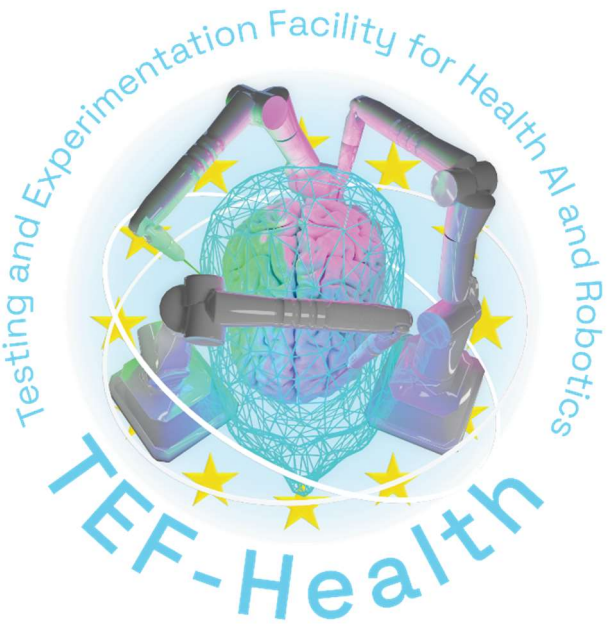
TEF-Health

Gobert, Alix; Rappe, Martin; Van Gyseghem, Jean-Marc; Bourguignon, Camille

Publication date:
2023

Document Version
Publisher's PDF, also known as Version of record



Public report

D2.1: Legal, Ethical Framework

Action number: 101100700
Action Acronym: TEF-Health
Action title: Testing and Experimentation Facility for Health AI and Robotics
Author(s): UNamur-CRIDS

Submission date: December 2023

This project document is published at https://www.tefhealth.eu/.

Co-funded by
the European Union

Table of content

1 TEF-Health

TEF-Health[1] develops a reference testing and experimentation facility (TEF) with a threefold Objective:

(1) Carrying out tests and experiments of AI solutions in real or realistic environments;
(2) Implementing evaluation activities to facilitate market access for trustworthy intelligent technologies considering regulatory requirements (certification, standardization, code of conduct), and ensuring easy access to these resources (link with digital innovation hubs); and
(3) Optimizing investments by capitalizing on past investments.

[1] This short description of TEF-Health (Section 1) is issued from Annex 1 of the Grant Agreement; see Grant Agreement, Annex 1 – Description of the action (Part A), Project Summary, p. 3.

TEF-Health has at project start high Maturity. It provides existing expertise and infrastructure for design and implementation of AI testing in real world environments at TRL 6-8.

The main asset lies in the general structure of each node, designed to address the broad environment of evaluation and testing, to speed up the development and the market access of AI solutions in healthcare. Each node combines several forms of testing:

- The real testing facilities (hospital platforms, both physical and data and compute infrastructures, living labs) and laboratory facilities.
- The supporting activities of defining evaluation protocols, developing evaluation tools, and assessing conformity complement the activities.

TEF-Health will generate Impact by increasing effectiveness, resilience, sustainability of health systems, reduce inequalities; and ensure compliance with legal, ethical, quality and interoperability standards.

The long-term business plan integrates with the one of EBRAINS RI on the ESFRI roadmap for financial Sustainability.

The project forms a network of leading EU hospitals and Medical Universities e.g., Charité and Karolinska Institute, National Metrology Institutes for definition of standards, and certification bodies as well as innovation clusters, e.g., European Institute of Technology EITHealth with links to the European Health Data Space.

TEF-Health addresses ethical, and societal aspects supported by patient organizations.

2 Introduction

2.1 Description and insertion of deliverable D2.1 'Legal, Ethical Framework' within TEF-Health

This document corresponds to the **deliverable D2.1 called 'Legal, Ethical Framework'**. The Lead beneficiary assigned in the Grant Agreement to carry out this deliverable is UNamur-CRIDS.

This deliverable is part of a more global **task T2.2 called 'Analysis of legal and ethical framework'**. Such a task is described in the Grant Agreement as follows: "This task will examine legal framework (EU and national) applicable to TEF-Health and provide the Consortium and users with guidelines on legally compliant development of technology and general conduct within the project"[2]. This is one of the tasks that must be accomplished within the **Work Package (hereafter "WP") 2 called 'Ethics, Legal & Society'** of TEF-Health for which the leader is UNamur-CRIDS.

The task T2.2 as well as this deliverable D2.1 must be understood as means to reach the objectives of WP2 within TEF-Health. These objectives are notably to "support project partners

[2] Grant Agreement, Annex 1 – Description of the action (Part A), List of Work packages, p. 9.

and the coordinator to keep [the] project in line with legal and ethical requirements" and to "analyze and understand needs stemming from new European regulatory approaches"[3].

More broadly speaking, this deliverable D2.1 aims to be a crucial stone in achieving one of the main objectives of TEF-Health, i.e., to "ensure compliance with legal, ethical, [...] standards"[4].

2.2 Main objectives of the deliverable D2.1 'Legal, Ethical Framework'

To be in line with T2.2 and the general objectives of WP2, the deliverable D2.1 is envisioned as being a document that must be **useful to the partners of TEF-Health Consortium**. The goal of this document is to provide the partners of the Consortium with an overview of the legal acts or legal acts proposals, and the legal requirements provided in these acts, that apply or will apply to them and/or to the users of TEF-Health, i.e., the SMEs that will use TEF-Health services offered by the partners.

This document aims to answer the two following needs:

- First, the partners must be informed and aware of the legal requirements they must comply with when offering services to TEF-Health users (the SMEs), e.g., which legal requirements must be complied with when they offer a service based on patient datasets.
- Secondly, the testing and experimentation services offered through TEF-Health must be designed in a way that ensures that the users' products (the SMEs' products) benefiting from these services are, in the end, thanks to TEF-Health services, compliant with the applicable legal provisions.

From such a perspective, this document is closely linked to the **Legal and Ethical Helpdesk** the WP2 implemented, through the creation of an email service, according to **Milestone 3** defined in the Grant Agreement. The objective of the Legal and Ethical Helpdesk is precisely to ensure permanent and day-to-day legal and ethical support for the partners of the TEF-Health Consortium. The intuition is that the deliverable D2.1 will help the partners identify and define the legal issues they might be facing within the services they offer through TEF-Health and then address accurate legal requests through the Legal and Ethical Helpdesk for which WP2 will be able to provide answers and guidelines.

2.3 Short introduction on the content of the deliverable D2.1 'Legal, Ethical Framework'

2.3.1 The scope of the legal acts and legal acts proposals analyzed

This document aims **to present and analyze several legal acts or legal acts proposals** that will or might apply to the partners of the Consortium within TEF-Health.

The material scope of this document must be coherent with the objectives of T2.2 and WP2, i.e., notably to "analyze and understand needs stemming from new European regulatory approaches"[5] and to provide "guidelines on legally compliant development of technology"[6].

[3] *Ibid*.
[4] Grant Agreement, Annex 1 – Description of the action (Part A), Project Summary, p. 3.
[5] Grant Agreement, Annex 1 – Description of the action (Part A), List of Work packages, p. 9.
[6] *Ibid*.

Consequently, this document focuses on legal acts or legal acts proposals that are now shaping the market regarding the products TEF-Health users (the SMEs) will aim to develop and put on the European market, i.e. medical devices based on artificial intelligence (hereafter also "AI"). These legal acts are for instance, digital regulations (i) applying to artificial intelligence systems, (ii) dealing with the sharing of data or (iii) with the processing of personal data, etc.

It does not, however, tackle other legal considerations that TEF-Health project may also face, that must be led by, or in collaboration with, other WPs of TEF-Health Consortium: (i) the considerations regarding the coordination between the partners within TEF-Health Consortium (e.g. the data management within TEF-Health Consortium or the drafting and implementation of the consortium agreement that correspond to tasks or deliverables that are under the lead of WP1) or (ii) the considerations regarding business aspects of the TEF-Health project (e.g. the pricing of TEF-Health services to be offered on the market or the compliance of such services with state aids laws that are under the lead of WP10).

On the opposite, this document will draw bridges with other WPs when the topics addressed must be analyzed with an interdisciplinary perspective. In particular, the legal analysis implied by the specificities of the products to be developed by the TEF-Health users (the SMEs) thanks to TEF-Health services (i.e., medical devices and artificial intelligence systems) will have to be made in parallel with the works done and to be done notably within WP6 'Standards and Quality' and WP7 'Certification'.

2.3.2 The focuses made in this document

To be able to reach the goal previously defined (being useful to the partners of TEF-Health Consortium), decisions that shaped the creation and the content of this document D2.1, had to be made. These decisions are the following:

- **Focus on identified legal acts and proposals (non-exhaustivity):** to keep this document efficient and readable (and then as short as possible), it has been decided to focus on the description of some legal acts, or legal acts proposals, identified as being the most critical ones to the partners for accomplishing the first steps of the TEF-Health project. Some other legal acts or proposals will be of interest to TEF-Health though. But they will be analyzed in a second phase. Therefore, this document is not to be considered exhaustive.

- **Focus on legal acts or proposals at European Union level (not national level):** it has been decided to draw a legal overview that is of interest to all the partners of TEF-Health with a European Union focus, and therefore to exclude national-specificities from the analysis at that stage. Such a decision is supported by the fact that a major part of the relevant legal acts or proposals to be considered at the first stage are adopted at European Union level.

- **Focus on legal considerations (without integrating ethical considerations *per se*):** it has also been decided that, in this document, the focus is made on legal considerations. The goal of this document is to provide a neutral analysis of the legal framework in force or about to be in force in the European Union. Ethical considerations are then not taken

per se into account in this document. They will be integrated into the reflections at further phases. This document must indeed be seen as a basis for deeper reflections that will be led at further stages along the project. However, there are always some ethical considerations in any European legislation dealing with data protection or health-related concepts.

3 Partners involved

The partner assigned as leader for this deliverable D2.1 is **UNamur-CRIDS**. This document was written by the UNamur-CRIDS members assigned to TEF-Health project, namely Camille Bourguignon, Alix Gobert, Martin Rappe and Jean-Marc Van Gyseghem. Some parts were peer-reviewed by other members of UNamur-CRIDS so that the document could benefit from their extra expertise on the topics. The part dedicated to the AI Act proposal was then peer-reviewed by Michael Lognoul and the parts dedicated to the Data Governance Act and the Data Act proposal were peer-reviewed by Manon Knockaert.

Since this document mainly focuses on the legal considerations raised by TEF-Health project, UNamur-CRIDS, as the only 'legal partner' in the Consortium, wrote this report without involving other partners of the TEF-Health Consortium on a systematic basis. Nevertheless, some partners were asked to collaborate in the writing of this document on specific parts when considered relevant and/or necessary. For instance, Ariana Sliwa (**TÜV Nord**, Project Lead TEF Health for WP7 'Certification') reviewed the part dedicated to the description of the Medical Devices Regulation so that some certification perspectives could be integrated; Jana Fehr (**Charité**) reviewed the parts dedicated to the AI Act proposal and the Medical Devices Regulation so that some ethical perspectives could already be considered.

4 Results

4.1 Introduction part

4.1.1 The contribution of TEF-Health project to a better implementation of the applicable legal acts or legal acts proposals

TEF-Health is part of the Digital Europe Programme which follows, among other goals, the objective to "support small and medium-sized enterprises (SMEs) that intend to harness the digital transformation in their production processes"[7]. Concretely, TEF-Health aims to "offer a combination of physical and virtual facilities, in which technology providers can get support to test their latest AI-based soft-/hardware technologies in real-world environments"[8].

The legislations to be complied with by businesses, and especially SMEs, when developing such technologies appear complex and various. They can be seen as real obstacles that hinder the

[7] Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme and repealing Decision (EU) 2015/2240, *O.J.*, L 166, 11 May 2021 (hereafter "Regulation Digital Europe Programme"), recital 16.

[8] European Commission, Shaping Europe's digital future – Sectorial AI Testing and Experimentation Facilities under the Digital Europe Programme, available on Sectorial AI Testing and Experimentation Facilities under the Digital Europe Programme | Shaping Europe's digital future (europa.eu), consulted on 29 November 2023.

introduction of these technologies to the market. As such, they can be seen as obstacles to innovation. Such assertion is even truer in the healthcare sector in which TEF-Health project is active since this sector presents specific risks and is therefore subject to specific legislations (e.g. the data that must be used to develop a product are often deemed sensitive, the products to be developed are regulated, etc.). In such a context, TEF-Health project is not only high-level technical support but also it can contribute to the right apprehension and implementation of these numerous complex legislations by businesses, and especially by SMEs, all over Europe. More broadly speaking, TEF-Health project can become the space where the balance between (i) innovation and (ii) safety and the necessary patient's trust (two objectives that justify these complex legislations) is ensured.

This deliverable D2.1 can be seen as the first stone to be laid so that these legislations are identified and analysed. It will allow the partners of TEF-Health Consortium to offer services that comply with these legislations and to ensure the products developed thanks to TEF-Health services are compliant with them.

4.1.2 The identification process of the legal acts analysed in deliverable D2.1

Digital technologies are now regulated by many different legislations. We remind that, for the reasons mentioned in part 2.3 *supra*, we will focus on the legislations adopted or proposed at EU level and will not address national specificities in this document.

Some actors made the difficult task to list these legislations in a comprehensive manner and arrived at the conclusion that EU legislations in the digital sector are more than 100 (including not only the legislations adopted and in force but also the legislations proposed and in negotiations as well as those that are only planned)[9].

One can easily understand that an analysis of any of these numerous legislations would not be efficient for this deliverable D2.1, nor useful[10]. Therefore, the first work that had to be done within this deliverable D2.1 was to identify, among the legislations applicable to the digital sector the ones that appeared the most relevant for TEF-Health project, at the early stage in which the deliverable D2.1 must be published (end of the first year of the project).

4.1.3 The legal acts dealing with the *products* concerned by TEF-Health project

TEF-Health project is part of the Digital Europe Programme. More precisely it follows the specific objective 2 in the identified key policy area of artificial intelligence[11]. Since the use of artificial intelligence is about to be regulated at European level through an important piece of legislation,

[9] K. ZENNER, « Digital factsheet #5: A dataset on EU legislation for the digital world", available on https://www.kaizenner.eu/post/digital-factsheet-5, consulted on 30 November 2023; For an overview of the legislations adopted or proposed in the period 2020-2023, see also Chronique de législation : droit de l'Union européenne et numérique (2020-2023), *R.D.T.I.*, 2024 (to be published).
[10] Regarding this necessity for a selection among the EU legislations applicable to the digital sector, also see *supra* point 2.3.
[11] Regulation Digital Europe Programme, recital 14 and art. 3(2) (b) and 5.

namely the AI Act[12], it appeared necessary to immediately focus on it, even though the final act is not adopted yet. Recital 74 of the AI Act proposal even refers to the "Testing and Experimentation Facilities established by the Commission and the Member States at national or EU level", such as TEF-Health, as being means to contribute to the implementation of the AI Act. The first part of this deliverable D2.1 is therefore logically an analysis of the AI Act proposal[13].

Besides, AI is also subject to other legal proposals that are now being negotiated at EU institutions level[14]. They deal with the liability rules applicable to AI. Nevertheless, it has been decided not to analyse them within this deliverable D2.1 because, as they aim to lay down rules to address the difficulties of proof at a stage where the product has created damage (i.e. where the product is already on the market), these future rules might not have a direct impact on the services to be developed through TEF-Health project (which will be offered before the product is introduced to the market).

The products to be developed by TEF-Health users (the SMEs) thanks to TEF-Health services are medical devices based on AI. Medical devices are to be considered regulated products, i.e. products for which the introduction to the market is regulated. These specific regulatory requirements are laid down in two general EU regulations dated 5 April 2017 that are already in force and implemented in the Member States: Medical Devices Regulation[15] (hereafter "MDR") and In Vitro Diagnostic Medical Devices Regulation[16]. Analysing and presenting the legal requirements laid down in MDR appeared of great importance for deliverable D2.1 since one of the main objectives of TEF-Health project is to facilitate the introduction of medical devices based on AI to the market through the definition of agile certification processes of medical devices[17]. It has been decided not to analyse In Vitro Diagnostic Medical Devices Regulation though, for reasons of efficiency and readability, and because, as far as we know, for now in vitro diagnostic medical devices are not at the core of TEF-Health project.

The analysis of the AI Act and of MDR will be proposed under point 4.2 of this document through an Annex 1, named "Products".

---

[12] Proposal for a Regulation of the European Parliament and the Council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain Union legislative acts, COM(2021) 206 final, 21st April 2021.
[13] See Annex 1 'Products', section 1.
[14] Proposal for a directive of the European Parliament and of the Council on liability for defective products, COM (2022) 495 final, 28 September 2022 and Proposal for a directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive), COM (2022) 496 final, 28 September 2022.
[15] 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, L 117/1, *J.O.*, 5 Mai 2017.
[16] Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU, L 117/176, *J.O.*, 5 May 2017.
[17] Grant Agreement, Annex 1 – Description of the action (Part A), List of Work packages, p.13.

4.1.4 The legal acts dealing with the *data* at the basis of the products concerned by TEF-Health project

The AI Act proposal expressly mentions that it must be without prejudice to and must complement the General Data Protection Regulation[18] (hereafter "GDPR")[19] which lays down the rules to protect personal data and especially sensitive data such as health data. GDPR compliance by the partners of TEF-Health Consortium when offering their services and by TEF-Health users (the SMEs) when using TEF-Health services, must be ensured. Proposing an analysis of GDPR in TEF-Health context seemed then necessary within deliverable D2.1.

The AI Act proposal also expressly refers to "Data Governance Act[20], the Open Data Directive[21] and other initiatives under the EU strategy for data[22], which will establish trusted mechanisms and services for the re-use, sharing and pooling of data that are essential for the development of data-driven AI models of high quality"[23].

Ones of the key pillars of this above-mentioned EU strategy for data is the definition of cross-sectoral measures for data access, use and sharing (through notably the Data Governance Act - hereafter "DGA"- mentioned above and the Data Act proposal[24])[25] as well as the creation of sector-specific data spaces, such as the European Health Data Space (hereafter "EHDS"). EHDS will allow both primary and secondary uses of health data[26]. The idea behind the creation of the EHDS is to make the industry "benefit from greater availability of electronic health data through privacy preserving mechanisms for citizens including infrastructures that are trustworthy by design, and the use of anonymisation, aggregation and synthetic data [and] from data that could help them develop new medicinal products or new devices involving AI"[27]. The future EHDS regulation will then be of high interest to the partners of TEF-Health Consortium when developing and offering their services and TEF-Health users (the SMEs) when using TEF-Health services.

As they lay down or will lay down the legal framework organising the access, the use and the sharing of data, and because data are at the basis of the major part of the services that will be offered through TEF-Health, DGA, Data Act proposal and EHDS proposal are analysed in

[18] AI Act proposal, explanatory memorandum, p. 4.
[19] Regulation (EU) 2016/679 of the European Union 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), *O.J.*, L119/1, 4 May 2016.
[20] Regulation (EU) 2022/268 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), *O.J.*, L 152/1, 3 June 2022.
[21] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (recast), *O.J.*, L 172/56, 26 June 2019.
[22] Communication from the Commission - A European strategy for data, COM(2020) 66 final, 19 February 2020 (hereafter "European Strategy for data").
[23] AI Act proposal, explanatory memorandum, p. 5.
[24] Proposal for a regulation on harmonised rules on fair access to and use of data (Data Act), COM(2022) 68 final, 23 February 2022.
[25] European Strategy for data, pp. 12-15.
[26] Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space, COM(2022) 197 final, 3 May 2022.
[27] Communication from the European Commission - A European Health Data Space: harnessing the power of health data for people, patients and innovation, COM(2022) 196 final, 3 May 2022, p. 16.

deliverable D2.1.

The analysis of GDPR, DGA, EHDS proposal and Data Act proposal will be proposed under point 4.3 of this document through an Annex 2, named "Data".

4.1.5 Some other legal acts that might need analysis at further stages of TEF-Health project

Beside the legal acts proposals mentioned above[28] completing the AI Act proposal on the liability aspects of AI and the In Vitro Diagnostic Medical Devices Regulation that may need a proper analysis later in the project, other legal acts might also be or become of interest at further phases of TEF-Health project.

For instance, since TEF-Health services will be proposed through a catalogue available online and since some partners aim to create platforms for allowing the SMEs to meet experts, e-commerce legislations, such as the e-commerce directive[29] and the Digital Services Act[30] could also be of interest to the partners of TEF-Health. Other legal texts regarding for instance cybersecurity[31] or interoperability[32] might also need some accurate analysis at further phases.

4.1.6 The period considered for the analysis

Since this document D2.1 had to be submitted for Consortium review on 1st December 2023, the analysis of the legal acts proposals announced - i.e. the ones that are not yet adopted and published in the EU Official Journal (namely the AI Act proposal, Data Act proposal, and EHDS proposal) is made on the last version publicly available of the proposal on the 1st December 2023. For the sake of completeness, reference to later versions is made in the document. Nevertheless, a proper analysis of these later versions could not be integrated into this document. Such analysis, or in case it appears more relevant, the analysis of the act finally adopted, will be proposed in later phases of the project.

4.2 'Products'

This part 'Products' 4.2 aims to analyse the legal acts and proposals applicable to TEF-Health users' (SMEs') products that will be tested and experimented through the TEF-Health services offered by the partners of TEF-Health Consortium.

---

[28] See *supra* point 4.1.3.
[29] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), *O.J.*, L 178, 17 July 2000.
[30] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), *O.J.*, L 277, 27 October 2022.
[31] For instance, 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), *O.J.*, L 333, 27 December 2022.
[32] Proposal for a regulation of the European Parliament and the Council laying down measures for a high level of public sector interoperability across the Union (Interoperable Europe Act), COM(2022) 720 final, 18 November 2022.

See Annex 1

4.3 'Data'

This part 'Data' 4.3 aims to analyse the legal acts and proposals organising the sharing of data that will take place within TEF-Health project for and when offering services to TEF-Health users (the SMEs).

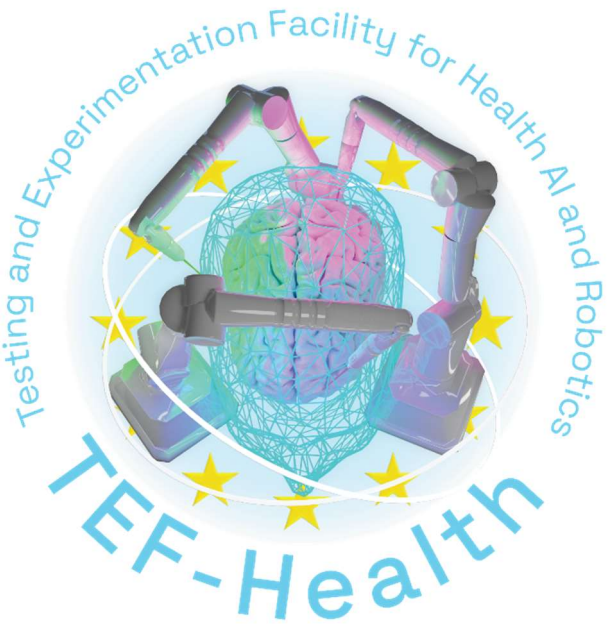
See Annex 2

5 Conclusion, next steps

This document must be seen as the first stone of a comprehensive analysis of the applicable or about-to-be-applicable legal frameworks for TEF-Health project.

Since the legal framework it aims to analyse is permanently evolving, this document must be a living document. The idea is to update this document each time it is necessary all along TEF-Health project (e.g. an update of this document will be deemed necessary when the Artificial Intelligence Act proposal is adopted and published in the EU Official Journal).

The idea is also to complement this document with analysis of applicative use cases the partners of TEF-Health Consortium may face and submit through the legal helpdesk.



Public report

D2.1: Legal, Ethical Framework Annex 1 'Products'

Action number: 101100700
Action Acronym: TEF-Health
Action title: Testing and Experimentation Facility for Health AI and Robotics
Author(s): UNamur-CRIDS

Submission date: December 2023

This project document is published at https://www.tefhealth.eu/.

