reimbursment by the health care services	○	○	○	○

6. If none of the previous options fits with your situation, specify the services you consider highly important.

7. Intellectual property - Please rank the importance of the following services for your organization *

	Slightly important	Somewhat important	Highly important	Not Applicable
Non Disclosure Agreements (NDAs)	○	○	○	○
Licenses (for software, datasets, etc)	○	○	○	○
Patents & standards	○	○	○	○
Copyright	○	○	○	○
Trademarks	○	○	○	○
Industrial design	○	○	○	○

8. If none of the previous options fits with your situation, specify the services you consider highly important.

9. Data management - Please rank the importance of the following services for your organization *

	Slightly important	Somewhat important	Highly important	Not Applicable
Data management plan and compliance	○	○	○	○
Standardized policies and processes for data management	○	○	○	○
Design of data lifecycle	○	○	○	○
Data sharing agreements	○	○	○	○
Secondary use of data	○	○	○	○
Legal compliance automation	○	○	○	○
Market entrance	○	○	○	○

10. If none of the previous options fits with your situation, specify the services you consider highly important.

11. Ethical compliance of research and product development - Please rank the importance of the following services for your organization *

	Slightly important	Somewhat important	Highly important	Not applicable
Application for ethical committee's authorization	○	○	○	○
Consent (e.g., vulnerable groups)	○	○	○	○
Open science (e.g., FAIR, open source)	○	○	○	○
Ethical risk assessment	○	○	○	○
Trustworthy AI self-evaluation	○	○	○	○

12. If none of the previous options fits with your situation, specify the services you consider highly important.

13. Contract drafting and other - Please rank the importance of the following services for your organization *

	Slightly important	Somewhat important	Highly important	Not Applicable
Agreements with external services	○	○	○	○
Consultancy agreements	○	○	○	○
Anti-fraud compliance (e.g. Anticorruzione 231/01)	○	○	○	○
Insurance or financial coverage of risks	○	○	○	○

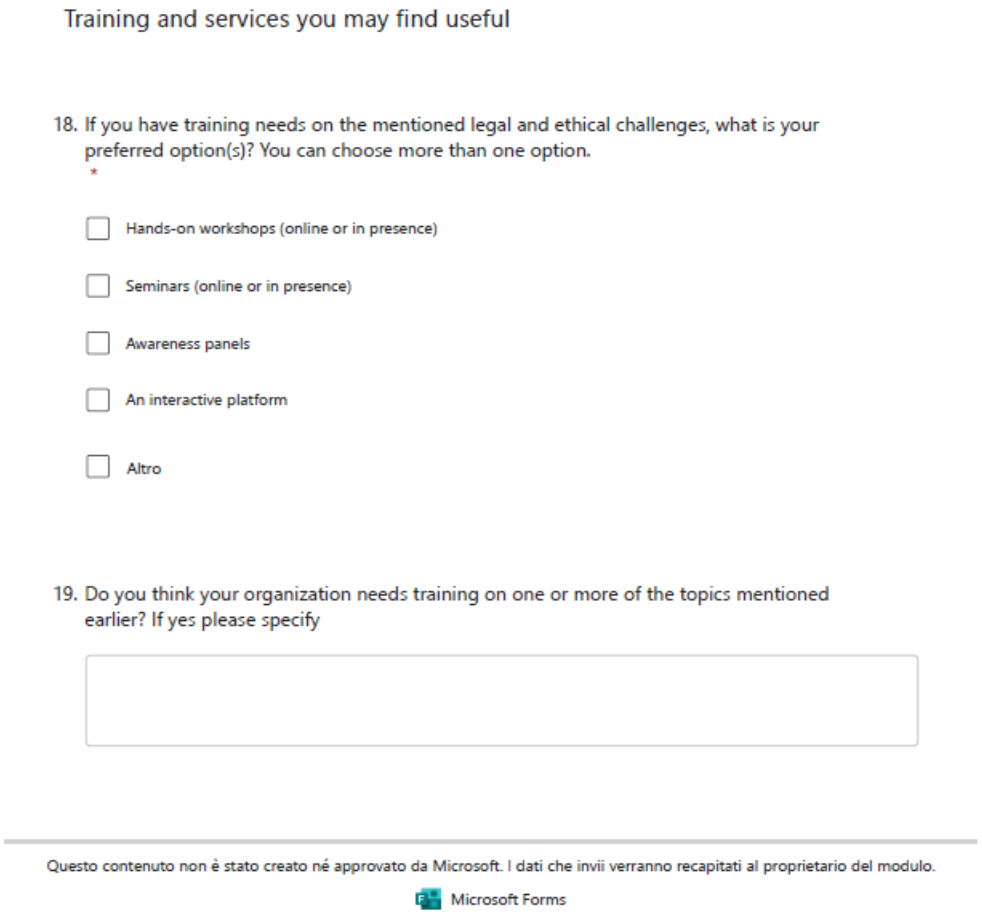
14. If none of the previous options fits with your situation, specify the services you consider highly important.