Co-funded by the European Union

Table of content

Co-funded by the European Union

1 Artificial Intelligence Act proposal (AI Act proposal)

1.1 Preamble

This analysis provides information about the AI Act proposal[1], on which a political agreement has recently been reached on 8 December 2023. As TEF-Health project aims to accelerate and facilitate the validation and certification of artificial intelligence (hereafter also "AI") and robotics in medical devices, this regulation would apply to the tools developed by TEF-Health users (the SMEs) using the services offered by TEF-Health consortium (hereafter the "Consortium"). It will likely also be directly applicable to some of the services offered through TEF-Health themselves. For these reasons, the content of this future regulation shall be analysed, which is the purpose of this section.

First, this section summarises the context in which the proposal for an AI regulation has been drafted by the European Commission and briefly recalls the discussions that have occurred since this moment. Second, it describes the material scope of the future AI Act and analyses the interactions between the stakeholders entering the personal scope of the text. Third, it focuses on the requirements imposed by the future regulation, the level of which mainly[2] depends on the level of risk that the AI system creates. Fourth, the section analyses the conformity assessment that must be performed by the provider of an AI system in some circumstances and discusses the implications of such obligations for TEF-Health. Finally, the section gives an overview of the rules applicable to the new regulatory sandboxes.

1.2 Context and purposes of the proposal

1.2.1 Main purpose and chosen approach

Artificial intelligence systems are raising expectations mainly in terms of their ability to make work more productive or decisions more relevant by enhancing capabilities of human beings. However, AI technology also raises risks for negative societal and environmental impacts during deployment. To address these concerns, the European Commission proposed the AI Act to foster the "development of an ecosystem of trust by proposing a legal framework for trustworthy AI"[3]. The proposal is built, among others, on the work of the High-Level Expert Group on Artificial Intelligence (AI-HLEG)[4]. In 2019, this group issued seven guiding requirements that must be met to realise a trustworthy AI system[5]. According to the experts, trustworthy AI shall be (i) subject to human agency and oversight, (ii) technically robust and safe. It (iii) shall ensure data governance and privacy, (iv) transparency, (v) diversity, non-discrimination, and fairness and (vi) societal and environmental wellbeing. Finally, the provider of an AI system shall also be subject to an (vii)

[1] Proposal for a Regulation of the European Parliament and the Council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain Union legislative acts, COM(2021) 206 final, 21st April 2021 (hereafter "AI Act proposal").
[2] Such an approach is partially questioned by some amendments voted by the European Parliament, see *infra,* points 1.4.2.1 and 1.4.3.
[3] AI Act proposal, explanatory memorandum, p. 1.
[4] AI Act proposal, explanatory memorandum, p. 8.
[5] High-Level Expert Group on Artificial Intelligence (hereafter "HLEG"), "Ethics Guidelines for Trustworthy AI", 8 April 2019, p. 14.

accountability principle[6]. These requirements partially appear on the proposal of the Commission and are more developed on the Parliament position, which suggests implementing them as principles that all AI systems shall comply with, irrespectively of the level of risk they raise[7].

The European Commission stresses that the creation of such a trustworthy AI ecosystem would strike a balance between promoting European innovation in AI and protecting people and their fundamental rights in relation to this technology[8]. This goal is closely related to the one pursued by the TEF-Health project, which aims to enable companies to develop trustworthy medical AI products for application in healthcare by establishing a testing and experimentation facility for rapid validation and certification[9]. It should be noted that some recitals of the AI Act proposal are directly referring to testing and experimentation facilities, such as TEF-Health. Recital 45 stresses that these TEFs "[...] should be able to access and use high quality datasets within their respective fields of activities which are related to this Regulation". It also highlights that "[...] European common data spaces established by the Commission and the facilitation of data sharing between businesses and with government in the public interest will be instrumental to provide trustful, accountable and non-discriminatory access to high quality data for the training, validation and testing of AI systems. For example, the European health data space will facilitate non-discriminatory access to health data and the training of artificial intelligence algorithms on those datasets, in a privacy-preserving, secure, timely, transparent and trustworthy manner, and with an appropriate institutional governance".

Recital 74 of the AI Act explains that the TEFs, the European Digital Innovation Hubs and AI-on demand platforms should contribute to the implementation of the AI Act by providing technical and scientific supports to AI providers and notified bodies in their respective fields of competences[10]. Recital 75 also targets all TEFs and, even more precisely, TEF-Health. It reads as follows: "It is appropriate that the Commission facilitates, to the extent possible, access to Testing and Experimentation Facilities to bodies, groups or laboratories established or accredited pursuant to any relevant Union harmonisation legislation and which fulfil tasks in the context of conformity assessment of products or devices covered by that Union harmonisation legislation. This is notably the case for expert panels, expert laboratories and reference laboratories in the field of medical devices pursuant to Regulation (EU) 2017/745 and Regulation (EU) 2017/746 [i.e. Medical Devices Regulation]".

[6] The HLEG develops its view on these principles on pp. 14-20 of its guidelines.
[7] See *infra*, point 1.4.2.1.
[8] AI Act proposal, explanatory memorandum, pp. 1-3.
[9] TEF-Health Grant Agreement, Annex I – Description of the action (part A), p. 3.
[10] "In order to minimise the risks to implementation resulting from lack of knowledge and expertise in the market as well as to facilitate compliance of providers and notified bodies with their obligations under this Regulation, the AI-on demand platform, the European Digital Innovation Hubs and the Testing and Experimentation Facilities established by the Commission and the Member States at national or EU level should possibly contribute to the implementation of this Regulation. Within their respective mission and fields of competence, they may provide in particular technical and scientific support to providers and notified bodies".

1.2.2 Adoption procedure status

The initial proposal for an AI Act was formulated by the European Commission on 21 April 2021. It was followed by the General Approach of the Council of the European Union[11] and then by the official position of the European Parliament, voted in plenary session on 14 June 2023[12]. Based on these three positions, the traditional trilogue between the European Commission, the Council and the European Parliament, began in July. A provisory political agreement on the final text has been reached on 8 December 2023[13]. However, as this report had to be submitted for the Consortium review on 1st December 2023, it could not take the content of this agreement into account. This section will be updated after the formal approvals of the Parliament and the Council and after publication of the adopted act in the Official Journal in 2024[14].

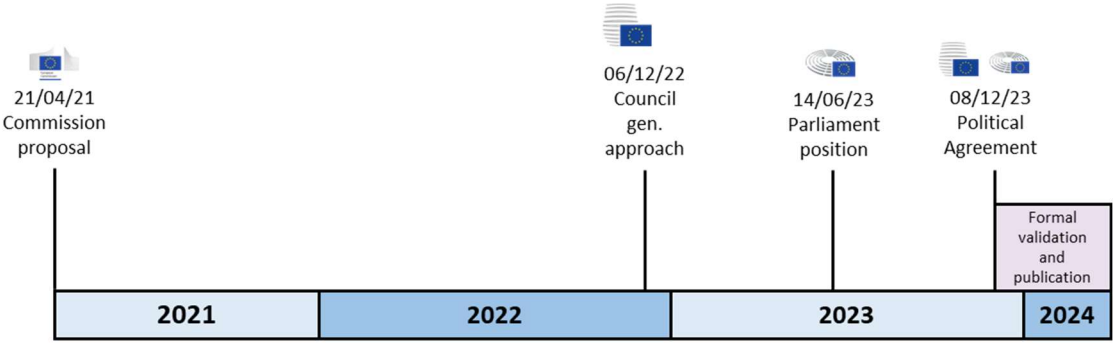


Figure 1 AI Act adoption procedure timeline

This analysis summarises therefore the three positions of the European institutions, i.e. the Commission, the Council and the Parliament. It mainly focuses on the Commission's proposal, supplemented by the Council's General Approach, and mentions the most sensitive points amongst those raised by the Parliament.

1.3 Scope and actors involved

1.3.1 Legal definition of an "artificial intelligence system"

The AI Act intends to regulate "artificial intelligence systems" (hereafter "AI systems"). This concept differs from one European institution's position to another. To make its definition future

[11] Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts - General approach, 2021/0106 (COD), 6 December 2022 (hereafter "Council position").
[12] Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD), P9_TA(2023)0236, 14 June 2023 (hereafter "Parliament position").
[13] European Parliament, "Artificial Intelligence Act: deal on comprehensive rules for trustworthy AI", available on https://www.europarl.europa.eu/news/en/press-room/20231206IPR15699/artificial-intelligence-act-deal-on-comprehensive-rules-for-trustworthy-ai, 9 December 2023.
[14] For the "next steps" related to the adoption of the final draft, see European Commission, "Commission welcomes political agreement on Artificial Intelligence Act*", available on https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6473, 9 December 2023.

proof and technologically neutral[15], the Commission proposed the following: "software that is developed with one or more of the techniques and approaches listed in Annex I [i.e. machine learning approaches, logic- and knowledge- based approaches and statistical approaches, Bayesian estimation search and optimization methods][16] and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with"[17]. When needed, the Commission would also be empowered to modify Annex I and include other techniques or approaches within the definition of AI systems[18].

The Council and Parliament rejected this part of the proposal. They opted for a more restrictive definition, centred on machine learning[19] and aligned with the definition of the Organization for Economic Co-operation and Development (OECD")[20]. According to the Council's position, an "AI system" should cover "a system that is designed to operate with elements of autonomy and that, based on machine and/or human-provided data and inputs, infers how to achieve a given set of objectives using machine learning and/or logic- and knowledge based approaches, and produces system-generated outputs such as content (generative AI systems), predictions, recommendations or decisions, influencing the environments with which the AI system interacts"[21]. The Parliament rather defines the AI system as a « machine-based system that is designed to operate with varying levels of autonomy and that can, for explicit or implicit objectives, generate outputs such as predictions, recommendations, or decisions, that influence physical or virtual environments"[22].

For the TEF Health project, the legal definition of AI is important. Products that will beneficiate from TEF Health services will be medical devices based on AI systems, developed by European SMEs. They will fall within the material scope of the AI Act. This is why the Consortium must pay attention to this future regulation so that the services proposed through TEF-Health efficiently reach their main goal, i.e., help SMEs to comply with its requirements.

1.3.2 Actors and other key-concepts

The other key-concepts do not differ greatly from one position to another. They can therefore be summarised as follows. In practical terms, the AI Act proposal follows a risk-based approach,

[15] AI Act proposal, explanatory memorandum, p. 12.
[16] The techniques and approaches listed in Annex 1 are precisely: "a) Machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning; b) Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems; an c) Statistical approaches, Bayesian estimation, search and optimization methods", AI Act proposal, Annex 1.
[17] AI Act proposal, art. 3(1).
[18] AI Act proposal, art. 3(1).
[19] Parliament position, recital 6a, pp. 12-13; Council position's, main elements of the compromise proposal, p. 4.
[20] Parliament position, recital 6, pp. 11-12.
[21] Council position, art. 3(1).
[22] Parliament position's, art. 3(1), p. 112.

"[...] differentiating between uses of AI systems that create (i) an unacceptable risk, (ii) a high risk, and (iii) low or minimal risk"[23].

The rules will apply mainly[24] to providers placing AI systems on the European Union (hereafter also "EU") market or putting them into services, to users (or "deployers")[25] of AI systems located within the EU and to providers and users (or "deployers") of AI systems that are in a third country, where the output produced by the system is used in the EU[26].

The different positions distinguish five principal "actors"[27], i.e. the provider, the importer, the distributor, the user (called "deployer" by the Parliament) and the affected person[28]. The definitions of these actors are afterwards presented.

The relationships between these actors are summarised in figure 2.

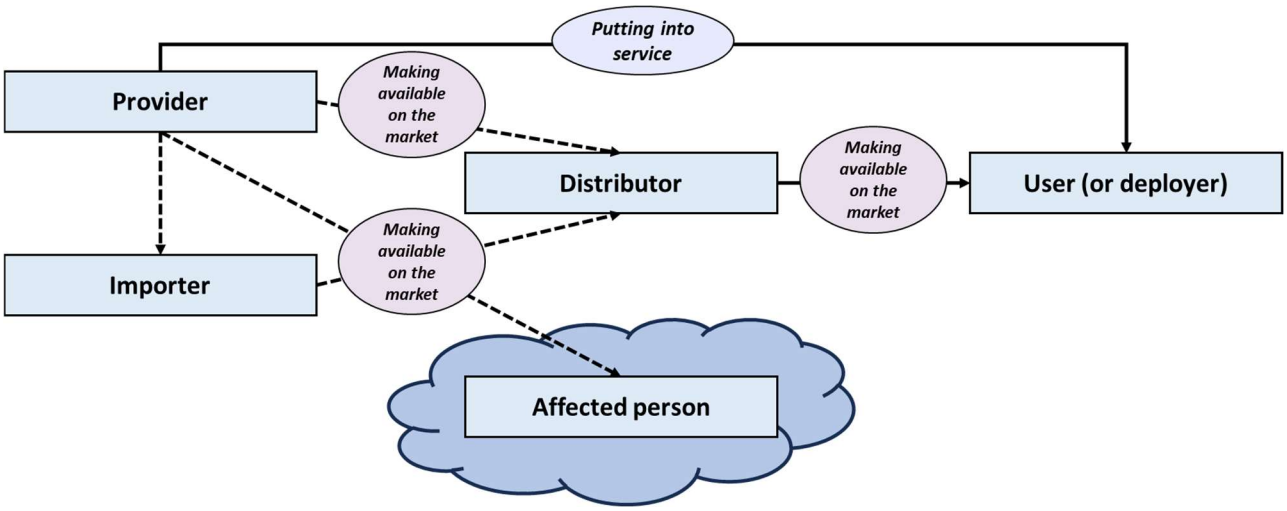


Figure 2 Relationships between the different actors under the AI Act

[23] AI Act proposal, explanatory memorandum, p. 12.
[24] There may, however, be differences between the positions of the Parliament and those of the Commission and the Council on these points. The scope of the Parliament's text is indeed slightly broader. The importance of these changes is, however, relative in the context of TEF-Health.
[25] The Commission and the Council refers both to the wording "user" when the Parliament prefers the wording "deployer" for the same concept but the definitions of this concept are strictly identical in all three positions.
[26] AI Act proposal, art. 2(1) (a) to (c).
[27] AI Act proposal, art. 3(8).
[28] The notion of "affected person" is proposed by the Parliament but it's not existing in the Commission's and the Council positions. See Parliament position's, art. 3(8a), p. 114.

The *provider* is any entity[29] that develops an AI system or that has an AI system developed with a view to placing it on the market or putting it into service *under its own name or trademark*[30].

- It may *place the AI system on the market*, i.e., make it available on the EU market for the first time[31]. The notion of "making available" "means any supply of an AI system for distribution or use on the Union market in the course of a commercial activity, whether in return for payment or free of charge" [32].
- The provider may also directly *put the system into service*, i.e. supply it "for first use directly to the user or for own use on the Union market for its intended purpose"[33].

It is important to stress that the concept of "putting into service" only targets the "user" within the meaning of the AI Act, i.e. the professional user (the "*user*" or "*deployer*") [34]. It means that the direct provision of an AI system to consumers (i.e. natural persons acting for personal purposes, such as patients directly using an AI system) within a Business to Consumer (B2C) relationship, is not covered. Indeed, "*user*" "means any natural or legal person, public authority, agency or other body using an AI system under its authority, *except where the AI system is used in the course of a personal non-professional activity*"[35] (highlighted by the author).

When the provider is established outside the EU, it may work with an *importer*, i.e., another entity that puts the system bearing the name or trademark of the provider on the market[36]. Of course, the supply chain may also include one or more *distributors* who act as a relay for the provider or importer and make the AI system available on the EU market without affecting its properties[37].

Finally, the notion of *affected person* refers to any person (or group of persons) subject to or affected in one way or another by the AI system[38]. This notion is very broad because of the choice made by the European Parliament to refer to the term "affected". One can assume that this primarily covers the end user (e.g., the patient in the field of healthcare activities). But it may also include people who are affected by a decision taken on the basis of an investigation made with or by an AI system. This would be the case, for example, of a person who was considered by an AI system not to be a priority for a transplant.

The fact that the patients are not included in the notion of "users" might have impacts in practice. At least, it will mean that the patients are not subject to the obligations applicable to the users in relation with high-risk AI systems[39], which may be of importance.

---

[29] It may be a natural person, a legal entity or a public authority, for example.
[30] AI Act proposal, art. 3(2).
[31] AI Act proposal, art. 3(9).
[32] AI Act proposal, art. 3(10).
[33] AI Act proposal, art. 3(11).
[34] We remind the term "user" is the one chosen by the Commission. The Parliament used the exact same definition but proposed to replace the reference to the "user" by a reference to the "deployer". See Parliament position, art. 3(4), p. 114.
[35] AI Act proposal, art. 3(4).
[36] AI Act proposal, art. 3(6).
[37] AI Act proposal, art. 3(7).
[38] Parliament position, art. 3(8a), p. 114.
[39] A. KISELEVA, "AI as a Medical Device: Between the Medical Devices Framework and the General AI Regulation" in H. Jacquemin (dir.), *Time to Reshape the Digital Society*, Brussels, Larcier, 2021, p. 502.

Finally, the AI Act proposal states that "a body that performs third-party conformity assessment activities, including testing, certification and inspection" is a "*conformity assessment body*"[40]. This definition is also important as it may have an impact on the TEF Health project, as explained hereafter[41].

1.3.3 Application to TEF Health

TEF-Health Consortium or its partners will not be the *provider(s)* of the AI systems developed through the use of the services offered by the Consortium (unless if for the provision of TEF-Health services an AI system is developed by a partner of the Consortium). Instead, the SMEs using TEF-Health services might qualify as *providers* of AI systems. In any case, through TEF-Health, the objective of the Consortium is to help them to comply with all the applicable requirements, that will be imposed by the AI Act proposal.

The following figure aims to present at which stage of the development of a product thanks to TEF-Health services the AI Act may apply.

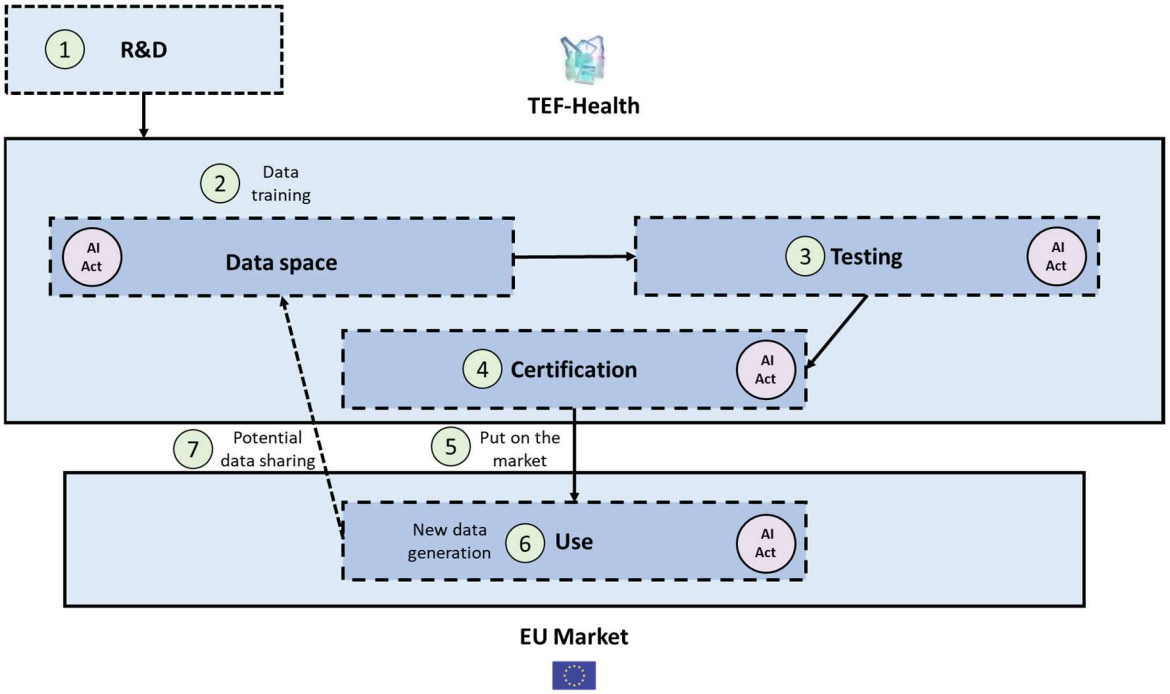


Figure 3 Potential application of the AI Act to the activities of TEF-Health

[40] AI Act proposal, art. 3(21).
[41] See *infra,* point 1.4.4.

For instance, the AI Act proposal states that some of its requirements are solely applicable to AI systems that present a high-level of risk. Some of these requirements, applicable to the AI product itself, are directly related to testing. Therefore, the Consortium precisely aims to help TEF-Health users (the SMEs) comply with these requirements[42].

Finally, there is a possibility that TEF-Health, or some particular partners, will be considered as conformity assessment body/bodies. These bodies must comply with specific requirements[43].

1.4 Requirements to be complied with

As previously mentioned, the AI Act proposal follows a risk-based approach[44].This approach implies that the requirements will be higher or lower depending on the level of risk that AI systems present to individuals and to their fundamental rights. Yet, it should be noted that the European Parliament proposed to additionally impose a set of requirements to some specific AI systems (i.e., generative AI), regardless of the risk-based approach[45].

The following figure presents the levels of requirements depending on the AI systems considered.

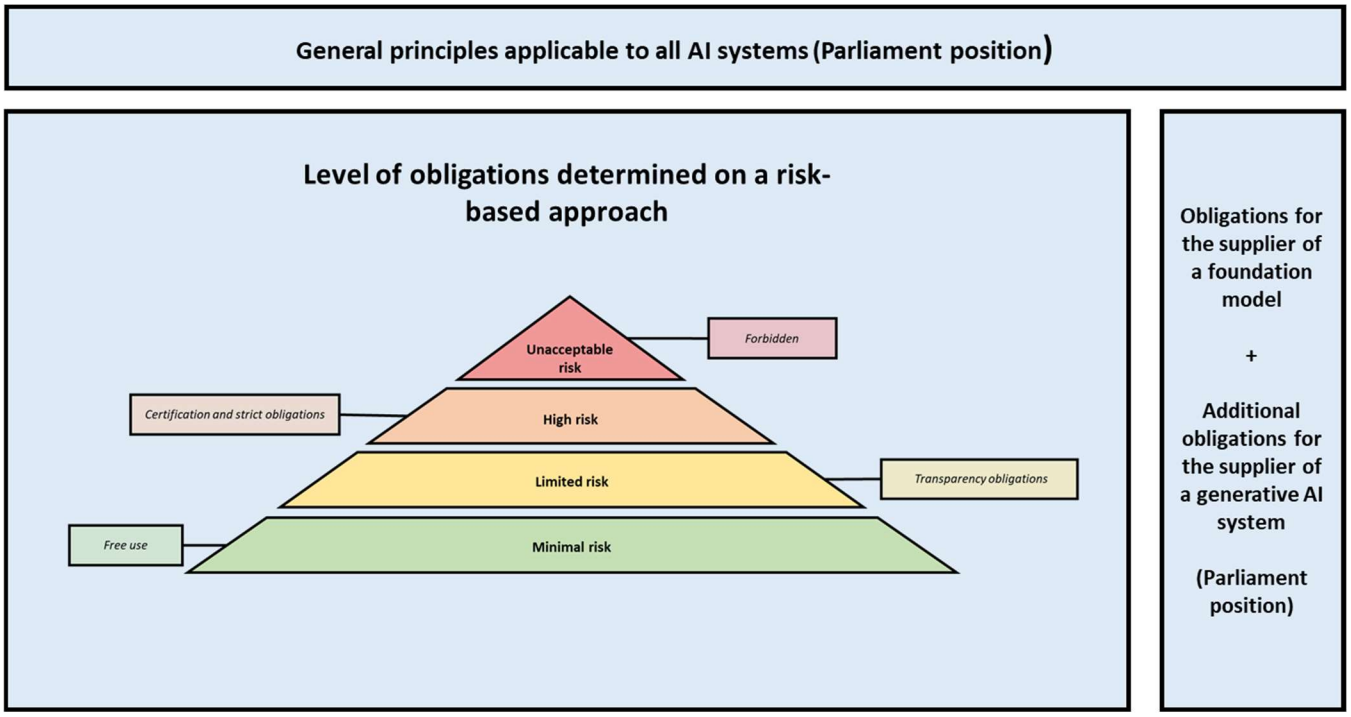


Figure 4 Modelized general structure of the AI Act

[42] See, for example, AI Act proposal, art. 9(5).
[43] Regarding these requirements, see *infra*, point 1.4.4.
[44] AI Act proposal, explanatory memorandum, p. 12.
[45] Regarding this point, see *infra*, point 1.4.2.1.

1.4.1 Forbidden AI systems

At the top of the risk pyramid, which is schematized in figure 4, are the AI systems that generate an unacceptable risk and will therefore be forbidden[46]. We do not go into detail about the content of the list of systems that will be concerned, which is subject of differences between the positions expressed by the three EU institutions[47].

For instance, the AI Act proposal prohibits the AI system "[...] that deploys subliminal techniques beyond a person's consciousness in order to materially distort a person's behaviour in a manner that causes or is likely to cause that person or another person physical or psychological harm"[48]. It also forbids the AI system "[...] that exploits any of the vulnerabilities of a specific group of persons due to their age, physical or mental disability, in order to materially distort the behaviour of a person pertaining to that group in a manner that causes or is likely to cause that person or another person physical or psychological harm"[49].

1.4.2 Authorised regulated AI systems

1.4.2.1 General principles applying to all AI systems

The Parliament wants all operators[50] falling under the AI Act to make their *best efforts* to develop and use AI systems[51], regardless of the level of risk they present, in accordance with six general principles[52].

The idea to impose such general principles is not to be found in the positions of the Commission and the Council. It remains to be seen whether it will be included in the final text.

Should this be the case, these principles are based on the seven requirements previously stressed by the HLEG[53], and are the following:

(i) human agency and oversight;
(ii) technical robustness and safety;
(iii) privacy and data governance;
(iv) transparency;

---

[46] AI Act proposal, art. 5.
[47] For example, the Commission and the Council want to ban real-time remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement. But they also want to implement exemption permitting to authorise such type of AI systems in certain circumstances. On the contrary, the Parliament goes further and wants a total ban of this practice when authorising only "post" remote biometric identification systems provided that it has been subject to a pre-judicial authorisation; See AI Act proposal, art. 5(1) (d); Council position's, art. 5(1) (d) and art. 5(2) to (4); Parliament position, art. 5 (1)(d) and (dd), pp. 133-135.
[48] AI Act proposal, art. 5(a).
[49] AI Act proposal, art. 5(b).
[50] Which includes all the actors previously mentioned.
[51] That do not fall within the prohibition mentioned in the previous point.
[52] Parliament position, art. 4a(1), pp. 128-130.
[53] Regarding that point, see *supra*, point 1.2.1.

(v) diversity, non-discrimination, and fairness; and
(vi) social and environmental well-being.

For example, Article 4a(c) of the Parliament position states that all AI systems must "be developed and used in compliance with existing privacy and data protection rules, while processing data that must meet high standards in terms of quality and integrity" (i.e., privacy and data governance principle). It means, among others, (i) that the data must be examined in view of possible biases, or (ii) that the data must be relevant, representative, free of errors and complete, also with regard to the patients to which the AI systems are intended to be applied[54].

Paragraph (d) of the same Article also states that "all AI systems shall be developed and used in a way that allows appropriate traceability and explainability, while making humans aware that they communicate or interact with an AI system as well as duly informing users of the capabilities and limitations of that AI system and affected persons about their rights" (i.e., transparency principle). It means that the users must be given sufficiently clear and understandable information in order to be able to interpret the system's output and use it appropriately[55].

As the provision refers to the terms "best efforts", the compliance with these principles should probably be considered an obligation of "means". Operators would have to demonstrate that they made reasonable efforts, in the context of their organisation, to respect them. The challenge will therefore be to decide what is "reasonable" in the field of TEF-Health project.

1.4.2.2 High-risk AI systems

The second layer of the risk pyramid relates to "high-risk" AI systems[56]. Examples of such high-risks AI systems are "AI systems intended to be used for recruitment or selection of natural persons, notably for advertising vacancies, screening or filtering applications, evaluating candidates in the course of interviews or tests"[57].

The AI system that is considered high-risk will be subject to strict obligations.

The system itself will have to meet requirements on data and data governance[58], risk-management systems[59], technical documentation[60], record-keeping[61], transparency[62], human oversight[63], accuracy, robustness and cybersecurity[64]. For example: "The technical documentation of a high-risk AI system shall be drawn up before that system is placed on the

[54] K.N. VOKINGER and U. GASSER, "Regulating AI in medicine in the United States and Europe", *Nature Machine Intelligence*, N°3, 2021, pp. 738-739.
[55] *Ibid*.
[56] AI Act proposal, art. 6 to 51.
[57] AI Act proposal, Annex III, point 4 (a).
[58] AI Act proposal, art. 10.
[59] AI Act proposal, art. 9.
[60] AI Act proposal, art. 11.
[61] AI Act proposal, art. 12.
[62] AI Act proposal, art. 13.
[63] AI Act proposal, art. 14.
[64] AI Act proposal, art. 15.

market or put into service and shall be kept up-to date [...]"[65]. It is also stated that: "High-risk AI systems shall be designed and developed in such a way that they achieve, in the light of their intended purpose, an appropriate level of accuracy, robustness and cybersecurity, and perform consistently in those respects throughout their lifecycle"[66]. The provider will have to ensure that these obligations are met, by design[67]. Therefore, he must have a quality management system in place[68], draw up the technical documentation of the system[69], keep the logs[70], *etc*.

When the AI system is part of or is a medical device, the manufacturer of the device is the one who must comply with the obligations imposed on providers under the AI Act[71]. This is important in the field of TEF-Health since TEF-Health users (the SMEs) may – in some situations[72] – be considered cumulatively as (i) manufacturers within the meaning of the medical devices regulations[73], and as (ii) providers within the meaning of the AI Act.

Besides, the authorised representative (if any)[74] will have to respect specific obligations[75] as well as the user, the distributor or the importer[76].

[65] AI Act proposal, art. 11(1).
[66] AI Act proposal, art. 15(1).
[67] AI Act proposal, art. 16(a).
[68] AI Act proposal, art. 16(b) and art. 17.
[69] AI Act proposal, art. 16(c).
[70] When under their control; see AI Act proposal, art. 16(d).
[71] AI Act proposal, art. 24.
[72] Regarding that point, see *infra,* part 2.2.
[73] This includes the 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, *O.J.*, L 117/1, 5 May 2017 (hereafter "Medical Devices Regulation" or "MDR") and the Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU, *O.J.*, L 117/176, 5 May 2017 (hereafter "In Vitro Medical Devices Regulation").
[74] Which shall be designated by the providers established outside the EU when an importer cannot be identified; AI Act proposal, art. 25.
[75] AI Act proposal, art. 25.
[76] AI Act proposal, art. 26 to 29.

The figure 5 below details more precisely the requirements each actor must follow.

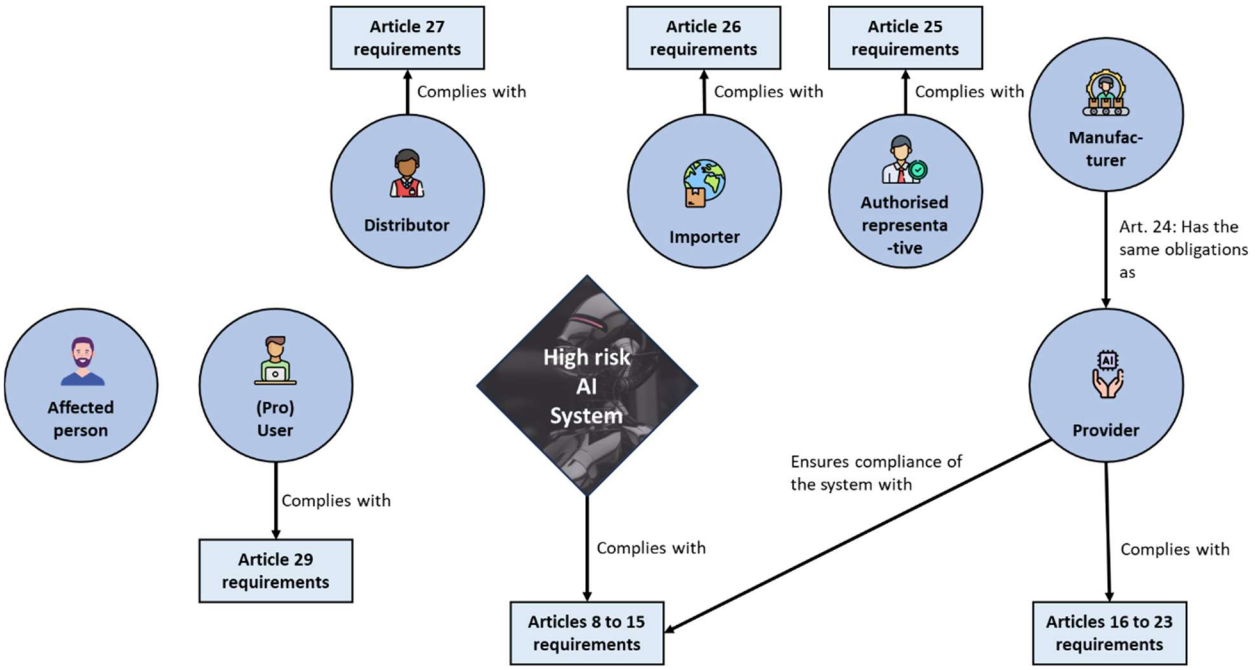


Figure 5 High-risk AI systems requirements applicable to each actor

Finally, the providers of high-risk AI systems will have to ensure that a conformity assessment has been carried out before placing them on the market[77]. The AI Act proposal provides specific rules with this regard[78]. Those rules are similar to the ones applicable to the products that fall under the scope of the Medical Devices Regulation.

The following figure identifies the rules applicable to the product depending on its specificities.

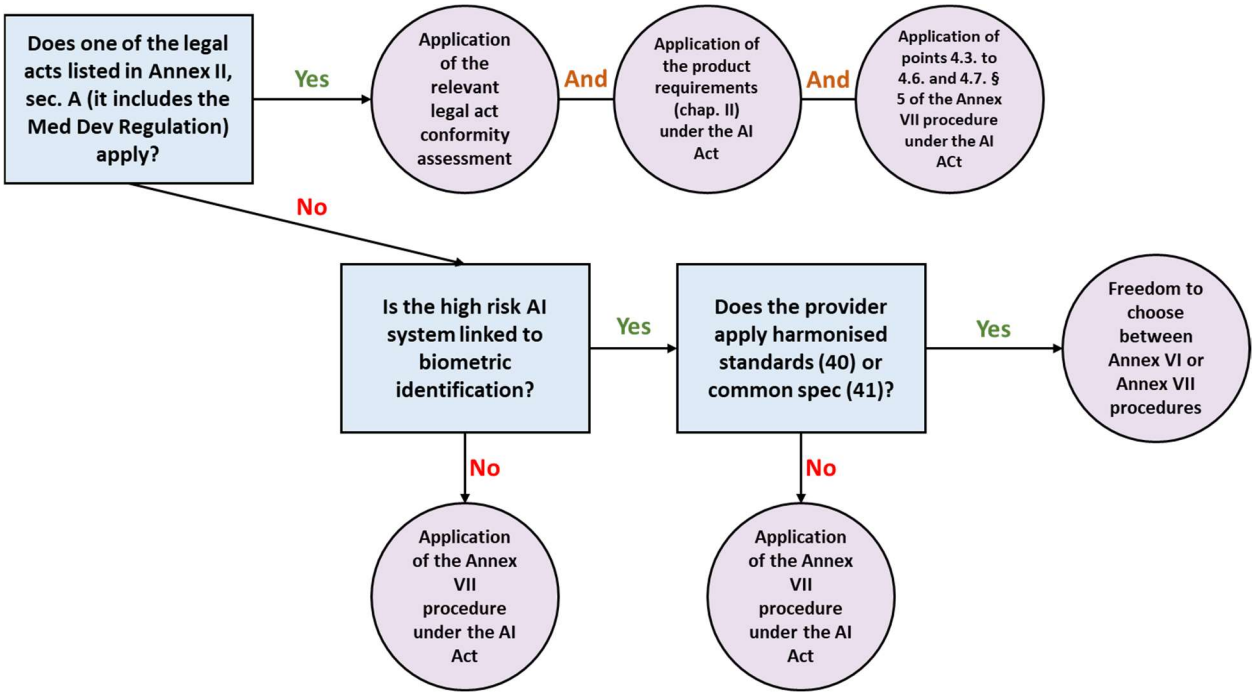


Figure 6 Flow chart related to the type of high-risk AI system conformity assessment which has to be performed

There are two main procedures to perform conformity assessments: the one contained into Annex VI (hereafter, P.VI) and the one contained into Annex VII (hereafter, P.VII). P.VI is relatively simple and involves no third-party intervention.

On the contrary, P.VII is much more complex and requires third-party examinations. It implies, for example, the assessment of the quality management system[79] or the examination of the documentation established by the provider[80] by a notified body. Article 43 gives precisions regarding the circumstances in which one or another of the procedures must be followed.

[77] AI Act proposal, art. 19.
[78] AI Act proposal, art. 43.
[79] AI Act proposal, Annex VII, point 3.2.
[80] AI Act proposal, Annex VII, point 4.3.

The provider must assess whether one of the legal acts listed in the Second Annex, Section A of the AI Act proposal (including Medical Devices Regulation) applies to the AI system it seeks to put on the market. If one of those acts applies, the provider must follow the conformity assessment procedure under the relevant legal act[81]. In addition, it has to ensure that the requirements directly applicable to the high-risk AI system under the AI Act are met[82]. Finally, it has also to follow the requirements provided in points 4.3. to 4.6. and in paragraph 5 of point 4.7. of the Annex VII procedure under the AI Act[83].

In the field of TEF-Health project, it is then important to note that the provider of the AI system which is also a medical device, or is a safety component of a medical device, will not have to comply with both the complete conformity assessment procedure laid down in the future AI Act and the one laid down in Medical Devices Regulation. It will be required to comply only with the one set out in Medical Devices Regulation and, in addition, with the requirements provided in points 4.3. to 4.6. and in paragraph 5 of point 4.7. of the Annex VII procedure under the AI Act. Regarding the precise articulation between AI Act proposal and MDR, further analysis must be done. A separate documentation will be drafted and communicated to the Consortium with this regard at a further stage.

When the high-risk AI system does not fall within one of the legislations listed by Annex II[84], the provider must assess whether it is intended to be used for the 'real-time' or 'post' remote biometric identification of natural persons[85]. If this is not the case, the provider will have to apply the Annex VII procedure[86]. Conversely, when real-time' or 'post' remote biometric identification of natural persons takes place, the provider will have to assess whether it has applied harmonised standards mentioned in article 40 or common specifications mentioned in Article 41 (provided that they exist)[87]. In the case the provider has applied such standards or specifications, it will have the right to choose between the Annex VII procedure and the simplified internal procedure established in Annex VI[88]. If it has not, it will be obliged to apply the Annex VII procedure[89].

[81] AI Act proposal, art. 43(3).
[82] AI Act proposal, art. 43(3).
[83] AI Act proposal, art. 43(3). Such requirements are, among others, related to the examination of the AI system documentation by the notified body and to the access to the source code that may be granted to such a notified body in some circumstances.
[84] Note that, in addition to the Medical Devices Regulation, this list contains, e.g., the Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC (*O.J.*, L153, 22 May 2014, p. 62) or the Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU (*O.J.*, L 117, 5 May 2017, p. 176); The Consortium shall therefore pay attention to the exact content of this Annex.
[85] AI Act proposal, art. 43(1) and Annex III, point 1.
[86] AI Act proposal, art. 43(2).
[87] AI Act proposal, art. 43(1).
[88] AI Act proposal, art. 43(1).
[89] AI Act proposal, art. 43(1).

1.4.2.3 *Limited-risk AI systems*

The third layer of the risk pyramid encompasses AI systems which give rise to certain specific but limited risks of manipulation[90]. Examples include "AI systems intended to interact with natural persons"[91], such as chatbots.

Unlike high-risk AI systems, they are not highly regulated. However, they must comply with certain transparency obligations[92]. For instance, the provider of AI systems intended to interact with natural persons must ensure that "natural persons are informed that they are interacting with an AI system"[93].

Emotion recognition system and biometric categorisation system are two other types of limited-risk AI systems. It must be ensured that natural persons facing them are informed of the operation performed by the systems[94].

The "AI system that generates or manipulates image, audio or video content that appreciably resembles existing persons, objects, places or other entities or events and would falsely appear to a person to be authentic or truthful ('deep fake') [...]"[95] is also subject to transparency requirements. The provider must disclose that the content produced through the deep fake system has been artificially generated or manipulated[96].

1.4.2.4 *Negligible-risk AI systems*

Finally, all AI systems that do not fall within one of the above categories are considered to generate minimal risk. They are therefore not subject to any obligation under the Commission and Council positions. As regards Parliament position, see above about general principles[97] and below about foundation models and generative AI[98].

1.4.3 Regulating foundation models and generative AI?

The European Parliament wants to include a new provision in the AI Act, to regulate *foundation models* and *generative AI* independently from the risk pyramid detailed above[99].

The *foundation model* is defined as "an AI system model that is trained on broad data at scale, is designed for generality of output, and can be adapted to a wide range of distinctive tasks"[100], whereas *generative AI* is defined as "foundation models used in AI systems specifically intended

---

[90] AI Act proposal, explanatory memorandum, p. 14.
[91] AI Act proposal, art. 52(1).
[92] AI Act proposal, art. 52.
[93] AI Act proposal, art. 52(1).
[94] AI Act proposal, art. 52(2).
[95] AI Act proposal, art. 42(3).
[96] AI Act proposal, art. 42(3).
[97] Regarding that point, see *supra*, point 1.4.2.1.
[98] Regarding that point, see *infra*, point 1.4.3.
[99] Parliament position, art. 28b, pp. 198-201.
[100] Parliament position, art. 3(1) (1c), p. 120.

to generate, with varying levels of autonomy, content such as complex text, images, audio, or video" [101].

The provider of a foundation model would have to respect several obligations, which are similar to the one applicable to high-risk AI systems[102]. It should also be noted that the obligations applicable to *foundation models* would be further strengthened vis-à-vis providers of *generative AI systems*[103].

This may be relevant for TEF-Health project because of the broad definition of the notions of *foundation model* and *generative AI*. For instance, there may be situations in which a TEF-Health user (a SME) would like to develop a *generative AI* that aids medical diagnosis decisions. In this case, the SME would be the provider of the *generative AI*. The Consortium or some of its partners will have to help it to comply with the requirements set up by the AI Act in this regard. Those requirements are, for example, related to testing[104] of the quality of the training datasets[105].

1.4.4 Requirements applying to conformity assessment bodies

Conformity assessment bodies must comply with the requirements laid down in Article 33 of the AI Act proposal, which are related, among others, to their organisational structure[106], their independence vis-à-vis the provider of a high-risk AI system in relation to which it performs conformity assessment activities[107], their ability to provide documentation[108] and to establish processes[109] or the level of internal competences they must have[110].

Such conformity assessment bodies must also apply for notification to a notifying authority[111], designated or established by a Member State[112], by following a strict notification procedure[113] in order to be able to deliver their services.

1.5 Regulatory sandboxes

The AI Act proposal aims to support innovative measures, including regulatory sandboxes. Indeed, in order to allow testing of the regulatory framework, the AI Act proposal "[...] encourages national competent authorities to set up regulatory sandboxes and sets a basic framework in terms of governance, supervision and liability [...]"[114]. The European Commission stressed that "Artificial intelligence [...] requires novel forms of regulatory oversight and a safe space for

[101] Parliament position, art. 28b (4), pp. 200-201.
[102] See Parliament position, art. 28b, pp. 198-201.
[103] Parliament position, art. 28b (4), p. 200-201.
[104] Parliament position, art. 28b (2) (a), p. 199.
[105] Parliament position, art. 28b (2) (b), p. 199.
[106] AI Act proposal, art. 33(3).
[107] AI Act proposal, art. 33(4).
[108] AI Act proposal, art. 33(12).
[109] AI Act proposal, art. 33(7).
[110] AI Act proposal, art. 33(10).
[111] AI Act proposal, art. 31.
[112] AI Act proposal, art. 30(1).
[113] AI Act proposal, art. 32.
[114] AI Act proposal, explanatory memorandum, p. 15.

experimentation [...]. [N]ational competent authorities from one or more Member States should be encouraged to establish artificial intelligence regulatory sandboxes to facilitate the development and testing of innovative AI systems under strict regulatory oversight before these systems are placed on the market or otherwise put into service"[115].

Concretely, these regulatory sandboxes will be established and controlled by one or more competent authorities (e.g., notifying authorities[116]) or by the European Data Protection Supervisor[117]. In these sandboxes, "[...] personal data lawfully collected for other purposes shall be processed for the purposes of developing and testing certain innovative AI systems [...]"[118] under the conditions detailed in Article 54. The systems must, for example, be developed for safeguarding public interest in one of the areas exhaustively listed within the provision[119]. Complete and detailed descriptions of the process and rationale behind the training, testing and validation of the AI systems must be kept together with the testing results as part of the technical documentation[120].

The eligibility criteria and the procedure for the application, selection, and participation to a regulatory sandbox will have to be set out in implementing acts adopted by the European Commission with the assistance of a committee[121], after the entry into force of the AI Act[122].

This topic is important for TEF-Health since one the main objectives of the Consortium is to establish an agile certification process for medical devices including AI[123]. As stated, in the Grant Agreement Annex: "A key component of an agile certification process are regulatory sandboxes where all relevant stakeholders (such as AI developers, companies, public authorities, notified bodies, clinical experts, legal experts, and citizens) can work together to create innovative testing and validation tools for trustworthy AI in medical devices for specific use-cases"[124]. It means that the Consortium will probably have to offer its services (e.g., testing) in the environment provided by regulatory sandboxes that will be established by the competent authorities. Consequently, TEF-Health will have to focus on the content of the implementing acts that will be adopted later on in the legislative process.

[115] AI Act proposal, recital 71.
[116] Under the AI Act proposal, art. 3 (43) defines the "national competent authority" as the "the national supervisory authority, the notifying authority and the market surveillance authority".
[117] AI Act proposal, art. 53(1).
[118] AI Act proposal, art. 54(1).
[119] Two examples of such area are "public safety and public health, including disease prevention, control and treatment" and "a high level of protection and improvement of the quality of the environment"; see AI Act proposal, art. 54(1) (a) (ii) and (iii).
[120] AI Act proposal, art. 54(1) (i).
[121] AI Act proposal, art. 53(6) and art. 74(1).
[122] AI Act proposal, art. 53(6).
[123] Grant Agreement, Annex I – Description of the action (part B) p. 9.
[124] Grant Agreement, Annex I – Description of the action (part B), pp. 9-10.

2 Medical Devices Regulation (MDR)

2.1 Context and purposes of the regulation

The European regulation on medical devices[125] has been adopted on the 5th of April 2017 and came into force on the 21st of May 2021 (hereafter "MDR"). This regulation repealed and replaced the directives 90/385/CEE and 93/42/CEE. In addition to MDR, there is also a regulation of 5 April 2017 on *in vitro* diagnostic medical devices which repealed Directive 98/75/EC and Commission Decision 2010/227/EU[126]. This regulation could also apply to TEF-Health project if in vitro medical devices are effectively developed in the context of the project. Nevertheless, this regulation will not be analyzed in this document for reasons of efficiency and readability.

The purpose of MDR is to provide a harmonized regulation concerning the placing on the market, making available on the market or putting into service of medical devices for human use and accessories for such devices in the European Union.

MDR also applies to clinical investigations concerning such medical devices and accessories that are conducted in the European Union[127].

Since the use of medical devices can entail specific risks, MDR establishes a conformity assessment procedure to evaluate the security and the safety of the product and minimize the risks for patients.

MDR has three main objectives[128] :

- To ensure and reinforce *patient safety* by imposing strict and rigorous quality and safety standards for medical devices (Annex I), in particular by introducing enhanced conformity assessment procedures both before they are placed on the market and after they have been certified and placed on the market.

- To reinforce *public confidence* by guaranteeing the *efficiency, quality and competence of notified bodies* through the introduction of specific rules and procedures concerning their designation, control and supervision.

- To implement *harmonized and adapted regulation* throughout the European Union to encourage innovation in the field of medical devices, notably by updating the regulation to keep up with medical and technological developments.