15. Cybersecurity - Please rank the importance of the following services for your organization *

	Slightly important	Somewhat important	Highly important	Not Applicable
Cyber-risk analysis	○	○	○	○
Conformity with cybersecurity certifications	○	○	○	○
Data breach crisis management (e.g. for NIS directive and GDPR)	○	○	○	○
(Cyber)security policies	○	○	○	○
Cybersecurity in contracting and product design	○	○	○	○

16. If none of the previous options fits with your situation, specify the services you consider highly important.

17. To provide legal-ethical support in your activities, what would best serve your organization (e.g., a dedicated role within the company, consultancy services, law firm...)? *



Training and services you may find useful

18. If you have training needs on the mentioned legal and ethical challenges, what is your preferred option(s)? You can choose more than one option.
*

- [ ] Hands-on workshops (online or in presence)
- [ ] Seminars (online or in presence)
- [ ] Awareness panels
- [ ] An interactive platform
- [ ] Altro

19. Do you think your organization needs training on one or more of the topics mentioned earlier? If yes please specify

Questo contenuto non è stato creato né approvato da Microsoft. I dati che invii verranno recapitati al proprietario del modulo.

Microsoft Forms

8.3 ANNEX 3: THE SURVEY REPLIES

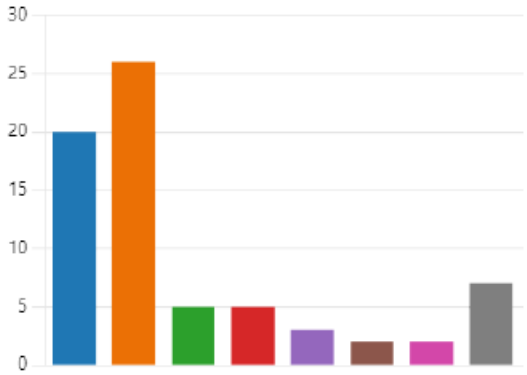
Here follows the complete list of visualizations taken from the survey replies. As well as in Annex II, transforming the original pdf document in a word one was creating problems with the deliverable template. Hence it was preferred to use the jpeg format.

Fit4MedRob Survey on ethical and legal compliance

59	09.27	Attivo
Risposte	Tempo medio per il completamento	Stato

1. What is your educational background? You can choose more than one option.

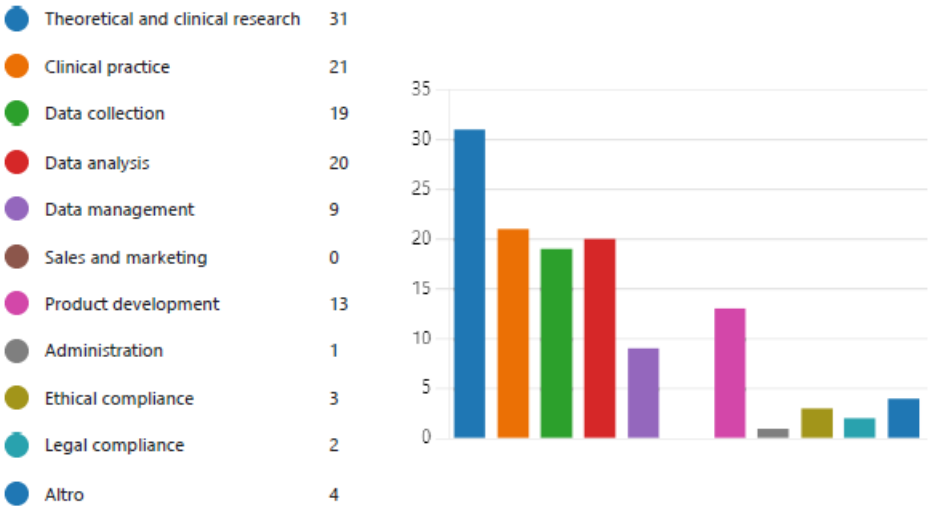
Medicine	20
Bioengineering	26
Software engineering	5
Computer science	5
Data science	3
Business & Management	2
Law	2
Altro	7