---

[125] Regulation EU) 2017/745 of the European Parliament and oft he 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, L 117/1, *J.O.*, 5 Mai 2017.
[126] Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU, L 117/176, *J.O.,* 5 May 2017.
[127] MDR, art. 1.
[128] MDR, recital 4; O. MIGNOLET, A. BRUYNDONCKX, V. MUROVEC., "*Les "implant files": point de vue de juristes sur un travail journalistique au regard des règles applicables aux dispositifs médicaux implantables en Europe (et en particulier en Belgique)* », *Revue de droit de la santé*, 2021/2, p. 92.

MDR is central to TEF-Health project, which aims notably to implement evaluation activities to facilitate innovation and market access for trustworthy technologies considering the applicable regulatory requirements, such as the certification procedures to be complied with to put a medical device on the market[129].

If MDR applies at every step of the lifecycle of a medical device, TEF-Health project specifically concerns the two following fundamental steps:
- *Testing process,* by providing testing infrastructures to TEF-Health users (the SMEs) which have already developed a prototype of medical device (WP3: physical testing centers and WP4: virtual testing centers) and by setting up consulting services for clinical trials, AI and robotics in healthcare (WP8: Clinic, AI and Robotics Competence);
- *Certification process,* by establishing standards for agile certification process (WP6: standards and quality), developing reference process for 'agile certification' of medical devices according to MDR (WP7: certification).

This following figure shows the different stages in a product's life cycle, identifying where the TEF-Health project will come into play.

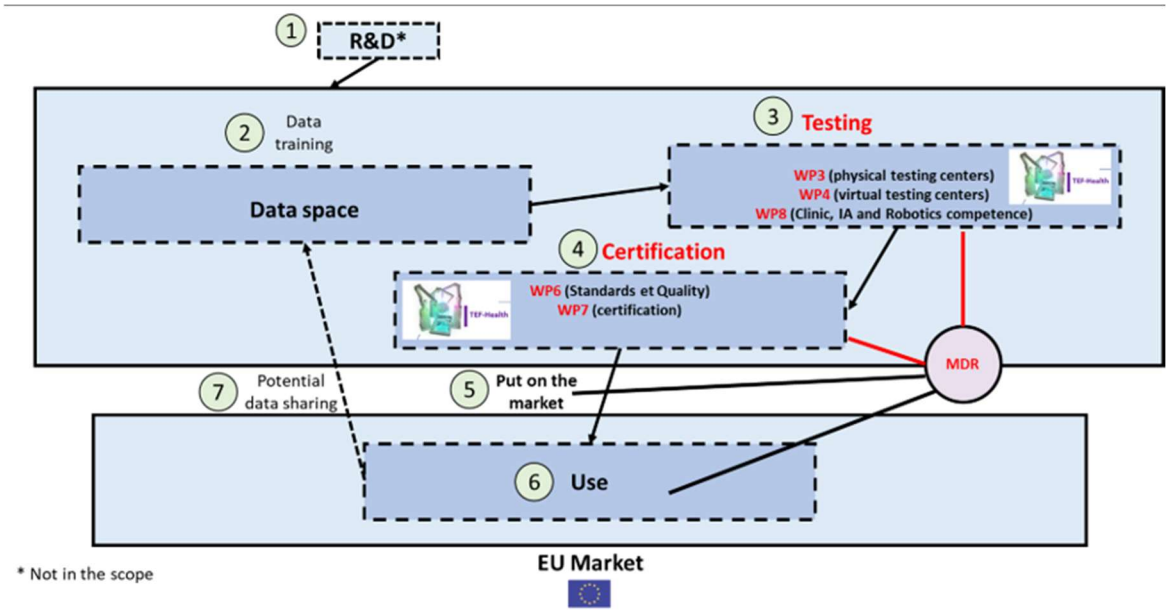


Figure 7 Lifecycle of a medical device product

[129] Grant agreement, Annex 1 - Description of the action (part A), Project Summary, p. 3 ; P. RITTER., "€60 million committed to establish AI and robotics in healthcare", available online : €60 million committed to establish AI and robotics in healthcare: Charité – Universitätsmedizin Berlin (charite.de), 2 January 2023.

2.2 Scope and actors involved

2.2.1 Regulated product: medical devices

2.2.1.1 Qualification

To find out whether MDR applies, the first question the manufacturer of the product must solve is whether the product in question is a medical device or not. Indeed, MDR will only apply if the product is qualified as a medical device or a medical device software.

Medical device

According to article 2 of MDR, 'medical device' means:

"Any instrument, apparatus, appliance, *software*, implant, reagent, material or other article intended by the manufacturer to be used, alone or in combination, for human beings for one or more of the following specific medical purposes:

- Diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease,
- Diagnosis, monitoring, treatment, alleviation of, or compensation for, an injury or disability,
- Investigation, replacement or modification of the anatomy or of a physiological or pathological process or state,
- Providing information by means of in vitro examination of specimens derived from the human body, including organ, blood and tissue donations

And which does not achieve its principal intended action by pharmacological, immunological or metabolic means, in or on the human body, but which may be assisted in its function by such means.

The following products shall also be deemed to be medical device:
- Devices for the control or support of conception;
- Products specifically intended for the cleaning, disinfection or sterilization of devices as referred to in Article 1(4) and of those referred to in the first paragraph of this point".

(highlighted by the author)

This is a broad definition, encompassing devices that pose no particular risk to patients, such as compresses or crutches, as well as more risky, invasive devices, such as breast implants, pacemakers, etc.

It must be noted that it is expressly mentioned that a software can be qualified as a medical device. Such an assertion was confirmed by the European Court of Justice[130].

[130] ECJ, case *Syndicat national de l'industrie des technologies médicales et Philips France v. Premier ministre, Ministre des affaires sociales et de la Santé*, 7 December 2017, C-329/16, EU:C:2017:947, point 34 : « It follows that software, of which at least one of the functions makes it possible to use patient-specific data for the purposes, inter alia, of detecting contraindications, drug interactions and excessive doses, is, in respect of that function, a medical device, within the meaning of Article 1(2)(a) of Directive 93/42, even if such software does not act directly in or on the human body".

Services that will be offered by TEF-Health Consortium are especially concerned by MDR because they aim to implement evaluation activities to facilitate and accelerate the validation and certification of *AI and robotics in medical devices*. The medical devices covered by TEF-Health project are products such as, for example, surgical and nursing robots[131], implant-based telemonitoring of heart insufficiencies with Biotronik[132], etc.

Medical device software

In the context of TEF-Health project, special attention must be paid to "Medical device Software". Indeed, according to EU legislation and relevant guidelines, it appears that AI can be deemed as software[133].

"Medical device software" is defined as a software that is intended to be used, *alone or in combination,* for a purpose as specified in the definition of a "medical device" in MDR[134]. A medical device software can exist by itself and have its own intended medical purpose, even if it is incorporated in a hardware medical device that it drives or influences[135].

It is important to emphasize that not all softwares used in healthcare sector are qualified as medical device[136]. According to guidance on medical device software established by the Medical Device Coordination Group[137], to be considered as a medical device, a software has to perform an action on data, or performs an action beyond storage, archival, communication, simple search, or lossless compression (i.e. using a compression procedure that allows the exact reconstruction of the original data)[138]. In other words, software that are intended only to transfer, store, convert, format, archive data are not qualified as medical devices in themselves[139].

---

[131] *Ibid*.
[132] European Commission, Grant Agreement, Annex 1 - Description of the action (part A), List of Work Packages, p. 16.
[133] A. KISELEVA., « AI as a Medical Device: Is It Enough to Ensure Performance Transparency and Accountability in Healthcare?", *European Pharmaceutical Law Review*, 1/2020, p. 9.
[134] Medical Device Coordination Group Document, Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR, MDCG 2019-11, available on: https://health.ec.europa.eu/system/files/2020-09/md_mdcg_2019_11_guidance_qualification_classification_software_en_0.pdf, October 2019, pp. 6-7.
[135] For example, melanoma image analysis software intended to drive a near-infrared laser light scanner or medical device software intended to measure and transmit blood glucose levels, calculate insulin dose required and drive the insulin pump to administer the calculated dosage (Medical Device Coordination Group Document, Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR, MDCG 2019-11, *op. cit.*, p. 7, note 2)
[136] *Ibid.*; Are not considered as having a medical purpose and, *de facto*, as medical device software software intended for non-medical purpose, such as invoicing or staff planning.
[137] The Medical Device Coordination Group ("MDCG") is established by Article 103 of MDR. The MDCG is composed of representatives of all Member States and it is chaired by a representative of the European Commission.
[138] Medical Device Coordination Group Document, Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR, MDCG 2019-11, *op. cit.*, p. 8 (decision step 3).
[139] *Ibid.*, p. 19.

The key element is to determine if the creation or modification of medical information processed, analyzed, created or modified by the software is governed by *a medical intended purpose*[140].

Software driving or influencing the use of a medical device

If a software is intended to drive or influences the use of a hardware medical device but has not, on its own, a medical purpose, the software is qualified as "software driving or influencing the use of a medical device" and must be considered as a component or an accessory of the hardware medical device concerned[141].

2.2.1.2 Classification

Generalities

Medical devices are divided into four classes: Class I, Class IIa, Class IIb, and Class III.

The classification of a medical device as belonging to one of these categories is based on its intended use and on the risks inherent in it. The classification must be carried out by the manufacturer of the device.

As showed in Figure 8 below, Class I covers medical devices that pose no particular risk to patients, while Class III covers medical devices that present a high risk to patients.

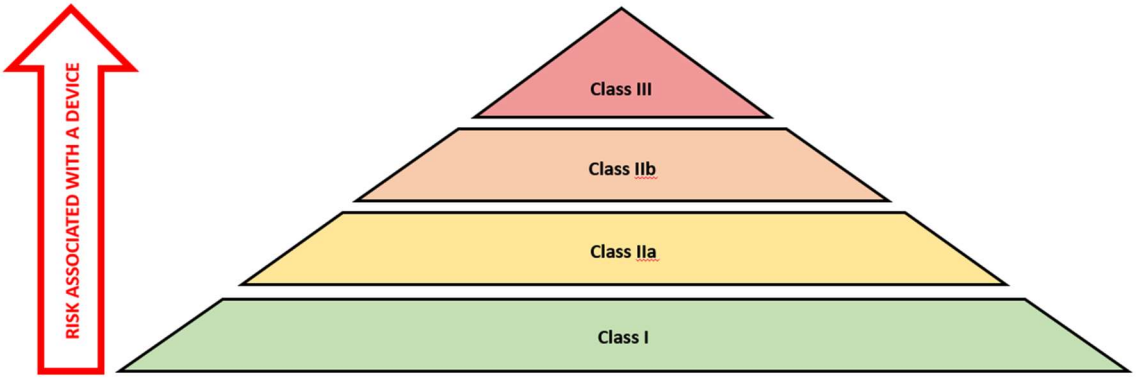


Figure 8 Classification of the risk of a medical device

The classification rules are set out in *Annex VIII, chapter III of MDR*.

The classification of a medical device determines the applicable conformity assessment procedure and the corresponding requirements to be complied with. Logically, manufacturers'

[140] *Ibid.*, p. 6.
[141] *Ibid.*, p. 6, point 3.3.

pre-marketing and post-marketing obligations[142] are proportionate to the risk class of the devices they produce. The higher the class and the risk to the patient are, the stricter and more rigorous the applicable rules are.

Combination between medical device software and medical device hardware

When a device combines hardware (medical device product) and software (medical device software), special attention must be paid to rule 3.3 of Annex VII of MDR.

First, *rule 3.2 of Annex VII* provides that "if the device in question is intended to be used in combination with another device, the classification rules shall apply separately to each of the devices".

Then, *rule 3.3 of Annex VIII* clarifies the regime applicable to software which drives or influences the use of a device by providing that *"software, which drives a device or influences the use of a device*, shall fall within the same class as the device" (highlighted by the author). It implies that a software which has not a medical purpose, but which drives or influences a hardware medical device has to be classified in the same class of the medical device he drives or influences.

Finally, *rule 3.3 of Annex VIII* clarifies the sort of independent software by providing that "if the software is independent of any other device, it shall be classified in its own rights". It concerns, for example, medical applications which are qualified as medical device software, but which works independently from another medical device.

The application of those rules implies that if a software is qualified as a medical device software because it has its own medical purpose, this medical device software has to be qualified on its own, even if it is used in combination with a hardware medical device.

Medical Device Software

If the software is considered as a medical device software (if the software has a medical purpose on its own), the classification of this medical device is mainly governed by *rule 11 of Annex VIII*, chapter III, which provides that:

"Software intended to provide information which is *used to take decisions with diagnosis or therapeutic purposes* is classified as *class IIa*, except if such decisions have an impact that may cause:

- Death or an irreversible deterioration of a person's state of health, in which case it is in Class III; or
- A serious deterioration of a person's state of health or a surgical intervention, in which case it is classified as *Class IIb*.

Software intended *to monitor physiological processes* is classified as *Class IIa*, except if it is intended for monitoring of vital physiological parameters, where the nature of variations of those

[142] See *infra*, point 2.3: requirements, which establishes some fundamental obligations of the manufacturers in the context of the certification process.

parameters is such that it could result in immediate danger to the patient, in which case it is classified as *Class IIb*.

All other software is classified as *Class I*".

(highlighted by the authors)

In this way, this rule implies that a lot of products which are qualified as medical devices implying software (such as software based on AI) should fall within Class IIa or higher, notably within Class IIb[143]. Nevertheless, it is also possible that a medical device implying a software fall into Class I[144]. The Guidance of MDCG gives as examples of this kind of medical device with software, the medical device intended to support conception[145].

Conclusion

Qualification and classification of medical devices require a case-by-case analysis of each product, notably to determine the intended purpose of the product.

2.2.2 Actors involved

MDR distinguishes several actors who play a fundamental role in some requirements of the regulation. It is important to define some of those actors which are particularly important in the context of TEF-Health in order to understand who is effectively concerned, in practice, by the requirements of MDR. The actors are involved in different steps of the lifecycle of a medical device.

Concerning the product, various actors are involved:

- The *manufacturer*:

  The manufacturer is "a natural or legal person who manufactures or fully refurbishes a device or has a device designed, manufactured or fully refurbished, and markets that device under its name or trademark"[146].

---

[143] *Ibid.*, p. 11.
[144] Cardio training applications offering workout recommendations and monitoring applications which are not used for diagnosis are also classified as Class I (Johner Institute, "MDR Classification Rule 11 for Medical Device Software", available at https://www.johner-institute.com/articles/regulatory-affairs/and-more/mdr-rule-11-software/, 22 July 2017.
[145] Medical Device Coordination Group Document, Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR, MDCG 2019-11, *op. cit.*, p. 28: "Medical device software app intended to support conception by calculating the user's fertility stats based on a validated statistical algorithm. The user inputs health data including basal body temperature and menstruation days to track and predict ovulation. The fertility status of the current day is reflected by one of three indicator lights: red (fertile), green (infertile) or yellow (learning phase/cycle fluctuation). This MDSW app should be classified as class I per Rule 11c)".

[146] MD, art. 2(30.

It is a key player, since it is the manufacturer who is responsible for all the procedures and obligations laid down in MDR to ensure safety and performance of the device[147]. He notably has the responsibility to carry out the adequate conformity assessment procedure[148].

In the context of TEF-Health, the manufacturers will be TEF-Health users (the SMEs) which create and develop medical devices and could be eligible for benefiting from the testing and experimentation facilities and services provided by the Consortium and its partners.

- The *importer:*

  The importer is "a natural or legal person established within the Union that places a device from a third country on the Union market"[149]. Concretely, when the manufacturer is established outside the European Union, it may place its products on the European market through an *importer*, i.e. "another entity that puts the system into service or places it on the market for the manufacturer"[150].

- The *distributor:*

  The distributor is "a natural or legal person in the supply chain, other than the manufacturer or the importer, that makes a device available on the market, up until the point of putting into services". It implies that the medical device has obtained the CE marking[151].

- The *user:*

  The user is "any healthcare professional or lay person who uses a device, once it is put on the market or into service"[152]. According to MDR, a 'lay person' means "an individual who does not have formal education in a relevant field of healthcare or medical discipline"[153]. This definition implies that a consumer or a patient could be considered as user of medical devices. This point differs with the definition of "user" in IA Act proposal[154].

[147] A. KISELEVA., « AI as a Medical Device: Is It Enough to Ensure Performance Transparency and Accountability in Healthcare?", *European Pharmaceutical Law Review*, 1/2020, pp. 11-12.
[148] See *infra*, point 2.3.
[149] MDR, art. 2(33).
[150] MDR, art. 2(33).
[151] MDR, art. 2(34).
[152] MDR, art. 2(37).
[153] MDR, art. 2(38).
[154] See *supra*, section 1.3.2 of this document.

This following figure shows the various actors involved in MDR.

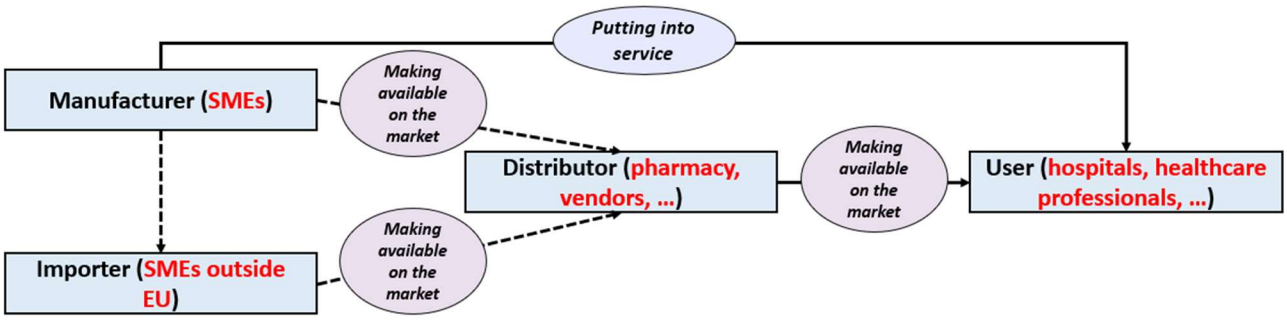


Figure 9 Actors involved in MDR

Concerning the conformity assessment procedure, different persons or organs can intervene:

- The *conformity assessment body* is a "body that performs third-party conformity assessment activities including calibration, testing, certification and inspection"[155].

- The *notified body* is "a conformity assessment body designated in accordance with the MDR" [156].

- The *sponsor* is "an individual, company, institution or organization which takes responsibility for the initiation, for the management and setting up of the financing of the clinical investigation" [157].

- *Ethics committee* is "an independent body established in a Member State in accordance with the law of that Member State and empowered to give opinions for the purposes of this Regulation, taking into account the views of laypersons, in particular patients or patients' organisations" [158]. Ethics committees have a specific role in the case of clinical investigations[159].

- *The person responsible for Regulatory Compliance,* is a person who possesses the requisite expertise in the field of medical devices[160] and who is designated in the organization of the manufacturer for ensuring, at least, that:
    - The conformity of the devices is appropriately checked, in accordance with the quality management system under which the devices are manufactured, before a device is released;

[155] MDR, art. 2(41).
[156] MDR, art. 2(42).
[157] MDR, art. 2(49).
[158] MDR, art. 2(46).
[159] Regarding that point, see *infra*, point 2.3.2.
[160] MDR, art. 15(1).

- The technical documentation and the EU declaration of conformity are drawn up and kept up-to-date;
- The post-market surveillance obligations are complied with in accordance with Article 10(10) of MDR;
- The reporting obligations referred to in Article 87 to 91 of MDR are fulfilled;
- In the case of investigational devices, the declaration is issued in accordance with Annex XV, Chapter 2, of MDR[161].

The person responsible for regulatory compliance has not to perform those tasks himself, he is merely responsible for their completion.

Micro and small enterprises within the meaning of Commission Recommendation 2003/361/EC[162] are not to be required to have the person responsible for regulatory compliance within their organization but must have such person permanently and continuously at their disposal[163].

2.3 Requirements to be complied with

2.3.1 Conformity assessment procedure

Conformity assessment procedures[164] are designed to demonstrate whether or not the requirements of MDR have been fulfilled, with a view to obtaining CE marking and authorization to place the medical device in question on the market[165].

Prior to placing a device on the market or putting into service a device that is not placed on the market, manufacturers must undertake an assessment of the conformity of that device[166].

Conformity assessment procedures vary according to the class to which the medical device concerned belongs. Conformity assessment procedures are set out in *Annexes IX to XI*. There are three types of assessments procedures[167]:

---

[161] MDR, art. 15(3).
[162] Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (*O.J.*, L 124, 20 May 2003, p. 36): small or micro organisations includes companies with fewer than 50 employees and an annual balance sheet of no more than 10 millions euros.
[163] MDR, art. 15(2).
[164] MDR, Chapter V.
[165] MDR, art. 2(40).
[166] MDR, art. 52(1) and 52(2).
[167] Some categories of medical devices are subject to specific conformity requirements:
-Class I devices are not subject to an assessment procedure. Manufacturers of these devices must themselves attest the conformity of their products by drawing up an EU declaration of conformity referred to in Article 19 of MDR, after having drawn up the technical documentation provided for in Annexes II and III of MDR. CE marking of these products does not therefore need to be approved by a notified body. An exception to this rule applies to Class I medical devices which are sterile and/or have a measuring function, or which are reusable surgical instruments. In this specific case, the manufacturers shall apply the procedures set out in Chapters I and III of Annex IX, or in Part A of Annex XI.
-Custom-made devices are subject to a specific conformity assessment procedure, as set out in Annex XIII of MDR. This special procedure requires the manufacturer to draw up a declaration containing various items of information, including a statement that the device complies with the general safety and

- Conformity assessment based on a *quality management system and on assessment of technical documentation* (Annex IX) ;
- Conformity assessment based on *type-examination* (Annex X). It is the procedure whereby a notified body[168] ascertains and certifies that a device fulfills the relevant provisions of MDR;
- Conformity assessment based on *product conformity verification* (Annex XI).

The application of one or other of these conformity assessment procedures depends on the class of the device concerned. Nevertheless, technical documentation is mandatory for all classes of medical devices.

The following figure gives an overview of which conformity assessment procedures applies depending on the class of medical device concerned.

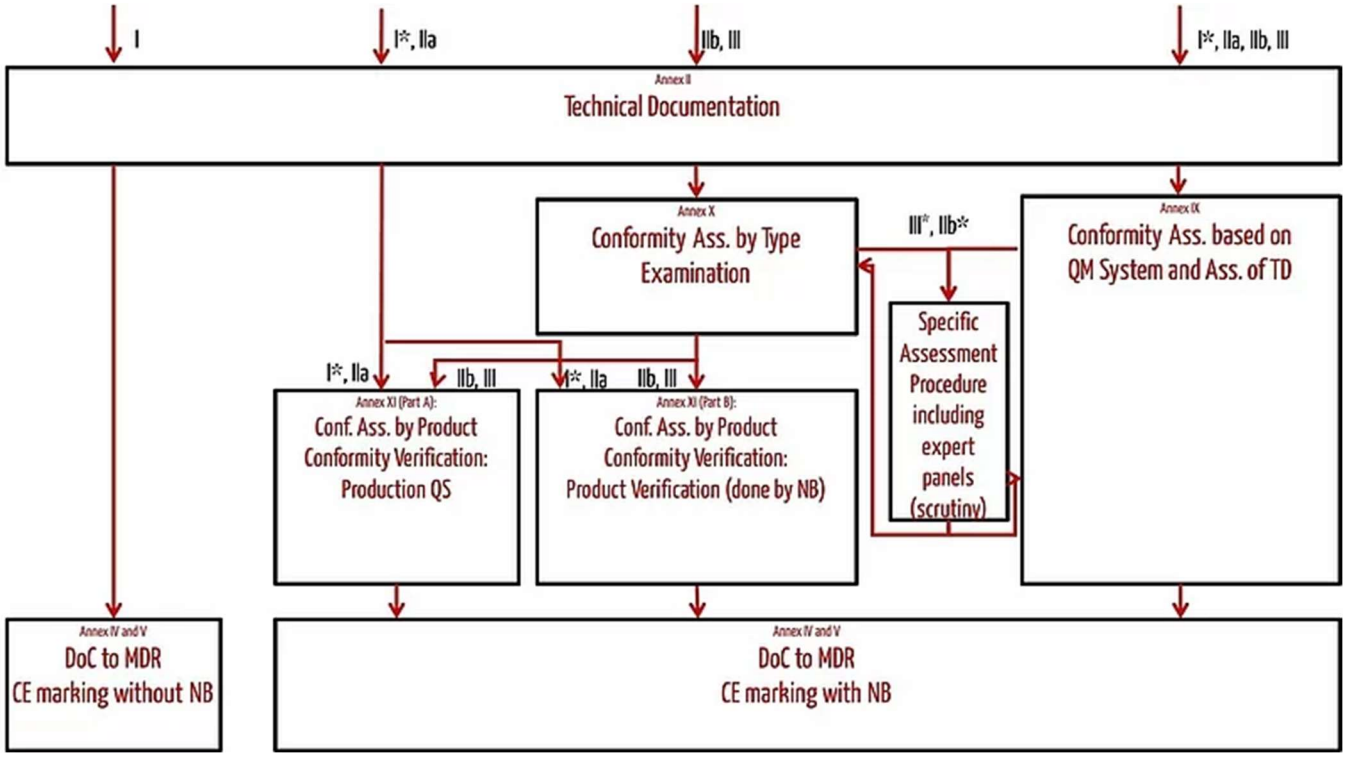


Figure 10 Conformity assessment procedures, Johner Institute website[169]

performance requirements of MDR. Nevertheless, manufacturers of Class III custom-made devices remain subject to the conformity assessment procedure under Annex XI, Part A.
However, in the context of the TEF-Health project, these specific compliance requirements are unlikely to have any impact, since as we see above, according to rule 11 of Annex VIII, most medical devices involving software (AI) will fall into at least category of Class IIa.

[168] Regarding that point, see *infra*, point 2.4.

[169] Johner Institute, "Conformity Assessment Procedures according to MDR", available on: https://www.johner-institute.com/articles/regulatory-affairs/and-more/conformity-assessment/, consulted on 26 November 2023. In the diagram, 'NB' means "Notified Body"; 'DoC' means "Declaration of conformity"; 'QM' means "Quality Management"; 'TD' means "Technical Documentation".

2.3.2 Clinical evaluation and clinical investigation[170]

A medical device may be placed on the market or put into service only if it complies with MDR[171]. Before the placing on the market or the putting into service, manufacturers have to demonstrate the conformity of their products.

2.3.2.1 Clinical evaluation

Demonstration of conformity with the general safety and performance requirements must include a clinal evaluation in accordance with Article 61 of MDR[172]. The obligation to carry out a clinical evaluation rests with the manufacturer to the exclusion of any other person[173].

It is important to emphasize that clinical evaluation is an ongoing process that takes place both before and after a product is marketed. It verifies whether the product complies with general safety and performance requirements, as well as assessing undesirable side effects and the acceptability of the benefit/risk ratio throughout the product's life. The obligation to carry out a clinical evaluation applies to all types of medical device.

According to Article 2(44) of MDR, *clinical evaluation* means "a systematic and planned process to continuously generate, collect, analyse and assess the *clinical data* pertaining to a device in order to verify the safety and performance, including clinical benefits, of the device when used as intended by the manufacturer" (highlighted by the author).

Clinical data means "information concerning safety or performance that is generated from the use of a device and is sourced from the following:

- Clinical investigation(s) of the device concerned,
- Clinical investigation(s) or other studies reported in scientific literature, of a device for which equivalence to the device in question can be demonstrated,
- Reports published in peer reviewed scientific literature on other clinical experience of either the device in question or a device for which equivalence to the device in question can be demonstrated,
- Clinically relevant information coming from post-market surveillance, in particular the post-market clinical follow up"[174].

The performance of the clinical evaluation is accompanied by several documents, which form an integral part of the technical documentation that must be supplied by the manufacturer to enable the notified body to assess the conformity of the device concerned[175]. Those documents are:

---

[170] MDR, Chapter VI.
[171] MDR, art. 5(1).
[172] MDR, art. 5(3).
[173] MDR, art. 10(3).
[174] MDR, art. 2(48).
[175] See MDR, art 10(4).

- A clinical evaluation plan[176], which ensures that the clinical evaluation is carried out before the device is marketed,
- A clinical evaluation report, which includes the results of the clinical evaluation and the clinical evidence on which it is based[177],
- A post market clinical follow-up plan, which contains an analysis and evaluation of the clinical data resulting from the use in or on humans of a device which bears the CE marking and is placed on the market or put into service within its intended purpose as referred to in relevant conformity assessment procedure, with the aim of confirming the safety and performance throughout the expected lifetime of the device, of ensuring the continued acceptability of identified risks and of detecting emerging risks on the basis of factual evidence[178].

2.3.2.2 Clinical investigation

As part of the clinical evaluation process, certain medical devices must also undergo *clinical investigation*. *Clinical investigation* means "any systemic investigation *involving one or more human subjects*, undertaken to assess the safety or performance of a device"[179] (highlighted by the author).

The conduct of a clinical investigation is subject to the consent of the persons concerned[180].

Clinical investigations are mandatory for *Class III devices and for implantable devices*[181]. There are exceptions to this obligation for certain types of devices and in certain specific cases[182].

In order to conduct a clinical investigation, the sponsor must comply with a number of preconditions. These include the obligation to obtain an authorization from the Member State in which the clinical investigation is to be conducted, as well as the obligation to obtain the favorable opinion of an ethics committee, set up in each Member State in accordance with its national law[183]. The rules governing the operation of ethics committees may therefore differ from one Member State to another. It is therefore essential to refer to the rules in force concerning clinical investigations and recourse to ethics committees in the Member State concerned.

The procedures to be followed when carrying out a clinical investigation are defined in detail in Annex XV of MDR[184]. Procedures may vary according to several criteria: the purpose of the clinical investigation concerned, the CE marking status of the medical device concerned, whether or not

[176] MDR, Annex XIV, Partie A, point 1, a).
[177] MDR, Annex XIV, Partie A, point 4.
[178] MDR, Annex XIV, Partie B, point 5.
[179] MDR, art. 2, (47).
[180] MDR, art. 62(4) (f). Specific consent requirements are contained in Articles 63 to 67.
[181] MDR, art. 61(4).
[182] MDR, art. 61(6).
[183] MDR, art. 62(4), a) et b).
[184] MDR, Annex XV.

the medical device is used for its intended purpose when the medical device is already CE certified, and the classification of the medical device concerned[185].

In TEF-Health project, WP8 is particularly involved in the process of clinical investigations and clinical evaluations. Among other tasks, it has to provide consulting services to assist companies in conducting clinical trials and clinical investigation of medical devices for human subjects (task T8.3)[186]. WP3 is also particularly involved in clinical investigation by setting up clinical experimentation labs[187].

2.3.3 CE marking

Medical devices considered to be in conformity with the requirements of MDR must bear the CE marking of conformity, as presented in Annex V of MDR[188]. The CE marking must be affixed before the device is placed on the market[189], and once the notified body has issued the certificate according to Annex VII of MDR[190].

2.3.4 Use and post-market surveillance[191]

Once the device has obtained to CE marking, it can be put on the market and be purchased and used by users. As part of the ongoing assessment of medical devices, manufacturers must plan, establish, document, implement, maintain and update a post-market surveillance system in a manner that is proportionate to the risk class and appropriate for the type of device[192].

The post-market surveillance system must be suited to actively and systematically gathering, recording and analyzing relevant data on the quality, performance and safety of a device throughout its entire lifetime. It must also be suited to drawing the necessary conclusions and to determining, implementing and monitoring preventive and corrective actions.

The post-market surveillance system implies the redaction of some documents:

- First, a post-market surveillance plan[193], the requirements for which are set out in section 1.1 of Annex III, of MDR;

[185] Agence nationale de sécurité du médicament et des produits de santé, « Avis aux promoteurs – Investigations cliniques de dispositifs médicaux relevant du règlement européen n° 2017/745 – Partie I », available on 2021-05-28-aap-partie-i-dispo-generales-ic-dm-v1-2-tqg.pdf, consulted on 30 October 2023, p. 8.
[186] Grant agreement, Annex 1 - Description of the action (part A), p. 15.
[187] Grant agreement, Annex 1 - Description of the action (part A), p. 10.
[188] MDR, art. 20(1).
[189] MDR, art. 20(4) .
[190] MDR, Annex XII.
[191] MDR, Chapter VII.
[192] MDR, art. 82(1).
[193] MDR, art. 84.

- Second, a post-market surveillance report (for medical devices of Class I)[194]. This report shall be updated when necessary and made available to the competent authority upon request[195];
- Third, a periodic safety update report (for medical devices of Class IIa, IIb and Class III). The periodic safety update report is part of the technical documentation on post-market surveillance established by the manufacturer in the context of the conformity assessment process[196].

All those documents relating to post-market surveillance form an integral part of the technical documentation and are essential for the conformity assessment. Especially the further development in this phase is an important part of AI products.

All the certificates issued by notified bodies (and certificates refused) are available on the platform EUDAMED[197].

2.4 Responsible authorities and notified bodies

According to MDR, *notified body* means "a conformity assessment body designated by a Member State in accordance with this regulation"[198].

Notified bodies are responsible to carry out conformity assessment of the product in accordance with Annex VII, in particular by assessing the technical documentation supplied by the product manufacturer. Once this assessment has been carried out, they are responsible for granting a certificate to the manufacturer which establishes the conformity of the device and is a prerequisite for declaring the conformity and for affixing the CE marking[199].

The proper functioning of notified bodies is crucial for ensuring a high level of health and safety protection and citizens' confidence in the framework and the market. That's why MDR strictly regulates the appointment and control of these bodies. An important difference between 'conformity assessment body' and 'notified body' is that only notified body are competent to award CE marking to medical devices.

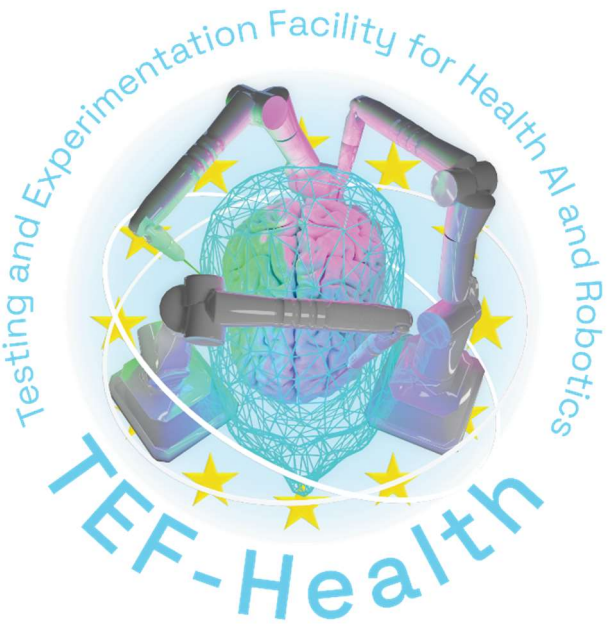
To ensure the proper functioning of notified bodies, MDR establishes a system for monitoring and assessing notified bodies. This surveillance is carried out by the authorities responsible for notified bodies, which must be designated in accordance with the national legislation of each Member State. In particular, the responsible authorities have the task of examining an appropriate number of assessments of the manufacturer's technical documentation, in particular the technical documentation relating to the clinical assessments carried out by the

[194] MDR, art. 85.
[195] MDR, art. 85.
[196] MDR, art. 86(1) and Annex III.
[197] EUDAMED stands for "European Database on Medical Devices". It is a centralized, secure, web-based platform developed by the European Commission to serve as a comprehensive database for medical devices in the European Union (EU), available on:https://ec.europa.eu/tools/eudamed/#/screen/home, consulted on 30 October 2023; MDR, art. 33 and 34.
[198] MDR, art. 2(42).
[199] MDR, Annex XII.

notified body, in order to verify the conclusions drawn by this body on the basis of the information supplied by the manufacturer.

Once a Member State designates a body as 'notified body' to carry out conformity assessments according to MDR, the Member State has the responsibility to notify this designation to the European Commission. All notified bodies are listed in a European database put in place in the context of the "single market compliance space" that everybody can consult online[200].

[200]Single Market Compliance Space, available on:https://webgate.ec.europa.eu/single-market-compliance-space/#/notified-bodies/notified-body-list?filter=legislationId:34,notificationStatusId:1, consulted on 27th November 2023.



Public report

D2.1: Legal, Ethical Framework Annex 2 'Data'

Action number: 101100700
Action Acronym: TEF-Health
Action title: Testing and Experimentation Facility for Health AI and Robotics
Author(s): UNamur-CRIDS

Submission date: December 2023

This project document is published at https://www.tefhealth.eu/.

Co-funded by the European Union

Table of content

1 The framework applicable to personal data (GDPR)

1.1 Preamble

This section analyses the General Data Protection Regulation (hereafter "GDPR")[1]. The purpose of this regulation is to ensure the protection of the rights and freedoms of people regarding the processing of personal data pertaining to them.

It is applicable to a lot of activities carried out by the TEF-Health Consortium which will require the processing of a large number of personal data, mainly health-related ones.

In this section, we first briefly describe the history of the right to privacy and data protection (1.2) before analysing the scope of the GDPR and the reasons why the Consortium should be attentive to its provisions (1.3). Afterwards, we highlight the key requirements with which the Consortium must comply with this regard (1.4).

1.2 Context and purposes of the regulation

1.2.1 Brief history of the right to privacy and data protection

The right to data protection arises from the broader fundamental right to privacy, set out at European level, in Article 8 of the European Convention of Human Rights (hereafter "ECHR")[2] of the Council of Europe and Article 8 of the European Charter of Fundamental Rights (hereafter "ECFR") of the European Union[3]. It aims, broadly speaking, to protect people against too intrusive practices having effect to make them losing control over their private life and to strengthen their "informational self-determination"[4].

The right to data protection has been for the first time implemented in a normative instrument at the international level through the Convention 108 of the Council of Europe[5]. This instrument contained different principles that are still applying today regarding, e.g., processing of special

[1] Regulation (EU) 2016/679 of the European Union 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), *O.J.*, L119/1, 4 May 2016.
[2] Convention for the Protection of Human Rights and Fundamental Freedoms, signed in Rome on 4 November 1950.
[3] Charter of Fundamental rights of the European Union, *O.J.*, C 364/1, 18 December 2000.
[4] This wording derives from a historic case law of the German Constitutional Court, under which "[...] If individuals cannot, with sufficient certainty, determine what kind of personal information is known to certain parts of their social environment, and if it is difficult to ascertain what kind of information potential communication partners are privy to, this could greatly impede their freedom to make self-determined plans or decisions. A societal order, and its underlying legal order, would not be compatible with the right to informational self-determination if citizens were no longer able to tell who knows what kind of personal information about them, at what time and on which occasion. Individuals who worry that non-conformist behaviour could be recorded at any time and that such information could permanently be stored, used or shared will try not to draw attention to themselves by not engaging in such behaviour [...]" ; German Federal Constitutional Court, 15 December 1983, available on https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1983/12/rs19831215_1bvr020983en.html, point 146.
[5] Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, *European Treaty Series – No 108*, 28 January 1981 (hereafter "Convention 108").

categories of data, the notion of personal data or data security[6]. In 1995, the European Union (hereafter, also the "EU") decided to go a step further in this field, by ensuring that all its Member States "[...] protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data" through a directive. It led to the adoption of the Directive 95/46/EC[7] which was then implemented in each Member State's national law.

1.2.2 The GDPR: a not-so-new approach?

In 2016, the European institutions switched their approach and reached an agreement on a new text, intended to replace the directive mentioned above: the GDPR. They mainly did it in order (i) to replace the directive by a regulation to reach a higher level of harmonisation between the various European Member States[8] and (ii) to ensure a better effectivity of the law by providing high fines in case of infringement[9].

That said, the GDPR, which entered into force the 25 May 2018[10], must not be considered disruptive. Indeed, if it provides some new requirements (to consider new technological developments, for example)[11], the GDPR is essentially built on the principles of the previous directive[12]. For this reason, the case law handed by the European Court of Justice (hereafter also the "ECJ") under the application of the Directive 95/46/CE is still relevant[13], to a certain extent, when assessing the conformity of certain practices regarding the provisions of the GDPR.

1.3 Scope and actors involved

This point 1.3 summarises the key-notions contained in the GDPR and, by doing so, analyses its scope. It focuses on the concepts of "processing", "personal data", "sensitive data", "controller", "processor" and "joint controllers".

1.3.1 Key notions delimiting the material scope

1.3.1.1 Notion of "personal data"

The significance of the concept of "personal data" appears to be growing. Under GDPR, this concept refers to "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in

[6] With this regard, see Convention 108, art. 6, 2 (a) and 7.
[7] Directive 95/46/CE of the European Parliament and of the Council of 24 October 1995 on the protection of the individuals with regard to the processing of personal data and on the free movement of such data, *O.J.E.C.*, L 281/31, 23 November 1995 (hereafter "Directive 95/46/CE"), art. 1 (1).
[8] GDPR, recitals 9 and 10.
[9] GDPR, recital 11.
[10] GDPR, art. 99 (2).
[11] See Y. Poullet, « Le RGPD – une volonté de bien faire : certes ! ... mais appropriée ? » *in* C. de Terwangne et K. Rosier (dir.), *Le règlement général sur la protection des données (RGPD/GDPR)*, 1st edition, Brussels, Larcier, 2018, p. 10.
[12] GDPR, recital 9.
[13] See for example EGC, *Single Resolution Board (SRB) v. European Data Protection Supervisor (EDPS)*, 26 April 2023, T-557/20, EU:T:2023:219, §88.

particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"[14]. To assess whether data are related to an identified or identifiable person "[...] account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. [...] The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable [...]"[15].

There are two main interpretations of these quotes. The authors defending the first one argue for a narrow interpretation of the concept of "anonymised data", and therefore for a broad interpretation of the concept of "personal data". For them, data are anonymised if there is technically absolutely, or almost absolutely, no risk of re-identification of a natural person thanks to these data (near-to-zero risk approach)[16]. The anonymisation process must therefore be irreversible[17]. The second approach is risk-based and accepts to consider data as anonymised even if a re-identification risk subsists, provided that such a risk is considered low after being assessed (risk-based approach)[18].

According to us, this second interpretation is the most relevant. First, it seems to be validated in a recent judgment of the European General Court (hereafter "EGC")[19]. Second, it is the only interpretation which is consistent with the recent approach the European legislator is now developing. The Data Governance Act (hereafter "DGA")[20] and the European Health Data Space regulation proposal (hereafter "EHDS" proposal)[21] both prohibit, for example, the re-identification of data subjects from anonymised data[22]. Such a prohibition would make no sense if the notion of "anonymised data" was considered under the near-to-zero risk interpretation in this context (first interpretation described above)[23]. Indeed, according to this near-to-zero risk

[14] GDPR, art. 4(1).
[15] GDPR, recital 26.
[16] A. MORETÓN et A. JARAMILLO, « Anonymisation and Re-Identification Risk for Voice Data », *E.D.P.L.*, n° 2, 2021, p. 275.
[17] Article 29 Working Party, Opinion 05/2014 on Anonymisation Techniques, WP216, 10 April 2014, p. 5.
[18] See, for example, S. STALLA-BOURDILLON and A. KNIGHT, « Anonymous data v. personal data – a false debate: an EU perspective on anonymization, pseudonymization and personal data », *Wisconsin International Law Journal*, disponible sur https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2927945, 2017, p. 15 ; M. FINCK et F. PALLAS, « They who must not be Identified – Distinguishing Personal from Non-Personal Data under the GDPR », *Max Planck Institute for Innovation and Competition Research Paper Series*, n°19-14, 2020, p. 8.
[19] See EGC, *Single Resolution Board (SRB) v. European Data Protection Supervisor (EDPS)*, 26 April 2023, T-557/20, EU:T:2023:219 ; For more information related to this topic, see A. GOBERT, M. KNOCKAERT, M. RAPPE and J-M. VAN GYSEGHEM, « À la croisée des enjeux de protection et d'ouverture: la donnée à caractère personnel et sa réutilisation », *J.T.*, 2024 (to be published).
[20] Regulation (EU) 2022/268 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), *O.J.*, L 152/1, 3 June 2022; this legal act is analyzed *supra*, Point 2.1.
[21] Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space, COM(2022) 197 final, 3 May 2022; this legal act proposal is analysed *supra*, Point 2.2.
[22] DGA, art. 5 and recital 8 and EHDS proposal, recital 49.
[23] A. GOBERT et al., *op. cit.*, (to be published).

interpretation, to be considered anonymized the data should be irreversibly de-linked to any natural person and re-identification should be therefore impossible. In such circumstances, there would be no need to expressly prohibit such re-identification[24].

In the context of TEF-Health when and if possible, it would be useful to use (process, share, etc.) data that are *legally*[25] considered anonymized. The GDPR would not apply to the processing of such data and the use and sharing of such data would then be facilitated. To ensure the data are *legally* considered anonymized and the risk of re-identification is minimized, we would therefore recommend drafting a standard document of risk assessment specifically intended to evaluate the risk of individuals' re-identification from the data processed in the course of the different activities of TEF-Health Consortium.

1.3.1.2 Notion of "sensitive data"

Another key-notion under the GDPR is the notion of "sensitive data", or, within the exact meaning of the regulation of "special categories of data". Article 9 of GDPR provides, indeed, that "[...] personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, [...] genetic data, biometric data [processed] for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation [...]" are special categories of data[26]. Their processing is prohibited in principle[27].

In addition, the recent ECJ's case law extends the meaning of this concept of "sensitive data". In the *OT* case, the ECJ states that "[article 9 of the GDPR] cannot be interpreted as meaning that the processing of *personal data that are liable indirectly to reveal sensitive information concerning a natural person* is excluded from the strengthened protection regime prescribed by those provisions, if the effectiveness of that regime and the protection of the fundamental rights and freedoms of natural persons that it is intended to ensure are not to be compromised"[28] [highlighted by the author]. In other words, data that are revealing indirectly sensitive information within the meaning of the GDPR shall be considered sensitive. For example, it means that a picture of a person wearing glasses shall be considered as a health data since the fact of wearing glasses gives indirect information about the vision of the individual, which is an information related to his or her health. The ECJ shares similar views in the *Meta Platforms* case by precising that: "In view of the significant risks to the fundamental freedoms and fundamental rights of data subjects arising from any processing of personal data falling within the categories referred to in Article 9(1) of the GDPR, the objective thereof is to prohibit such processing, *irrespective of its stated purpose*"[29].

---

[24] *Ibid*.
[25] One should pay attention to the fact that the data may be technically pseudonymised but legally anonymised following our proposed approach presented hereabove. It may raise some confusion.
[26] GDPR, art. 9(1).
[27] GDPR, art. 9(1).
[28] ECJ (gd ch.), case *OT v. Vyriausioji tarnybinės etikos komisija*, 1st August 2022, C-184/20, EU:C:2022:601, §127.
[29] See ECJ (gd ch.), case *Meta Platforms Inc. v. Bundeskartellamt*, 4 July 2023, C-252/21, EU:C:2023:537, §70.

In TEF-Health context, it is highly likely that a major part of the data that will be processed by the Consortium and its partners when offering their services and by TEF-Health users (the SMEs) when using TEF-Health services, as long as they are personal, will be considered "sensitive data". It will be the case despite of the stated purposes of their processing and even when the concerned data reveal sensitive health information only indirectly.

1.3.1.3 Notion of "processing"

GDPR applies to the "processing" of personal data[30]. The wording "processing" is broad in this context. It refers to "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction"[31]. It should be noted that even "consultations" are targeted by the provision. One should therefore consider that almost every small, and even indirect, interaction with personal data is a "processing" of such data.

1.3.2 Actors

1.3.2.1 Notions of "controller" and "processor"

Under GDPR, two main categories of actors are subject to obligations: the *data controller* and the *data processor*.

The *controller* is defined as "the natural or legal person, public authority, agency or other body which, alone or jointly with others, *determines the purposes and means of the processing of personal data*; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law"[32] [highlighted by the author]. In other words, the controller is any entity or individual which/who (i) determines – i.e., decides certain key elements[33] – (ii) the purposes and means – i.e., the "why" and the "how"[34] – of the processing activity. In its guidelines, the European Data Protection Board (hereafter "EDPB")[35] states with this regard that:

---

[30] GDPR, art. 2 (1).
[31] GDPR, art. 4 (2).
[32] GDPR, art. 4 (7).
[33] European Data Protection Board, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.1, 7 July 2021, p. 11, point 20.
[34] European Data Protection Board, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.1, 7 July 2021, p. 11, point 35.
[35] The EDPB defines itself as follows: "The European Data Protection Board (EDPB) is an independent European body. It is the umbrella organisation which brings together the national data protection authorities (National Supervisory Authorities) of the countries in the European Economic Area, as well as the European Data Protection Supervisor (EDPS). The EDPB ensures that the General Data Protection Regulation and the Law Enforcement Directive are applied consistently and ensures cooperation, including on enforcement"; description available on: https://edpb.europa.eu/about-edpb/who-we-are/edpb-chairmanship_en, consulted on 23 November 2023.