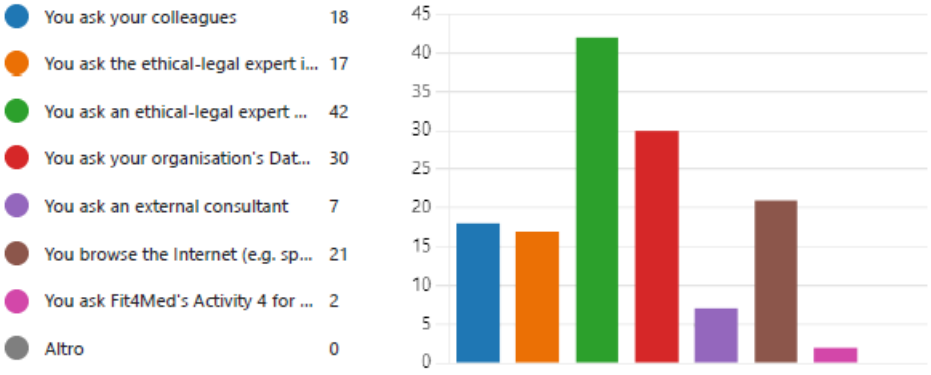
2. Where do you work? You can choose more than one option.

Academic institution	28
Company	5
Healthcare facility	14
Public institution	14
Altro	6

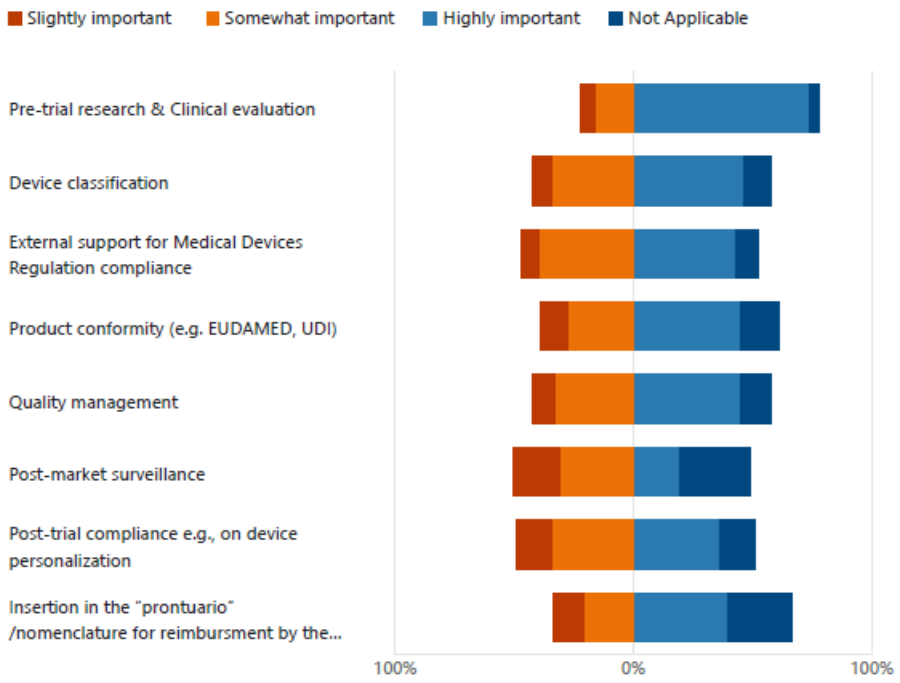
3. What is your role within the Fit4MedRob project ? You can choose more than one option.