"[...] One should look at the specific processing operations in question and understand who determines them, by first considering the following questions: "why is this processing taking place?" and "who decided that the processing should take place for a particular purpose?""[36].

Under GDPR, the *processor* is "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller"[37]. The processor is then any entity or individual that is (i) separate in relation to the controller (no hierarchy between them) and (ii) processes personal data on the controller's behalf[38] – i.e., for its benefit[39]– but otherwise than under its direct authority or control[40].

In practice, it is not always easy to assess whether a specific actor should be considered processor or a (joint) controller[41]. The EDPB provided an example, citing the case of a company ABC which hires an IT-specialist from another company to fix a bug in a software that is currently being used by the company ABC[42]. In this case, the IT-specialist shall be considered a processor (excluding then the qualification of "(joint) controller") if the company ABC takes security measures in order to prevent the IT-specialist from processing personal data in an unauthorised manner[43].

1.3.2.2 Notion of "joint controllers"

It may also exist situations in which several entities are considered both *"joint" controllers*. The EDPB precises that: "[...] The overarching criterion for joint controllership to exist is the joint participation of two or more entities in the determination of the purposes and means of a processing"[44]. According to it, "[...] joint participation can take the form of a common decision taken by two or more entities or result from converging decisions by two or more entities regarding the purposes and essential means"[45]. To identify a converging decision, it should be assessed "[...] whether the processing would not be possible without both parties' participation in the purposes and means in the sense that the processing by each party is inseparable, i.e., inextricably linked [...]"[46]. There is also joint control if the two parties take a common decision, i.e., decide together to start a new specific processing activity[47].

There are a few illustrations of joint controllership in the case law of the ECJ. A recent example is the *Fashion ID* case[48]. In this judgment, the ECJ founded that: "[...] Fashion ID's embedding of

---

[36] EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.1, 7 July 2021, p. 11, point 20.
[37] GDPR, art. 4(8).
[38] EDPB, Guidelines 07/2020, p. 25, point 76.
[39] EDPB, Guidelines 07/2020, p. 26, point 79.
[40] EDPB, Guidelines 07/2020, p. 26, point 80.
[41] Regarding this notion, see *supra*, point 1.3.2.2.
[42] EDPB, Guidelines 07/2020p. 28.
[43] EDPB, Guidelines 07/2020, p. 28.
[44] EDPB, Guidelines 07/2020, p. 19, point 53.
[45] EDPB, Guidelines 07/2020 p. 19, point 54.
[46] EDPB, Guidelines 07/2020, pp. 19-20, point 55.
[47] EDPB, Guidelines 07/2020, pp. 19, point 55.
[48] ECJ, case *Fashion ID GmbH & Co. KG v. Verbraucherzentrale NRW eV*, 29 July 2019, C-40/17, EU:C:2019:629.

the Facebook 'Like' button on its website allows it to optimise the publicity of its goods by making them more visible on the social network Facebook when a visitor to its website clicks on that button. The reason why Fashion ID seems to have consented, at least implicitly, to the collection and disclosure by transmission of the personal data of visitors to its website by embedding such a plugin on that website is in order to benefit from the commercial advantage consisting in increased publicity for its goods; those processing operations are performed in the economic interests of both Fashion ID and Facebook Ireland, for whom the fact that it can use those data for its own commercial purposes is the consideration for the benefit to Fashion ID"[49]. For this reason, one might have thought that it was a "converging decision" situation under the EDPB's comprehension. For its part, the Court did not go into such precision, but it stated that Fashion ID and Facebook were joint controllers[50].

1.3.3 Application to TEF-Health

In the field of the activities of the TEF-Health Consortium, a lot of different actors will be involved, depending on the services offered. Given the number of possible relationships that may exist, we only illustrate the reflections that may arise regarding the qualification of these actors as controllers, joint controllers or processors. For this purpose, we choose the examples of the reflections that must be performed (i) at Consortium – or some of its partners – level and (ii) at TEF-Health users (SMEs) level. However, a case-by-case analysis should be performed, by design, for each processing activity carried out by the Consortium or one of its partners.

For instance, the Consortium itself envisions, through certain partners, an access to a "TEF Data Space of health data"[51] that will permit testing and experimentation in real conditions of artificial intelligence (hereafter also "AI") systems. On their side, the TEF-Health users (the SMEs) will use the services, including the (sensitive) personal data put at their disposition and will bring training and testing data to some partners of the Consortium, in charge of testing and experimenting their products.

In this example, it seems that there could not be a "common" decision taken (and then a "joint controllership") between the Consortium (or the partners concerned by the creation of such data space) and the TEF-Health users (the SMEs) regarding the creation of the data space and the merging of datasets for this purpose. Indeed, such a data space will only be developed by the Consortium (or some of its partners), and more specifically by the partners involved in Work Package (hereafter "WP") 4[52].

Finally, it will be important, to determine whether the Consortium (or some of its partners) will use the services offered by some external suppliers, such as cloud providers for example. In such cases, it must be analysed whether these external suppliers have an important role or control on the processing activities for which they assist the Consortium.

[49] ECJ, *Fashion ID* above, §80.
[50] ECJ, *Fashion ID* above, §81.
[51] Grant Agreement, Annex 1 – Description of the action (Part A), List of Work packages, p. 9.
[52] Grant Agreement, Annex 1 – Description of the action (Part A), List of Work packages, p. 9.

We must highlight that, with regard to (joint) controllership in general, each situation must be assessed factually and independently, based on the elements exposed within this subsection.

1.4 Key requirements to be complied with

Since the Consortium, and its partners, will probably be the controller(s) of some processing activities, we must raise attention to the main GDPR requirements with which they will have to comply.

1.4.1 General principles

First, any processing of personal data must respect 6 general principles, contained in Article 5 of GDPR: (i) transparency, (ii) purpose limitation, (iii) data minimisation, (iv) accuracy, (v) storage limitation and (vi) integrity and confidentiality.

1.4.1.1 Transparency

The transparency is one of the most important principles under GDPR. A lack of transparency may, indeed, generate infringement to other provisions of the GDPR, such as informed consent[53] or right of data subjects to be informed[54].

Transparency is also linked to the purpose limitation principle, that obliges the controller to specify the purpose(s) for which it processes the data in comprehensive and transparent way[55]. For these reasons, Article 5(1) (a) GDPR states broadly that personal data shall be: "processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')". In other words, it means that any information and communication relating to the processing of personal data must be easily accessible and easy to understand, and that clear and plain language must be used[56].

At least, it must be given "[...] information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed [...]"[57].

In the context of TEF-Health, it means that privacy statements or policies will have to be drafted and communicated to the data subjects.

1.4.1.2 Purpose limitation

The purpose limitation principle may be split in three parts.

[53] GDPR, art. 7 (4).
[54] GDPR, art. 13 and 14.
[55] See *supra*, point 1.4.1.2.
[56] GDPR, recital 39.
[57] GDPR, recital 39.

First, it implies that data must necessarily be processed for (i) specified, (ii) relevant and (iii) limited purposes[58].

Second, once they have been processed for this/these purpose(s) they may not be processed for another one, unless this "further processing" is not "incompatible" with the first one[59].

For instance, hospitals collect data when the carry out their therapeutical day-to-day activities. In TEF-Health context, these data could be re-used in order to test and/of certify AI tools. This would be an example of "further processing" of health data[60].

It must be noted that: "[...] further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes"[61]. In addition, recital 33 precises that: "It is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose".

Third, there are two possibilities to further process data even for incompatible purposes, i.e. (i) if the data controller has obtain the consent[62] of the data subject to such a further processing of his or her data or (ii) if this possibility of further processing "[...] constitutes a necessary and proportionate measure in a democratic society to safeguard [...]" a number of general interest objectives detailed in Article 23 GDPR[63].

1.4.1.3 Principle of minimisation

The data minimisation principle implies that only data which are "[...] necessary for the purposes for which they are processed"[64] are processed.

In the context of TEF-Health, if there is no need to process personal data to reach the objectives that are settled, there is no reason to do so. In addition, even if such a need exists, only the data the processing of which is strictly necessary to reach these objectives may be processed. This will also be the case if the data may be useful in the future but are not when the decision to potentially process them is taken. It also means that the Consortium must perform processing activities that are as less intrusive as possible.

[58] GDPR, art. 5(1) (b).
[59] GDPR, art. 5(1) (b).
[60] In this context, note that the secondary use of health data within the European Union will be – in some cases – also governed by the rules provided by the EHDS proposal; see *infra*, point 2.2.
[61] GDPR, art. 5(1) (b).
[62] GDPR, art. 6(4).
[63] GDPR, art. 6(4).
[64] GDPR, art. 5 (1) (c).

1.4.1.4 Accuracy

When processing data, the controller shall also ensure that these data are "[...] accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy')"[65].

This means that the controller must set organisational and technical means to ensure this duty.

1.4.1.5 Storage limitation

Article 5(1) (e) GDPR states that the data must be "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject".

What is important for what concerns the Consortium is that a retention period for each category of data processed must be determined.

1.4.1.6 Integrity

The sixth principle presented here is related to data security.

Article 5(1) (f) GDPR provides that personal data must be "[...] processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')". This principle is also enshrined in Article 32, that applies specifically to data security and provides a risk-based approach, which is usual in this field[66]. Article 32 reads as follows "Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk [...]"[67].There is

[65] GDPR, art. 5 (1) (d).
[66] This is in line with the good practices provided by internationally known information security standards, such as ISO 27000 for instance.
[67] GDPR, art. 32(1).

another link to make between this principle and Articles 33 and 34, that provides notification procedures to comply with in case of a data breach[68].

Organisational and technical measures to ensure a level of security appropriate to the risk presented by the processing concerned – which will have to be assessed - will have to be settled.

1.4.2 Lawfulness of processing

Second, processing of personal data is only possible under the condition that it is justified on the ground of one of the legal basis laid down in Article 6 GDPR[69]:

a. consent of the data subject,
b. necessity for the performance of a contract,
c. necessity for the compliance with a legal obligation,
d. necessity to protect vital interests of the data subjects or another natural person,
e. necessity for a task carried out in the public interest or
f. necessity for the purposes of the legitimate interests of the controller[70].

In addition, if the data processed fall within one of the "special categories of data" of Article 9 (1) (i.e., notably health data), they may not be processed at all, unless the controller is able to justify the application of one of the exceptions of Article 9(2). Since the data that will be processed within TEF-Health project will probably be often considered as health data, i.e., sensitive data (unless they are anonymised[71]), we analyse these two provisions.

1.4.2.1 Legal basis under Article 6

In order to legally process personal data, it is necessary to base the processing activity on one of the six grounds of Article 6 GDPR. Note that the data controller may choose alternatively between these legal bases, one does not prevail on another.

The data controller would have to assess, case-by-case, which of these legal bases is the most relevant to justify the processing activity it undertakes[72].

---

[68] Article 33 provides the procedure to follow to assess whether a notification to the competent supervisory authority has to be performed and how it has to be done when it is the case; Article 34 precises the conditions under which the breach shall also be notified to the data subject himself.
[69] See GDPR, art. 6(1).
[70] "[...] [Except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child"; GDPR, art. 6(1) (f).
[71] See *supra*, point 1.3.1.1.
[72] Regarding some specific processing of health data, when the future EHDS regulation will be adopted, the principles it lays down will also have to be taken into account to lead such analysis; For the analysis of EHDS proposal, see *infra*, point 2.2.

Consent

The most commonly known of these bases, i.e., consent of the data subject to the processing of his/her data, is contained in Article 6(1) (a) GDPR. It should be emphasised that some conditions must be met in order to ensure the consent is considered valid. Consent is defined, under Article 4(11) GDPR, as "[...] any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".

First, it must be given *freely*, which means that a real choice must be provided to the data subject and that the notion of imbalance of power between the data subject and the controller must be taken into account with this regard[73]. Second, the consent must be *specific* to the processing activities for which it is given. This is, among others, related to the notion of granularity, highlighted by the EDPB[74] and the European Court of justice[75]. It signifies that when a service involves multiple processing activities operations for more than one purpose, consent shall be given separately for each of them, and the data subject must be free to choose which purpose he or she accepts and which he or she denies[76]. The data subject must also be sufficiently informed in a transparent way and in plain language before making his or her choice. Finally, consent will be valid only if it is obtained through an active action of the data subject. One cannot use pre-ticked boxes for example.

Necessity for the performance of a contract

The data controller may also justify a processing activity based on the necessity for the performance of a contract concluded with the data subject. Nevertheless, it must be highlighted that the ECJ has recently stated that: "[...] in order for the processing of personal data to be regarded as necessary for the performance of a contract [...], it must be *objectively indispensable* for a purpose that is integral to the contractual obligation intended for the data subject. The controller must therefore be able to demonstrate how the main subject matter of the contract cannot be achieved if the processing in question does not occur"[77]. The ECJ added that: "The fact that such processing may be referred to in the contract or may be merely useful for the performance of the contract is, in itself, irrelevant in that regard. The decisive factor for the purposes of applying the justification set out in point (b) of the first subparagraph of Article 6(1) of the GDPR is rather that the processing of personal data by the controller must be essential for the proper performance of the contract concluded between the controller and the data subject and, therefore, that there are no workable, less intrusive alternatives"[78].

It means that this legal basis could, for example, cover processing of health data in order to verify that the conditions of a healthcare insurance policy are met in a specific situation. On the

[73] p. 7, point 13.
[74] P. 12, points 42 to 45.
[75] See, for example, ECJ (gd ch.), *Meta Platforms,* C-252/21, presented *supra* (point 1.3.1.2), §151.
[76] P. 12, point 42.
[77] ECJ (gd ch.), *Meta Platforms*, C-252/21, presented *supra* (point 1.3.1.2), §98.
[78] ECJ (gd ch.), *Meta Platforms*, C-252/21, presented *supra* (point 1.3.1.2), §99.

contrary, it would not cover the processing of health data held by hospitals carried out by the Consortium (or some of its partners) in order to test and certify an AI system. .

Necessity for the compliance with a legal obligation or for carrying out a task of public interest

The third and the fourth legal basis for processing we analyse are the necessity for the compliance with a legal obligation (c) and the necessity for carrying out a task of public interest (e). They are, in practice, closely related. Recital 45 GDPR states, for instance, that: "Where processing is carried out in accordance with a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority, the processing should have a basis in Union or Member State law. [The GDPR] does not require a specific law for each individual processing. A law as a basis for several processing operations based on a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority may be sufficient. It should also be for Union or Member State law to determine the purpose of processing. Furthermore, that law could specify the general conditions of [GDPR] governing the lawfulness of personal data processing, establish specifications for determining the controller, the type of personal data which are subject to the processing, the data subjects concerned, the entities to which the personal data may be disclosed, the purpose limitations, the storage period and other measures to ensure lawful and fair processing. It should also be for Union or Member State law to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public authority or another natural or legal person governed by public law, or, where it is in the public interest to do so, including for health purposes such as public health and social protection and the management of health care services, by private law, such as a professional association".

One example of such a Union law will be the EHDS regulation. These two legal bases could therefore be the ones on which several processing activities carried out by the Consortium could be based in the future. We analyze further this question *supra* in point 2.2.

Necessity for protecting the vital interests of the data subject or another natural person

According to recital 46 of the GDPR: "The processing of personal data should also be regarded to be lawful where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person. Processing of personal data based on the vital interest of another natural person should in principle take place only where the processing cannot be manifestly based on another legal basis. Some types of processing may serve both important grounds of public interest and the vital interests of the data subject as for instance when processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread or in situations of humanitarian emergencies, in particular in situations of natural and man-made disaster".

Given the strict necessity threshold referred by the recital, this legal basis should not be relevant in order to justify the activities of TEF-Health. The only possibility to rely on it in this context should probably be in case of an emergency situation, such as, for instance, during a pandemic

or an epidemic, during which it would have a need to test and certify more quickly certain AI systems.

Legitimate interest

Finally, it is also possible to justify a processing activity based on the legitimate interest of the controller. Nevertheless, three conditions must be met in order to be able to rely on this legal basis: (i) the pursuit of a legitimate interest by the data controller or by a third party, (ii) the need to process personal data for the purposes of the legitimate interests pursued and (iii) that the interests or fundamental freedoms and rights of the person concerned by the data protection do not take precedence over the legitimate interest of the controller or of a third party[79].

In the TEF-Health context, the third element (point (iii) above) would probably be the most difficult to meet according to us. It entails the realisation (and the documentation) of a "balancing test", between the legitimate interest of the controller and the fundamental rights of the data subjects, taking into account the specific circumstances of the case [80]. The ECJ stated that " [...] it is necessary, in such a balancing exercise, to pay particular attention to the situation where the data subject is a child [...]"[81] and that " [...] the interests and fundamental rights of the data subject may in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect such processing [...]"[82]. The scale of the processing at issue and its impact on the data subjects are also criteria that must be taken into account by the controller when it performs such a test[83].

In the *Meta Platforms* case, the ECJ considered, for instance, that Meta could not rely on its legitimate interest in order to justify the activities carried out for personalised advertising purposes since "[...] despite the fact that the services of an online social network such as Facebook are free of charge, the user of that network cannot reasonably expect that the operator of the social network will process that user's personal data, without his or her consent, for the purposes of personalised advertising [...]"[84].

In the TEF-Health context, the possibility of being able to rely on the legitimate interest will mainly depends of criteria such as the reasonable expectations of the patient and the scale of the envisioned processing activity. A balancing test will have to be performed and documented case-by-case.

Nevertheless, note that public authorities cannot use this legal basis[85]. It may be important, for instance, with regard to public hospitals in the context of TEF-Health.

[79] See, for instance, ECJ, *Mircom International Content Management & Consulting (M.I.C.M.) Limited v. Telenet BVBA*, 17 June 2021, C-597/19, EU:C:2021:492, §106 ; ECJ, *Meta Platforms*, C-252/21, presented *supra* (point 1.3.1.2), §106.
[80] ECJ, Mircom, C-597/19, presented *supra* (point 1.4.2.1.5), §106 ; ECJ, *Meta Platforms*, C-252/21, presented *supra* (point 1.3.1.2), §110.
[81] ECJ, *Meta Platforms*, C-252/21, presented *supra* (point 1.3.1.2), §111.
[82] ECJ, *Meta Platforms*, C-252/21, presented *supra* (point 1.3.1.2), §112.
[83] ECJ, *Meta Platforms*, C-252/21, presented *supra* (point 1.3.1.2), §117.
[84] ECJ, *Meta Platforms*, C-252/21, presented *supra* (point 1.3.1.2), §118.
[85] GDPR, art. 5(1) *in fine*.

1.4.2.2 Exemptions to article 9 (1)

As mentioned above, by principle the processing sensitive data targeted by Article 9(1) such as health data is prohibited. The only way to process such data is to argue for the application of one of the exemptions listed in Article 9(2).

These exemptions are:

a. explicit consent,
b. necessity for carrying out obligations or rights in the field of employment and social security,
c. necessity for protecting the vital interests of the data subject or another natural person,
d. legitimate activities of a foundation,
e. processing of personal data which are manifestly made public,
f. necessity for the establishment, exercise of defence of legal claims,
g. necessity for a substantial public interest,
h. necessity for the purposes of preventive or occupational medicine,
i. necessity in the area of public health and
j. necessity for archiving, scientific or historical research purposes.

They are of strict interpretation.

Some of these exemptions, such as the legitimate interest of a foundation or the necessity for carrying out obligations or rights in the field of employment and social security, will not be relevant for TEF-Health. In addition, when applicable, the future EHDS regulation will provide guidelines on the legal bases that the data controller must use to justify the processing of health data it carries out[86].

We analyse hereafter two exemptions bases that could be used by the Consortium in order to justify some of its activities, i.e. explicit consent (a) and (e) processing of personal data that are manifestly made public. Note that exemptions (g) necessity for a substantial public interest, (h) necessity for the purpose of preventive or occupational medicine, (i) necessity in the area of public health and (j) necessity for archiving, historical or scientific research purposes might also be relevant, in particular when the EHDS regulation would apply. This link between the EHDS proposal and the GDPR, as well as the legal bases mentioned, are analysed *infra* (point 2.2.3.4 of this document).

Explicit consent

In the cases in which the data subject is already asked for his or her consent in order to justify one or several processing activity/activities for the purpose of compliance with Article 6, the most accurate exemption would probably be the one laid down in article 9(2) (a), i.e. consent. Pursuant to this exemption: “the data subject has given *explicit consent* to the processing of

[86] For more information on this field, see *infra* point 2.2.5.1 of this document.

those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject" (highlighted by the author).

It means that if the data subject (e.g. the patient) has given a consent to the processing of his or her health data for the purposes of carrying out the activities of TEF-Health project, the prohibition will not apply.

Processing of data manifestly made public

The data controller may also process special categories of personal data, such as health data, when the data have been "[...] manifestly made public by the data subject"[87]. It should be highlighted that, according to the ECJ, this exemption must be interpreted restrictively[88] and applies only when the data have been made public by the data subject himself of herself[89]. In addition, the Court stated that " [...] for the purposes of the application of the exception laid down in Article 9(2) (e) of the GDPR, it is important to ascertain whether the data subject had intended, explicitly and by a clear affirmative action, to make the personal data in question accessible to the general public"[90].

For instance, a person who has publicly mentioned a health issue during an interview has made publicly available health data related to him or her.

1.4.3 Main obligations of the data controller

Third, the data controller is bound by different obligations under GDPR. We focus on the most accurate ones for what concerns TEF-Health project, i.e. the accountability principle, the privacy by design, the maintaining of a record of processing activities, the appointment of a Data Protection Officer (hereafter a "DPO") and the obligation to conduct a Data Protection Impact Assessment (hereafter "DPIA").

We therefore not analyse in detail the provisions related to the rights of the data subjects[91], the obligations to conclude an agreement between the controller and the processor[92] or between joint controllers[93], security of personal data[94], cooperation with supervisory authorities[95], data breaches[96] or transfer of personal data to third countries or international organisations[97]. This does not mean, however, that these points are not relevant or important. Nevertheless, this

[87] GDPR, art. 9(2) (e).
[88] ECJ, *Meta Platforms*, C-252/21, presented *supra* (point 1.3.1.2), §76.
[89] ECJ, *Meta Platforms*, C-252/21, presented *supra* (point 1.3.1.2), §75.
[90] ECJ, *Meta Platforms*, C-252/21, presented *supra* (point 1.3.1.2), §77.
[91] GDPR, art. 13 to 23.
[92] GDPR, art. 28(3).
[93] GDPR, art. 26.
[94] GDPR, art. 32.
[95] GDPR, art. 31.
[96] GDPR, art. 33 and 34.
[97] GDPR, art. 44 to 50.

document pursues a general information purpose. We let therefore these points open and able to be tackled, at further stages in the project.

1.4.3.1 Accountability

The most important, in practice, to highlight in first instance is the accountability principle. Article 5(2) GDPR provides that: "The controller shall be responsible for and be able to demonstrate compliance with [the general principles set out in article 5(1)] ('accountability')".

It means that the first obligation of the controller is related to its ability to proof that it acts in conformity with the general aims of the regulation, translated within the general principles[98]. In addition, it must be added that the controller is also accountable for the actions of the processor acting on its behalf[99]. So, it will be important to assess which these processors may be, i.e. to identify all the external providers involved in the processing of personal data, to conclude data processing agreements with them[100] and to put in place controls (e.g. through audits possibility) to assess their effective compliance with the legal requirements.

1.4.3.2 Data protection (or privacy) by design and by default and security of personal data

The controller must also ensure that privacy and data protection are a concern "by design and by default". Concretely, it means that: "Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects"[101].

In other words, every time that it will envision a new processing activity in the course of the establishment of the testing and experimentation facilities, the Consortium, or its partners, will have to take appropriate measures to protect the data, to store them in a secure way, to minimise the impact on the data subject, and so on. An example of measures that could be taken is pseudonymisation measures, i.e. measures aiming to de-identify directly data which could nevertheless "[...] be attributed to a natural person by the use of additional information"[102].

In addition, the controller "[...] shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data

[98] Regarding these general principles, see *supra*, point 1.4.1.
[99] GDPR, art. 28(1).
[100] GDPR, art. 28(3).
[101] GDPR, art. 25 (1).
[102] GDPR, recital 26.

collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons"[103].

It imposes the Consortium, and / or its partners, to take technical and organisational measures ensuring that the storage limitation, the minimisation and limitation of purpose principles developed hereabove are respected. With this respect, it is, for example, important to implement access management measures and to keep the logs in order to be able to demonstrate that only relevant people have access to the data.

Finally, when it/they is/are considered as a data controller, the Consortium, and/or its partners, will also have to take technical and organizational measures to ensure the security of the personal data, such measures depending on the level of risk of varying likelihood and severity for the rights and freedoms of natural persons[104]. In TEF-Health context, given the nature of the data processed (the major part will be related to the health of the data subjects), one can assume that the risk must be considered high or very high and that the measures that must be taken will be strict. It is important to precisely document the risk evaluation with this regard in order, for the Consortium, to be able to justify its analysis and the adequation of the measures taken.

Article 35(1) provides examples of measures that may be envisioned, when appropriate: (i) pseudonymisation and encryption of the data, (ii) measures ensuring confidentiality, integrity, availability and resilience of processing systems and services, (iii) measures ensuring the ability to recover after a security incident and (iv) regular testing, assessment and evaluation of the measures.

1.4.3.3 Record of processing activities

When it is / they are considered as data controller(s), the Consortium, and/or its partners, will also have to maintain and to update a "record of processing activities"[105].

This record must contain at least the information listed in Article 30(1) GDPR, such as, for instance, the purpose of the processing and a description of the categories of data subjects and the categories of personal data. Maintaining this record is not only an administrative requirement, but also an important tool to map all the personal data processed, which is essential in order to manage them.

In practice, different tools exist to facilitate compliance with this point. Several data protection authorities, such as the CNIL[106] for example, provide free templates of such a record in an excel format. Data management platforms also provide modules which serve data mapping or data mapping automation.

[103] GDPR, art. 25 (2).
[104] GDPR, art. 32 (1).
[105] GDPR, art. 30.
[106] The CNIL's template is available here: https://www.cnil.fr/sites/cnil/files/atoms/files/record-processing-activities.ods.

1.4.3.4 Appointment of a data protection officer (DPO)

Since the TEF Health Consortium's core activities will "[...] consist of processing on a large scale of special categories of data pursuant to Article 9 [...]"[107], i.e. health data, it will have to designate a DPO who will have to be easily accessible to each of the partners[108].

The DPO "[...] shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices [...][109] and may be alternatively a member of one of the partners of the Consortium or an external service provider[110].

The DPO will be involved in all issues which relate to the protection of personal data in the course of the activities of the Consortium, and its partners, and may not receive instructions regarding the exercise of his or her tasks[111]. He or she may fulfil other tasks and duties as far as it does not result in a conflict of interest[112].

1.4.3.5 Data protection impact assessment (DPIA)

Finally, the Consortium, and probably some of its partners, will have to realise a Data Protection Impact Assessment (DPIA) prior to carrying out a large part of its/their activities and in all cases before carrying out the activities linked to the processing of health data of many people[113].

Article 35(7) GDPR provides that: "The assessment shall contain at least: (a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller; (b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes; (c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned".

Here also, templates of such kind of assessment exists. The CNIL provides several "guides" in relation with this topic[114], for example.

[107] GDPR, art. 37 (1) (c).
[108] See GDPR, art. 37 (2).
[109] GDPR, art. 37 (5).
[110] GDPR, art. 37 (6).
[111] GDPR, art. 38 (1) and (3).
[112] GDPR, art. 38 (6).
[113] GDPR, art. 35 (3) (b).
[114] These guides are available on https://www.cnil.fr/en/PIA-privacy-impact-assessment-en.

2 The framework applicable to the sharing of data (Data Governance Act, European Health Data Space and Data Act)

2.1 Data Governance Act

2.1.1 Preamble

This section analyses the provisions of the Data Governance Act (hereinafter "DGA")[115], intended to be applicable to, among other, the sharing of – both personal and non-personal – data within the European Union. The DGA entered into force the 24 September 2023[116].

This section details how this legislation is a keystone of the European strategy for data[117] and how it concretely implements the vision the European Commission had when issuing this strategy. It also explains why this text should be understood in the broader context of its articulation with sectoral legislations, such as in health sector, the future European Health Data Space Regulation (the already mentioned the "EHDS" proposal)[118].

The DGA organises three aspects of the sharing of data:

- the re-use of certain categories of data held by public sector bodies,
- the data intermediation services, and
- the data altruism organisations.

Since these aspects may be of interest for TEF-Health project, they will be analysed in this section.

2.1.2 Context and purposes of the DGA

In its European Strategy for data, the European Commission identified four pillars on which it decided to build its actions regarding the data legislative framework[119]. One of these pillars is linked to "cross-sectoral governance for data access and use"[120]. With this regard, it stated that: "Cross-sectoral (or horizontal) measures for data access and use should create the necessary over-arching framework for the data-agile economy, thereby avoiding harmful fragmentation of the internal market through inconsistent actions between sectors and between the Member States. Such measures should nonetheless take into account the specificities of individual sectors and of the Member States. The Commission's approach to regulation is to create

[115] Regulation (EU) 2022/268 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), *O.J.*, L 152/1, 3 June 2022.
[116] DGA, art. 38.
[117] Communication from the Commission - A European strategy for data, COM(2020) 66 final, 19 February 2020 (hereinafter "European Strategy for data").
[118] Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space, COM(2022) 197 final, 3 May 2022; this legal act proposal is analysed *supra*, point 2.2.
[119] European Strategy for data, p. 11.
[120] European Strategy for data, pp. 12-15.

frameworks that shape the context, allowing lively, dynamic and vivid ecosystems to develop. [...]"[121].

The DGA is the concretisation of this vision. It notably aims to "improve the conditions for data sharing in the internal market, by creating a harmonised framework for data exchanges and laying down certain basic requirements for data governance, paying specific attention to facilitating cooperation between Member States"[122]. In other words, the main purpose of the DGA is to promote rules that help organisations to share and re-use data while fully respecting fundamental rights (such as the right to privacy and data protection)[123]. With this regard, the European legislator states namely that rising a European internal market in which data could be used irrespective of its physical storage location could be, *inter alia*, pivotal for the rapid development of artificial intelligence technologies[124].

The DGA intends to be applicable to all sectors indifferently[125], including then health sector. It may be completed by some sector-specific legislations, such as, for example, the future EHDS regulation. When both the DGA, i.e. the general legislation, and sector-specific legislations, e.g. the future EHDS regulation, apply, it is expressly provided that the specific one should derogate to the general one[126], which is usual. In our example, EHDS regulation would apply first and should prevail in case of inconsistencies.

2.1.3 Scope and actors involved

2.1.3.1 Structure and scope

The DGA contains four main corpuses of rules, namely (i) the one related to the re-use of certain categories of data held by public sector bodies (Chapter II), (ii) the one applicable to data intermediation services (Chapter III), (iii) the one related to data altruism operations (Chapter IV) and (iv) the one establishing a European Data Innovation Board (Chapter VI)[127].

We will only focus on the first three of these corpuses within this section, as illustrated in figure 1.

[121] European Strategy for data, p. 12.
[122] DGA, recital 3.
[123] DGA, recital. 1.
[124] DGA, recital 2.
[125] DGA, recital 3.
[126] DGA, art. 1(2) and recital 3.
[127] See DGA, art. 1(1).

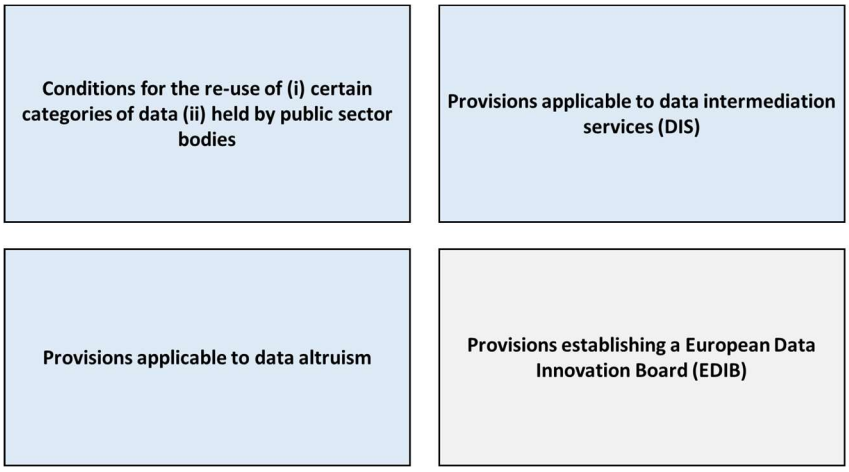


Figure 1 Main corpuses of rules within the DGA

The idea is to identify the impacts the DGA could have on TEF-Health project when designing the TEF-Health services and offering them to TEF-Health users (the SMEs).

2.1.3.2 Definitions

Data

The DGA defines broadly the concept of "data". The latest applies to "any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audiovisual recording"[128]. This formulation includes not only both personal and non-personal data, but also copyrighted works, entire data bases, trade secrets, etc.

Re-use

The notion of "re-use" of data[129] applies only to the data held by public sector bodies, whether it is performed for commercial purposes or not. Concretely, there would be a "re-use", under the DGA, if there is (i) a use, by any entity, of data (ii) held by a public sector body (iii) for another purpose that the initial one. The key-criterion of this definition is therefore the change of purpose for which the data are processed.

Article 2(2) of DGA also provides that the exchange of data between public sector bodies purely in pursuit of their public tasks is not a "re-use".

[128] DGA, art. 2 (1).
[129] DGA, art. 2 (2).

Data holder

Under the DGA, the "data holder" is a legal or natural person "[...] who is not a data subject with respect to the specific data in question, which, in accordance with applicable Union or national law, has the right to grant access to or to share certain personal data or non-personal data"[130].

It would include, for example, hospitals storing health data of their patients and having the right to share them under the conditions provided by the EHDS proposal[131].

Data user

The data user is a legal or a natural person who has access to and the right to legally use the data[132].

A SME using the data of patients, based on their consent, to develop AI solutions is an example of data user.

Data sharing

The concept of data sharing is applicable to the voluntary provision of data by a data subject or a data holder to a data user for the purpose of the joint or individual use of such data[133]. It may be subject to a fee or free of charge with this regard[134].

Data sharing may be qualified as "direct" or "indirect"[135]. It is "direct" when the data subject or the data holder shares himself the data with the data user and has a direct relationship with him (figure 2 below). On the contrary, it is "indirect" when it passes through an intermediary for doing so (figure 3 below).

[130] DGA, art. 2 (8).
[131] See *infra* point 2.2.3 of this document for what is related to the conditions under which data holders, such as hospitals in this example, must/may share the data they held according to the EHDS proposal.
[132] DGA, art. 2 (9).
[133] DGA, art. 2(10).
[134] DGA, art. 2(10).
[135] Article 2 (10) DGA provides that the provision of data may occur "[...] directly or through an intermediary".

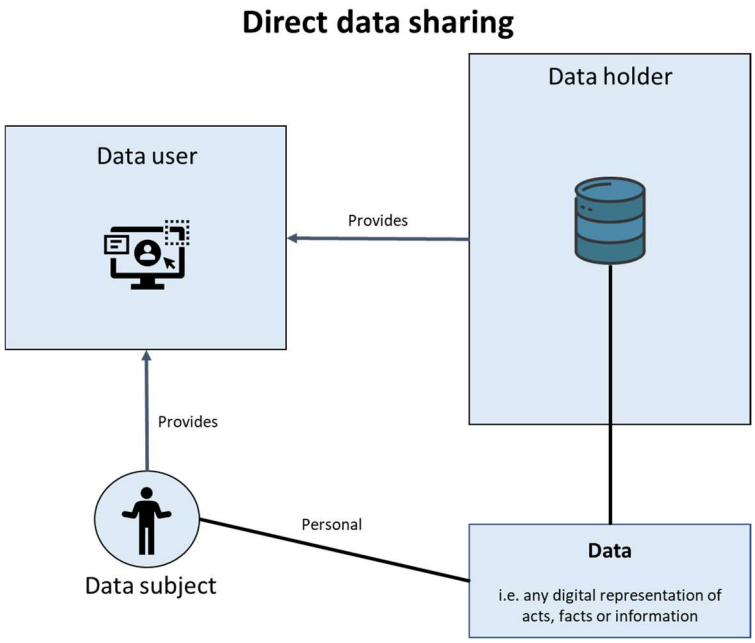


Figure 2 Direct data sharing

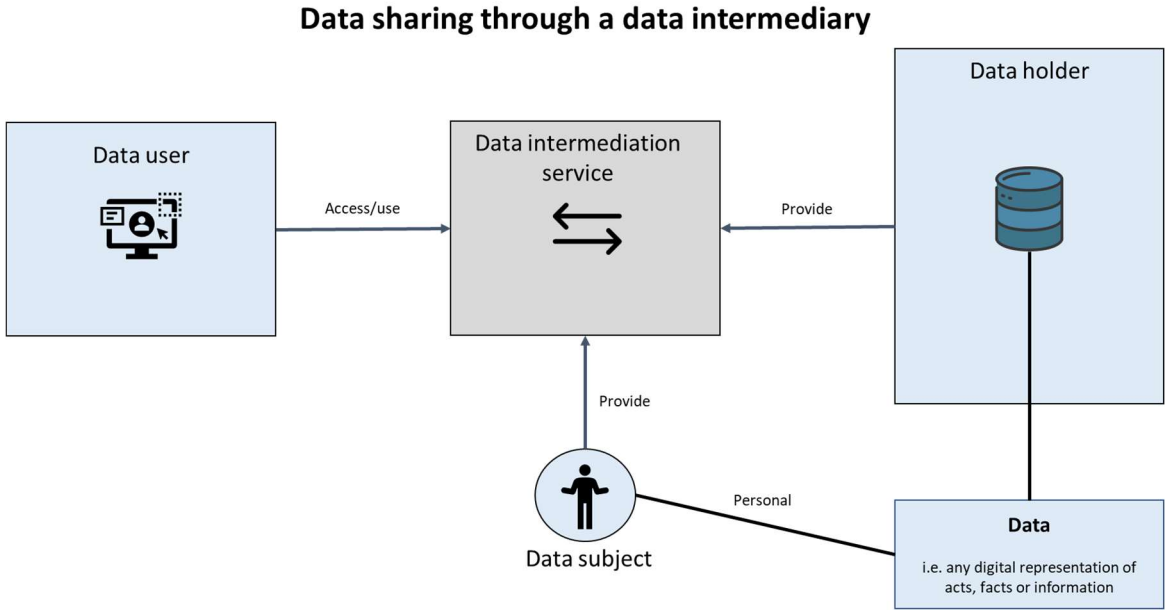


Figure 3 Indirect data sharing

Data intermediation service (DIS)

The DGA defines the "data intermediation service" (hereafter also "DIS") as a

i. service
ii. which aims to establish commercial relationships
iii. for the purpose of (indirect) data sharing
iv. between an undetermined number of data subjects or holders on the one hand and
v. an undetermined number of data users on the other hand[136].

In practice, it means that a data intermediation service is a data intermediary (such as data marketplaces[137], e.g.) that aims to establish commercial relationships between data users and data holders or subjects, even if the intermediary itself is a not-for-profit organisation[138] for example. The establishment of a commercial relationship between users and data subjects or holders is the key-criterion.

It is expressly stated that the concept of DIS includes organisations pursuing purposes linked to the exercise of the rights of data subjects in relation to personal data[139].

On the contrary, it is also provided that services which tend to enrich or transform the data in order to add substantial value and to license it are not DIS, unless they establish a commercial relationship between holders and users[140]. Services that focus on the intermediation of copyright-protected contents (e.g., YouTube or Twitch) are excluded[141]. This is also the case of data sharing services offered by public sector bodies that do not aim to establish commercial relationships[142]. Finally, services that are exclusively used by one data holder in order to enable the use of the data held by that data holder, or that are used by multiple legal persons in a closed group are neither considered as DIS[143]. With regard to this last point, the recitals give the example of "[...] supplier or customer relationships or collaborations established by contract, in particular those that have as a main objective to ensure the functionalities of objects and devices connected to the Internet of Things"[144].

Data altruism

Data altruism is a particular form of data sharing, which, as is, could also be direct or indirect.

[136] DGA, art. 2 (11).
[137] DGA, art. 10 (a) and recital 28.
[138] DGA, art. 15.
[139] DGA, art. 10 (b).
[140] DGA, art. 2 (11).
[141] DGA, art. 2 (11) (b).
[142] DGA, art. 2 (11) (c).
[143] DGA, art. 2 (11) (d).
[144] DGA, recital 28.

It is characterised by two main specificities:

- First, it implies (i) a permission from the data holder (if the data are non-personal) or (ii) the consent of the data subject (if the data are personal). Such permission or consent cannot be given for profit purposes[145]. At most, the data holder or subject may share the data at the cost price. In this context, it differs from the DIS hypothesis since no commercial relationship is established between the data holders or subjects and the data users.

- Second, the sharing must be performed for pursuing a general interest objective, such as healthcare for example[146]. The DGA does not contain an exhaustive list of what could be such general interest objectives, it only gives some examples[147]. It should therefore be assessed on a case-by-case basis if a specific objective may be qualified as a general interest one. One can already note that the regulation aims, with this regard, "[...] to contribute to the emergence of sufficiently sized data pools made available on the basis of data altruism in order to enable data analytics and machine learning, including across the Union [...]"[148].

2.1.4 Requirements to be complied with

2.1.4.1 Conditions for the re-use of certain categories of data held by public sector bodies

As previously detailed, the DGA contained, in addition to the chapter dedicated to the scope and definitions, three corpuses of rules which are analysed through this section. The first one is related to the re-use of certain categories of data held by public sector bodies (Chapter II of the DGA). It aims to complete the Directive 2019/1024 on open data and the re-use of public sector information (hereafter "Open Data Directive")[149], as detailed hereafter.

It is interesting to note that this Chapter could have implications on the activities of TEF-Health Consortium.

Application to TEF Health: is/are the Consortium or/and some of its partners to be considered "public sector bodies"?

The concept of "public sector body" includes "associations formed by one or more" public sector bodies[150]. This notion is similarly defined within the Open Data Directive[151], that precises,

[145] DGA, art. 2(16).
[146] DGA, art. 2(16).
[147] Article 2(16) of the DGA mentions healthcare, combating climate change, improving mobility, facilitating the development, production and dissemination of official statistics, improving the provision of public services, public policy making or scientific research purposes in the general interest.
[148] DGA, recital 45.
[149] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (recast), *O.J.*, L 172/56, 26 June 2019.
[150] DGA, art. 2 (17).
[151] Open Data Directive, art. 2(1).

in addition, that the notion comes from the directive 2014/24 on public procurement (hereafter "Directive 2014/24")[152,153]. More specifically, the notion is defined the same manner as the concept of "contracting authorithy" in the Directive 2014/24. This last directive referred to a case law intended to clarify which entity must be considered a "contracting authority"[154]. However, this case law is mainly linked to the notion of "bodies governed by public law"[155] and the question is, according to us, left open. It must be analysed on a case-by-case basis[156].

With this regard, it remains uncertain whether the Consortium and/or some of its partners shall be considered itself/themselves public sector bodies under the meaning of the DGA. In addition, it shall be stressed that all the TEF-Health partners that are "contracting authorities" within the meaning of the directive 2014/24 shall be considered public sector bodies under the DGA.

Public hospitals may for, instance, "[...] be qualified as public sector bodies under European law"[157].

The provisions of Chapter II of DGA may also be interesting for TEF Health Consortium because it may have to re-use data held by other public sector bodies and falling into one the categories of data expressly identified in DGA.

Scope of the main legal implications

DGA aims to complete the Open Data Directive. The Open Data Directive sets of minimum rules governing the re-use of existing documents held by public sector bodies and by some public undertakings[158]. With this regard, the European legislator has specified in the recitals of the DGA that the directive "[...] ensure[s] that the public sector bodies make more of the data they produce easily available for use and re-use. However, certain categories of data, such as commercially confidential data, data that are subject to statistical confidentiality and data protected by intellectual property rights of third parties, including trade secrets and personal data, in public databases are often not made available [...]"[159].

This is why the DGA focuses on the re-use of these types of data. Indeed, the categories of data held by public sector bodies falling within the scope of the Chapter II of DGA are those which are protected on grounds of:

i. commercial confidentiality,
ii. statistical confidentiality,
iii. intellectual property rights of third parties or

[152] Open Data Directive, recital 29.
[153] Directive (EU) 2014/24 of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC, *O.J.*, L 94/65, 28 March 2014 (hereinafter "Directive 2014/24").
[154] Directive 2014/24, recital 10.
[155] See Directive 2014/24, recital 10.
[156] Directive 2014/24, recital 11.
[157] Free translation ; B. CAMBRIER, P. LAGASSE and A. PATERNOSTRE, "Les concepts régissant le champ d'application ratione personae", in S. Ben Messaoud et F. Viseur (dir.), *Marchés publics*, 1st edition, Brussels, Larcier, 2014, p. 70.
[158] Open Data Directive, art. 1 (a) (b).
[159] DGA, recital 6.

iv. the protection of personal data (provided that these personal data do not fall within the scope of the Open Data Directive)[160].

Main legal obligations – A prohibition of exclusive agreements

With regard to these categories of data held by public sector bodies, the DGA prohibits agreements (or similar practices) "[...] which grant exclusive rights or which have as their objective or effect to grant such exclusive rights or to restrict the availability of data for re-use by entities other than the parties to such agreements [...]"[161].

A derogation is only possible "[...] to the extent [that such an agreement is] necessary for the provision of a service or the supply of a product in the general interest that would not otherwise be possible"[162] and provided that its duration does not exceed 12 months[163] and is transparent and made publicly available online[164].

Main legal obligations – The conditions of the re-use

Additionally, the regulation gives precisions on the conditions under which a re-use of the data concerned may occur[165].

- It states, for example, that these conditions must be made publicly available by the public sector body which is competent to grant or refuse access to the re-use[166].
- The public sector body shall ensure that the protected nature of data is preserved[167]. It may, with this regard, provide for requirements related (i) to the anonymisation or the data shared prior to their re-use[168], (ii) to the access to the data remotely within a secure environment controlled by the public sector body[169] or (iii) to access and re-use the data within the physical premises of the public sector body in some circumstances[170].
- All the information that must be made available in accordance with what we previously said must be easily accessible at a single information point, which is competent to receive enquiries or requests for the re-use[171]. Re-users must follow a specific procedure in order to introduce a request, such procedure being also established by the DGA[172].

[160] DGA, art. 3 (1) (a) to (d).
[161] DGA, art. 4 (1).
[162] DGA, art. 4 (2).
[163] DGA, art. 4 (4).
[164] DGA, art. 4 (5).
[165] DGA, art. 5.
[166] DGA, art. 5 (1).
[167] DGA, art. 5 (3).
[168] DGA, art. 5 (3) (a) (i).
[169] DGA, art. 5 (3) (b).
[170] DGA, art. 5 (3) (c).
[171] DGA, art. 8 (1) and (2).
[172] DGA, art. 9.

2.1.4.2 Data intermediation services (DIS)

Application to TEF Health: which qualifications for the Consortium and/or its partners, TEF-Health users (the SMEs) regarding this notion of DIS?

It must be questioned whether the Consortium, or several of its partners or TEF-Health users (the SMEs) could be qualified DIS under DGA.

For instance, according to the Grant agreement, the WP4 will have to "[set up] a TEF dataspace of health data, where trusted stakeholders can safely share, merge and use datasets based on high quality consensus standards and practices and incentive mechanisms. This dataspace will capitalize as much as possible on existing infrastructures (EBRAINS, HDH, various university hospitals) and ensure interoperability with external dataspaces"[173]. With this regard, the Consortium, and/or the partners of WP4 concerned by such a task, could be qualified as intermediaries establishing relationships between data users, i.e. TEF-Health user (the SMEs), and data holders, i.e. the existing infrastructures such as EBrains, HDH and the various university hospitals.