4. When you have a legal or ethical question, what do you usually do? You can choose more than one option.



5. Regulation of medical devices - Please rank the importance of the following services for your organization

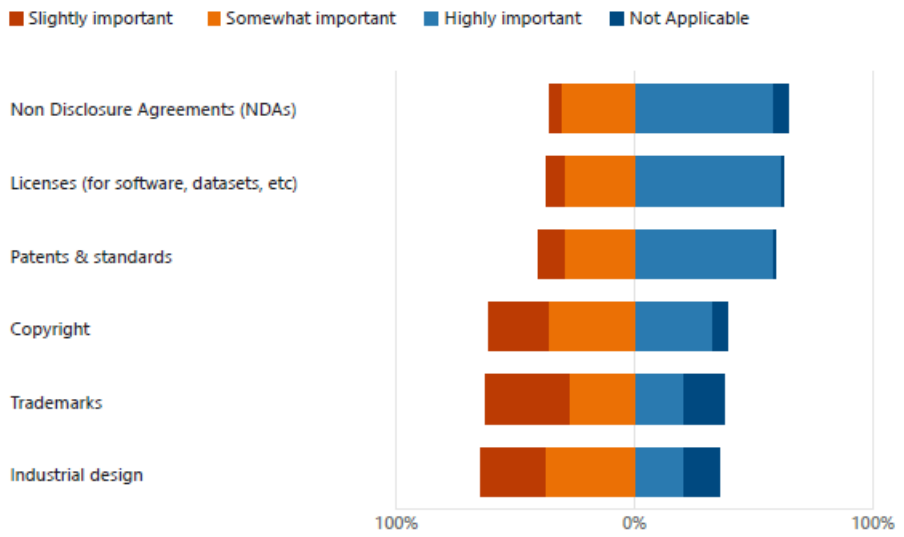


6. If none of the previous options fits with your situation, specify the services you consider highly important.

0
Risposte

Risposte più recenti

7. Intellectual property - Please rank the importance of the following services for your organization

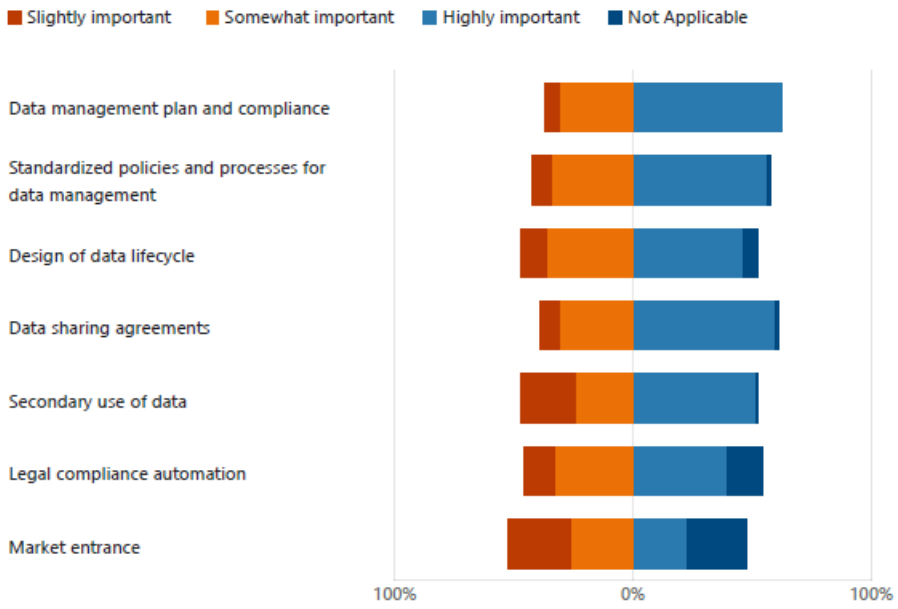


8. If none of the previous options fits with your situation, specify the services you consider highly important.

1
Risposte

Risposte più recenti

9. Data management - Please rank the importance of the following services for your organization

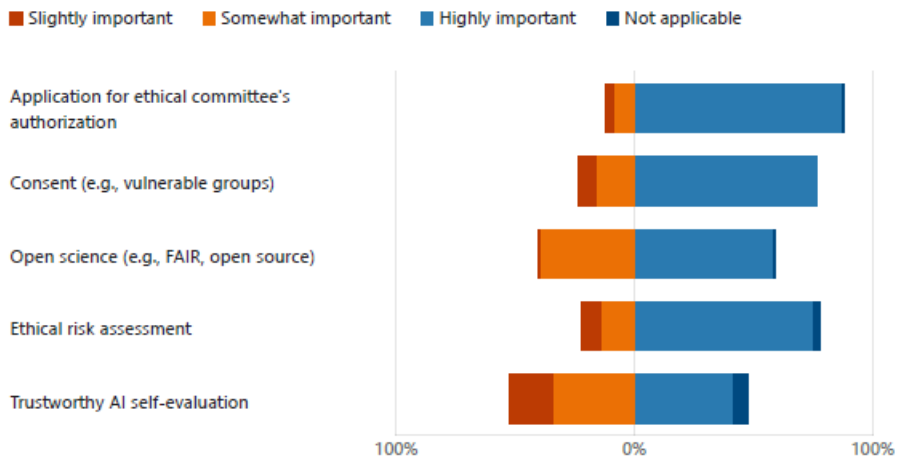


10. If none of the previous options fits with your situation, specify the services you consider highly important.

0
Risposte

Risposte più recenti

11. Ethical compliance of research and product development - Please rank the importance of the following services for your organization

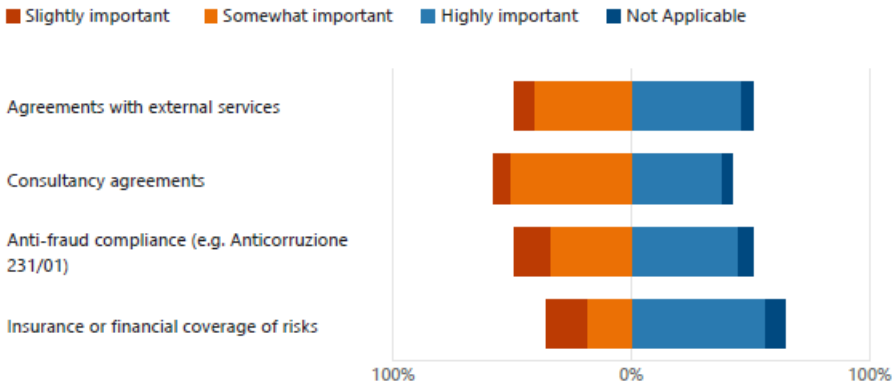


12. If none of the previous options fits with your situation, specify the services you consider highly important.

0
Risposte

Risposte più recenti

13. Contract drafting and other - Please rank the importance of the following services for your organization

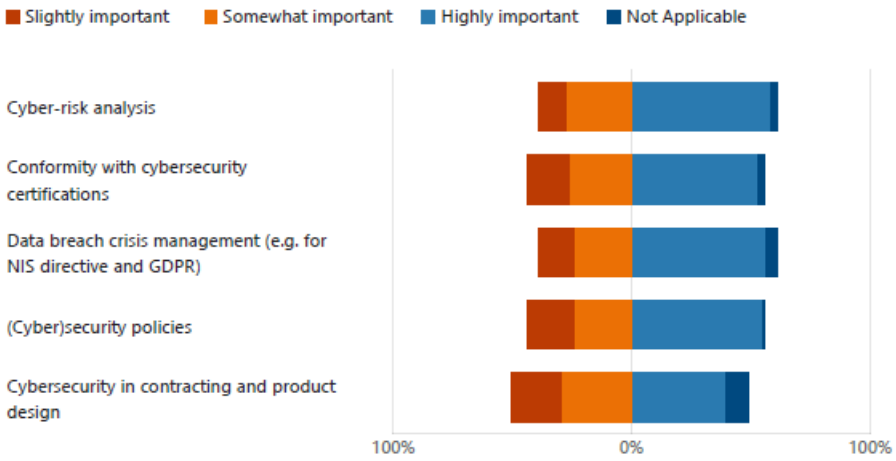


14. If none of the previous options fits with your situation, specify the services you consider highly important.

1
Risposte

Risposte più recenti

15. Cybersecurity - Please rank the importance of the following services for your organization



16. If none of the previous options fits with your situation, specify the services you consider highly important.

0
Risposte

Risposte più recenti

17. To provide legal-ethical support in your activities, what would best serve your organization (e.g., a dedicated role within the company, consultancy services, law firm...)?

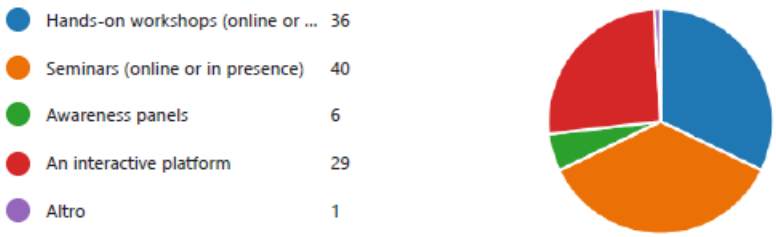
59
Risposte

Risposte più recenti
"A dedicated role inside the company."
"ease to access to a consultancy service"
"dedicated role and external consultancy"

Aggiorna

22 intervistati (**40**%) hanno risposto **dedicated role** a questa domanda.

18. If you have training needs on the mentioned legal and ethical challenges, what is your preferred option(s)? You can choose more than one option.



19. Do you think your organization needs training on one or more of the topics mentioned earlier? If yes please specify

25
Risposte

Risposte più recenti
"yes, a continous training is always important"

Aggiorna

List of Abbreviations

ML	Mission Leader
AL	Activity Leader
SC	Scientific Committee
BoD	Board of Directors
GA	General Assembly
CoE	Centre of Excellence
CCB	Cascade Calls Board
AI	Artificial Intelligence
CTR	Clinical Trials Regulation
DA	Data Act
DGA	Data Governance Act
EHDS	European Health Data Space
GDPR	General Data Protection Regulation
GSPD	General Safety of Products Directive
GSPR	General Safety of Products Regulation
MD	Machinery Directive /Medical Device
MDR	Medical Devices Regulation
MR	Machinery Regulation
MS	Member State
AIA	AI act
OES	Operators of Essential Services

DSP	Digital Services Providers
CSIRT	Computer Security Incident Response Team
EE	Essential Entities
IE	Important Entities
PLDU	Product Liability Directive Update
AILD	AI non contractual Liability Directive
IPR	Intellectual Proprerty rights
E&L	Exceptions and limitations
LPBI	Legal Protection of Biotechnological Inventions
SEP	Standard Essential Patents
UPP	Unitary Patent Protection

REFERENCES

[1] European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL))OJ C 252, 18.7.2018, p. 239–257.

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

[3] Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety (Text with EEA relevance) OJ L 11, 15.1.2002, p. 4–17 General Safety of Products Directive (GSPD)

[4] Regulation (EU) 2023/988 of the European Parliament and of the Council of 10 May 2023 on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council and Directive (EU) 2020/1828 of the European Parliament and the Council, and repealing Directive 2001/95/EC of the European Parliament and of the Council and Council Directive 87/357/EEC (Text with EEA relevance) PE/79/2022/REV/1 OJ L 135, 23.5.2023, p. 1–51General Safety of Products Regulation.

[5] 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) (Text with EEA relevance) OJ L 157, 9.6.2006, p. 24–86, Machinery Directive.

[6] 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 (Text with EEA relevance) PE/6/2023/REV/1 OJ L 165, 29.6.2023, p. 1–102 Machinery regulation

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

[8] National Implementation of the MDR D.lgs 137/2022 and decrees 12 April 2023. GU 13 June 2023 n.136.

[9] Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR https://ec.europa.eu/docsroom/documents/37581 accessed 27 October 2023.

[10] Clinical Trials regulation (and its implementation in Italy): Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC Text with EEA relevance OJ L 158, 27.5.2014.

[11] National implementation of Clinical Trials Regulation into the Italian discipline: 26, 27, 30 January 2023 decrees

[12] ALTAI, Assessment list. Trustworthy Artificial Intelligence Self-Assessment https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment . Accessed 25 October 2023.

[13] AI act proposal (general regulation for Artificial Intelligence, COM/2021/206 final), AI act.
[14] Product liability directive proposal (COM/2022/495 final) (PLDU).
[15] AI civil liability directive proposal (COM/2022/496 final) (AILP).
[16] Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services (Text with EEA relevance.) PE/26/2019/REV/1 OJ L 136, 22.5.2019, p. 1–27 (DCDS).
[17] Directive (EU) 2019/771 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC (Text with EEA relevance.) PE/27/2019/REV/1 OJ L 136, 22.5.2019, p. 28–50 771(SG).
[18] European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) OJ L 119, 4.5.2016.
[19] Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety (Text with EEA relevance) OJ L 11, 15.1.2002, p. 4–17 General Safety of Products Directive (GSPD)
[20] D. lgs 193/2003 updated with D.lgs. 101/2018, Italian Code of Privacy
[21] 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] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9124510 Accessed 25th October 2023.
[22] 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] https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9069637 Accessed 25th October 2023.
[23] Parere ai sensi sensi dell'art. 110 del Codice e dell'art. 36 del Regolamento - 30 giugno 2022 [9791886] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9791886 Accessed 25th October 2023.
[24] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (Text with EEA relevance) PE/85/2021/REV/1 OJ L 152, 3.6.2022, p. 1–44
[25] Data Act (rules on access and re-use of personal and non-personal data from IoT, COM/2022/68 final)
[26] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 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) Text with EEA relevance. PE/24/2024/REV/1OJ L, 2024/1689
[27] Product liability directive proposal (COM/2022/495 final) (PLDU)
[28] 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], https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/10016146 Accessed, 11 October 2024.
[29] 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) PE/49/2023/REV/1 OJ L, 2023/2854, 22.12.2023, (DA)
[30] European Health Data Space (EHDS, secondary use of health Data for research, COM/2022/197 final) Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, OJ L 77, 27.03.1996, p. 20-28. (The Database directive).
[31] 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)
[32] 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)
[33] D.P.C.M., No. 81 of April 14, 2021 (DPCM 2) Presidential Decree No. 54 of February 5, 2021, Decree Law 82/2021.

[34] D.P.C.M. No. 131 of July 30, 2020 (DPCM 1)
[35] Legislative Decree N. 65 of May 18, 2018, Decree-Law of September 21, 2019 (Perimeter Decree).
[36] 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, p. 1–30 NIS Directive
[37] Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs (Codified version) (Text with EEA relevance), OJ L 111, 05.05.2009, p. 16-22. (the Software directive).
[38] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, OJ L 167, 22.06.2001, p. 10-19 (the Information Society Directive, known, hereinafter InfoSoc Directive)
[39] 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. (The Copyright in the Digital Single Market Directive, hereinafter CDSMD)
[40] Directive 2006/116/EC of the European Parliament and of the Council of 12 December 2006 on the term of protection of copyright and certain related rights (Codified version), OJ L 372, 27.12.2006, p. 12-18 (the Term Directive).
[41] The Unitary Patent Protection Regulation 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.
[42] EPO, The EPO at a glance, https://www.epo.org/en/about-us/at-a-glance. Accessed on 11 October 2024.
[43] EPO, The EPO at a glance, https://www.epo.org/en/about-us/at-a-glance. Accessed on 11 October 2024.
[44] EPO, Decision of the Boards of Appeal, https://www.epo.org/en/case-law-appeals/decisions. Accessed 11 October 2024.
[45] R. Bekkers, Pilot Study for Essentiality Assessment of Standard Essential Patents, 2020, https://op.europa.eu/en/publication-detail/-/publication/1829605f-2d3a-11eb-b27b-01aa75ed71a1/language-en, accessed 11 October 2024.
[46] EUR-Lex, Enforcement of intellectual property rights, https://eur-lex.europa.eu/EN/legal-content/summary/enforcement-of-intellectual-property-rights.html Accessed 11 October 2024.
[47] Proposed Regulation on Standard Essential Patents 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
[48] F. Gennari, “Standard Setting Organisations for the IoT: How To Ensure a Better Degree of Liability?”, Masaryk University Journal of Law and Technology, 15, 2, 2021, 153-173.
[49] Gleiss- Lutz, « European Parliament Gives Green Light For Regulation on Standard Essential Patents” https://www.gleisslutz.com/en/news-events/know-how/european-parliament-gives-green-light-regulation-standard-essential-patents. Accessed on 11 October 2024.
[50] 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. (Trade Secrets Directive)
[51] WIPO Intellectual Property Handbook. Available at https://www.wipo.int/standards/en/handbook.html, accessed on 11 October 2024.
[52] Council Regulation (EC) No 6/2002 of 12 December 2001 on Community designs OJ L 3, 5.1.2002, p. 1–24
[53] 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 (Design directive)
[54] Intellectual Property Rights Enforcement Directive (IPRED) 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.