This is represented by figure 4 below.

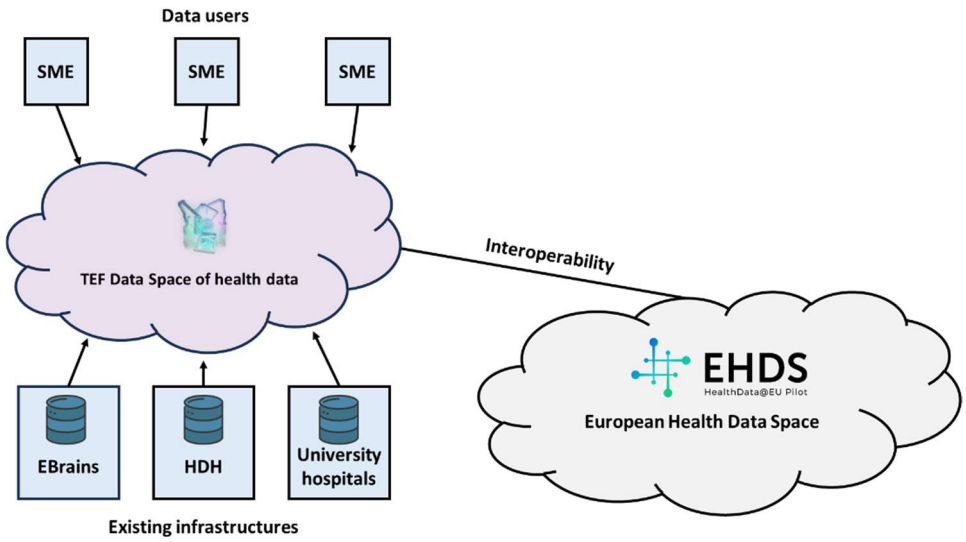


Figure 4 Relationship between the SMEs, the existing infrastructures and the TEF Data Space of health data

In this context, some services offered by the Consortium might be considered DIS under the conditions that they (i) aim to establish commercial relationships between an (ii) undetermined number of data holders and (iii) data users[174]. With this respect, it should therefore be clarified whether the Consortium, and/or the partners concerned, aim(s) to establish a commercial relationship between the dataset's holders and TEF-Health users (the SMEs) through the TEF

[173] Grant agreement, Annex 1 – Description of the action (Part A), List of Work packages, p. 11.
[174] DGA, art. 2 (11).

dataspace of health data. That would be the case if data holders intend to make profit from the provision of the data they held.

Second, it is unclear whether the number of data holders concerned will be undetermined or not. If this is not the case, the Consortium's services regarding the data space will not be considered as DIS.

Under the condition that it is granted legal personality, the Consortium, or some of its partners, could also be qualified data users, given that they have lawful access to personal and non-personal data and have the right, including under GDPR for what concerns personal data, to use these data for certain purposes[175]. If it is granted legal personality, the Consortium, or some of its partners, will also be considered data holders, having the right to share or to grant access to certain personal or non-personal data to TEF-Health users (the SMEs)[176].

As far as they are concerned, it is clearer that both the hospitals, partners in the Consortium, and TEF-Health users (the SMEs) will be qualified data users, since they must have the right to use the data put are their disposal in the TEF data space of health data. Hospitals will also be considered data holders of the data they make available within the TEF data space of health data.

Main legal implications

Before offering the intermediation services, the DIS shall submit a notification to the competent authority for data intermediation services, which will be established with this regard by the Member State concerned[177] [178].

We must stress that when a DIS is established in more than one Member State, it shall be deemed to be under the jurisdiction of the one in which it has its main establishment[179]. For instance, if one considers the whole Consortium as a DIS, it shall probably be Germany[180], but this has to be confirmed.

The notification must at least include some information such as, among others, the data intermediation services provider's legal status or its contact persons and contact details[181].

Once it has notified the authority, the DIS may start the activity under some conditions[182]:

- For example, it may not use the data for which it provides data intermediation services for purposes other than to put them at the disposal of data users[183].

[175] DGA, art. 2(9).
[176] DGA, art. 2(8).
[177] DGA, art. 11(1).
[178] DGA, art. 13.
[179] DGA, art. 11 (2).
[180] Since Charité, i.e., TEF-Health project's coordinator is established in this Member State; recital 41 DGA precises, indeed, that: "The main establishment of a data intermediation services provider in the Union should be the place of its central administration in the Union. The main establishment of a data intermediation services provider in the Union should be determined in accordance with objective criteria and should imply the effective and real exercise of management activities [...]".
[181] For all the information that must be provided, see art. 11(6).
[182] DGA, art. 11 (10).
[183] DGA, art. 12 (a).

- In addition, it must ensure that the procedure for access to its services is fair, transparent and non-discriminatory for both data subjects and data holders[184]. The commercial terms, including pricing, for the provision of the services must also, e.g., "[...] not be dependent upon whether the data holder or data user uses other services provided by the same data intermediation services provider or by a related entity, and if so to what degree the data holder or data user uses such other services"[185].

Upon request from the DIS, the competent authority must confirm its compliance with Article 11 (notification procedure) and 12 (conditions for performance of data intermediation services)[186]. The DIS having received this confirmation will have the right to use the label 'data intermediation services recognised within the Union'[187]. Of course, DIS must also notify the competent authority of any changes in the information it has to provide under Article 12[188] or if it ceases its services[189].

The competent authorities must ensure compliance of all DIS with the requirements set out in Chapter III of the DGA, including on the basis of a request of a legal or natural person[190]. When it finds an infringement, the competent authority must notify the DIS and gives it 30 days to state its views[191]. To ensure compliance, the competent authority may take different measures when it finds an infringement[192]. These measures include imposition of administrative fines, suspension of the services until the correction of the situation and asking for definitive cessation of the services in case of repetitive infringement[193].

The European Commission will also be notified of every new notification by the competent authorities and will maintain a register of all DIS that are active within the European Union[194].

Note that all DIS shall comply with their obligations pursuant to Chapter III of the DGA by 24 September 2025. On their side, Member States had to designate their competent authority regarding DIS by 24 September 2023[195].

[184] DGA, art. 12(f).
[185] DGA, art. 12(b).
[186] DGA, art. 11(9).
[187] DGA, art. 11(9) ; The Commission has adopted the label and the common logo mentioned within the provision ; They are available on https://digital-strategy.ec.europa.eu/en/library/logos-data-intermediaries-and-data-altruism-organisations-recognised-union.
[188] DGA, art. 11(12).
[189] DGA, art. 11(13).
[190] DGA, art. 14(1).
[191] DGA, art. 14(3).
[192] DGA, art. 14(4).
[193] DGA, art. 14(4).
[194] DGA, art. 11(10) ; This register is empty on 10 October 2023 as no DIS has already been notified yet ; It is however already available on https://digital-strategy.ec.europa.eu/en/policies/data-intermediary-services.
[195] DGA, art. 13 (1).

2.1.4.3 Data altruism

Application to TEF Health: could the Consortium, and/or some of their partners, be deemed as offering data altruism services?

The services offered to TEF-Health users (the SMEs) by the Consortium, and/or some of their partners, should probably not be considered as data altruism ones in our view. Indeed, in order to be so, data should be made available for general interest (such as healthcare) purposes "[...] as provided for in national law, where applicable [...]"[196]. It is not the case of the data that will be provided to TEF-Health users (the SMEs) by the Consortium for testing and certification purposes since this provision will not be processed under a specific national law.

On the contrary, the possibility that data holders, i.e. notably the hospitals, will be considered as data altruism organisations exists if the national law of their country of establishment provides conditions under which they may make data available for healthcare purposes[197] and provided that (i) they operate on a not-for-profit basis and are legally independent from any entity that operates on a for-profit basis, (ii) that they carry out their data altruism activities through a structure that is functionally separate from their other activities and that they (iii) comply with the rulebook referred to in article 22 DGA[198].

Main legal applications

On this field, it should be noted that Member States may have in place technical or organisational arrangements to facilitate data altruism, they may e.g. establish national data altruism policies[199].

Second, in order to provide data altruism services, entities must obtain a registration into a public national register of data altruism organisations, kept and regularly updated by each authority competent with this regard[200]. The European Commission must also maintain such a register, for information purposes[201].

Provided that it is properly registered in its public national register of data altruism organisations, an entity is habilitated to use the label "data altruism organisation recognised in the Union", as well as a common logo[202] established by the European Commission, in its written and spoken communication[203].

[196] DGA, art. 2(16).
[197] See hereinafter what it may imply regarding the obtention of a status of "recognised" data altruism organisation.
[198] DGA, art. 18.
[199] DGA, art. 16.
[200] DGA, art. 17(1).
[201] DGA, art. 17(2) ; This register is available on https://digital-strategy.ec.europa.eu/en/policies/data-altruism-organisations.
[202] This logo is available on https://digital-strategy.ec.europa.eu/en/library/logos-data-intermediaries-and-data-altruism-organisations-recognised-union.
[203] DGA, art. 17(2).

In order to be able to be registered that way, an entity must meet several requirements[204]. It must of course carry out data altruism activities[205] , "be a legal person established pursuant to national law to meet objectives of general interest as provided for in national law, where applicable"[206] and "carry out its data altruism activities through a structure that is functionally separate from its other activities"[207]. Once an organisation meets all these requirements, it must follow a specific procedure for application, detailed in article 19. This provision includes, for instance, some information which must be contained in the application[208].

In order to enhance transparency, recognised data altruism organisations must then keep four different records regarding:

i. all natural or legal persons that were given the possibility to process data held by that recognised data altruism organisation, and their contact details,
ii. the date or duration of the processing of personal data or use of non-personal data[209],
iii. the purpose of the processing as declared by the natural or legal person that was given the possibility to process and
iv. the fees paid by natural or legal persons processing the data, if any[210].

Recognised data altruism organisations must transmit an annual activity report to the relevant competent authority[211].

They must also respect several requirements intended to safeguard rights and freedoms of data subjects and data holders whose data are collected for general interest purposes[212]. They must, for example, inform them prior of the processing about the objectives of general interest for which the data are processed or shall provide tools (e.g. webforms) for obtaining consent from data subjects or permissions to process data made available by data holders[213].

As it is the case of competent authorities for DIS, competent authorities for data altruism organisations will ensure compliance of data altruism organisations with all the provisions previously detailed[214]. If it founds an infringement, the competent authority will first notify the data altruism organisation concerned[215]. If the organisation does not react after this notification, it will "[...] lose its right to use the label 'data altruism organisation recognised in the Union' in any written and spoken communication"[216] and/or will "be removed from the relevant public

[204] DGA, art. 18.
[205] DGA, art. 18 (a).
[206] DGA, art. 18 (b).
[207] DGA, art. 18 (d).
[208] DGA, art. 19(4).
[209] DGA, art. 20(1).
[210] DGA, art. 20(1).
[211] DGA, art. 20(2).
[212] DGA, art. 21.
[213] DGA, art. 21(1) and (3).
[214] DGA, art. 24.
[215] DGA, art. 24(4).
[216] DGA, art. 24(5) (a).

national register of recognised data altruism organisations and the public Union register of recognised data altruism organisations"[217].

Finally, the text gives power to the European commission regarding the establishment of a "European data altruism consent form" which "[...] shall allow the collection of consent or permission across Member States in a uniform format"[218]. This consent will give data altruism organisations the opportunity to fit with the requirements set out by the regulation regarding the provisions of tools with this regard and will "[...] contribute to additional transparency for data subjects that their data will be accessed and used in accordance with their consent and also in full compliance with the data protection rules. It should also facilitate the granting and withdrawing of consent and be used to streamline data altruism carried out by undertakings and provide a mechanism allowing such undertakings to withdraw their permission to use the data [...]"[219]. It is also stated that: "[...] In order to take into account the specificities of individual sectors, including from a data protection perspective, the European data altruism consent form should use a modular approach allowing customization for specific sectors and for different purposes"[220].

[217] DGA, art. 24(5) (b).
[218] DGA, art. 25(1).
[219] DGA, recital 52.
[220] DGA, recital 52.

2.2 European Heath Data Space proposal

2.2.1 Context and purposes of the proposal

2.2.1.1 Adoption procedure status

The European Health Data Space (hereafter "EHDS") proposal[221] deals with data in the specific sector of health.

The initial proposal for this text was adopted by the European Commission on 3rd May 2022[222]. EHDS proposal is still in negotiations. This contribution is based on this initial proposition of the European Commission.

On the 7th of December 2023, the Council agreed its position and gave mandate for negotiations with the European Parliament[223]. On 13rd of December 2023, the European Parliament adopted amendments and finalized its position[224]. However, as this report had to be submitted for the Consortium review on 1st December 2023, it could not take the content of these two positions into account. This section will be updated after the formal approvals of the Parliament and the Council and after the publication of the final draft in the Official Journal.

2.2.1.2 Main purpose of the proposal

The EHDS proposal is a key pillar of a strong European Health Union and would be the first common EU data space in a specific area, namely the health sector, to emerge from the European strategy for data[225].

EHDS proposal focuses specifically on the *access,* the *control* and on the *sharing* of electronic health data.

According to the proposal of the European Commission, the general purpose of the EHDS proposal is to create a health specific ecosystem comprised of rules, common standards and practices, infrastructures and a governance framework that aims at[226]:

- First, *empowering individuals* through increased digital access to and control of their electronic personal health data, at national level and EU-wide, and support to their free

[221] Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space, COM(2022) 197 final, 3 May 2022.
[222] *Ibid*.
[223] Proposal for a Regulation on the European Health Data Space – Mandate for negotiations with the European Parliament, 2022/0140(COD), 7 December 2023.
[224] Amendments adopted by the European Parliament on 13 December 2023 on the proposal for a regulation of the European Parliament and of the Council on the European Health Data Space, COM(2022)0197.
[225] Communication from the Commission - A European strategy for data, COM(2020) 66 final, 19 February 2020,. A. KISELEVA and P. DE HERT., "Creation a European Health Data Space. Obstacles in Four Key Legal Areas", *E.P.L.R.*, available on https://papers.ssrn.com, 2021, p. 1.
[226] EHDS proposal, art. 2.

movement, as well as fostering a genuine single market for electronic health record systems, relevant medical devices and high-risk AI systems. The EHDS proposal refers to this as "primary use of data"[227].

- Secondly, providing a consistent, trustworthy and efficient set-up for *the use of health data for research, innovation, policy-making and regulatory activities*. This is called by EHDS proposal "secondary use of data"[228].

This diagram from the European Commission illustrates the purposes of the EHDS proposal. In violet, we made a focus on the purposes which concern specifically TEF-Health.

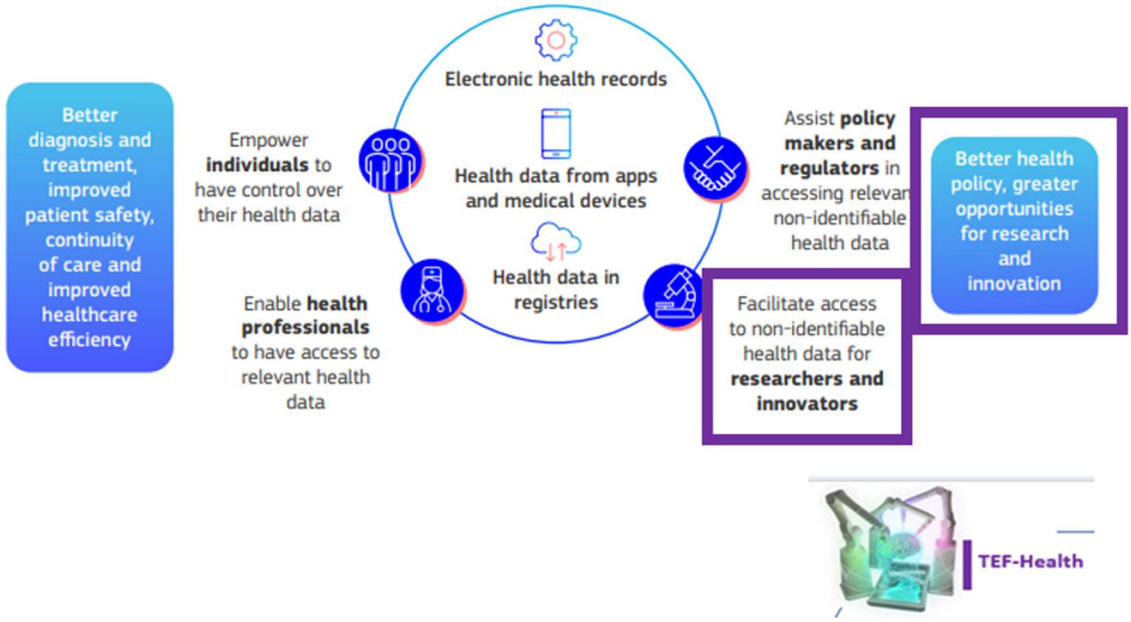


Figure 5 Objectives and benefits for users of EHDS, European Commission, adapted by the author for TEF-Health project (framed parts relevant for TEF-Health)[229]

[227] EHDS proposal, art. 2 (d): 'primary use of electronic health data' means the processing of personal electronic health data for the provision of health services to assess, maintain or restore the state of health of a natural person to whom the data relates, including the prescription, dispensation and provision of medicinal products and medical devices, as well as for relevant social security, administrative or reimbursement services.

[228] EHDS proposal, art. 2 (e): 'secondary use of electronic health data' means the processing of electronic health data for purposes set out in Chapter IV of this Regulation. The data used may include personal electronic health data initially collected in the context of primary use, but also electronic health data collected for the purpose of the secondary use.

[229] Figure illustrating the objectives and the benefits for users of the European Health Data Space, FactSheet of the Directorate-General for Health and Food Safety, 3rd May 2022, available online: EUROPEAN HEALTH DATA SPACE (europa.eu). Figure adapted by UNamur - CRIDS to the TEF-Health project.

The second purpose of the EHDS proposal (i.e. providing a framework for the secondary use of health data) is particularly relevant for TEF-Health project.

Access to health data will indeed be essential for developing, testing and ensuring the safety of medical devices involving artificial intelligence before their put into service or on the market[230]. As indicated in the communication of the European Commission concerning the European Health Data Space, by providing a secure access to health data, the EHDS proposal will have a great impact on industry[231]. It will indeed benefit from data that could help the industry develop new medical devices involving artificial intelligence[232]. As expressly mentioned in the Strategy, the construction of the so-called European health data space combined with testing and experimentation facilities, such as TEF-Health, will greatly boost and accelerate innovation[233].

Given the importance of the secondary use of data in TEF-Health project, this analysis of EHDS proposal will only be focused on this aspect.

2.2.2 Scope and actors involved

2.2.2.1 Access to electronic health data for secondary use

Concerning the secondary use of electronic health data, the EHDS proposal lays down rules and mechanisms supporting this use and establishes a mandatory cross-border infrastructure[234]. The regulation concerning the secondary use of electronic health data is contained in chapter IV of EHDS proposal.

Market actors involved

According to Article 1.3 of EHDS proposal, the regulation will apply :

- To *manufacturers and suppliers* of Electronic Health Record (HER) systems[235] and wellness applications[236] placed on the market and put in service in the EU and to the *users* of such products;

[230] For an analysis of the legal framework for the marketing of medical devices (namely, the Medical Devices Regulation), see Annex 1, point 2.
[231] Communication from the Commission to the European Parliament and the Council, "A European Health Data Space: harnessing the power of health data for people, patients and innovation", 3rd May 2022, COM(2022 196 final, p. 16.
[232] *Ibid*.
[233] *Ibid*.
[234] EHDS proposal, art. 1(2) (c) and (e).
[235] EHDS, art. 2(2) (n): 'EHR system' (electronic health record system) means "any appliance or software intended by the manufacturer to be used for storing, intermediating, importing, exporting, converting, editing or viewing electronic health records".
[236] EHDS, art. 2(2) (o): 'wellness applications' means "any appliance or software intended by the manufacturer to be used by a natural person for processing electronic health data for other purposes than healthcare, such as well-being and pursuing healthy life-styles".

- To *controllers and processors* established in the EU processing electronic health data of Union citizens and third-country nationals legally residing in the territories of Member States;
- To *controllers and processors* established in a third country that has been connected to or are interoperable with MyHealth@EU[237];
- To *data users* to whom electronic health data are made available by *data holders* in the EU.

According to EHDS proposal:

- *data holder* means:
  - "any natural or legal person, which is an entity or a body in the health or care sector, or performing research in relation to this sectors, as well as Union institutions, bodies, offices and agencies"
  - "who has the right or obligation, in accordance with this Regulation, applicable Union law or national legislation implementing Union law, or in the case of non-personal data, through control of the technical design of a product and related services, the ability"
  - "to make available, including to register, provide, restrict access or exchange certain data"[238].
- *data user* means a "natural or legal person who has lawful access to personal or non-personal electronic health data for secondary use"[239].

National competent authorities

To ensure the governance and mechanisms for the secondary use of electronic health data, EHDS proposal creates the notion of "health data access bodies". "Health data access bodies" must be designated by each Member State.

Member States are allowed to design more than one health data access body. Where a Member State designates several health data access bodies, it must designate one health data access body to act as coordinator, with responsibility for coordinating requests with the other health data access bodies[240].

Health data access bodies are the entities which are responsible, among other tasks[241], to ensure that electronic health data are made available by data holders to data users[242]. In practice, those national bodies play a role of intermediary between data holders and data users. Health data access bodies can be new organizations of a Member State which provide access to

[237] According to article 2 (t) 'MyHealth@EU' means the cross-border infrastructure for primary use of electronic health data formed by the combination of national contact points for digital health and the central platform for digital health.
[238] EHDS proposal, art. 2(2) (y).
[239] EHDS proposal, art. 2(2) (z).
[240] EHDS proposal, art. 36(1).
[241] EHDS proposal, art. 37
[242] EHDS proposal, art. 36.

electronic health data to third parties, or being part of an existing organization, as a data intermediation service building on the Data Governance Act[243].

This diagram aims to shows the relations between the different players involved.

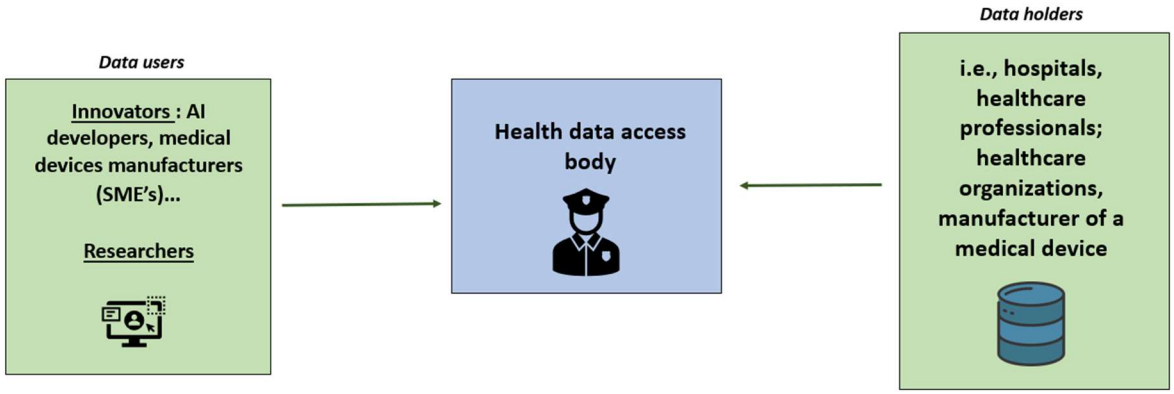


Figure 6 Illustration of the actors involved

The qualifications of *data holders* and *data users* are particularly relevant in the case of secondary use and in the case of TEF-Health. Applied to TEF-Health project, indeed, several partners of Consortium could be both *data users* and *data holders*. Some members of WP4 (hospitals like CHU of Charleroi and CHU of Rennes) might be deemed as *data holders* since they hold datasets of their patients collected during their medical activities (clinical trials, treatments, ...). In the same time, members of WP4 could also be considered *data users*, as they could need datasets from other data holders to develop their testing infrastructures[244]. SMEs participating to TEF-Health project would be considered as *data users* when they ask access to data for secondary use in the context of the development of a product.

2.2.2.2 Cross-border access to electronic health data for secondary use

When the data user and the data holder are from different Member States, we refer to it as "cross-border access to electronic health data".

[243] EHDS proposal, explanatory memorandum, p. 13.
[244] Grant Agreement, Annex 1 – Description of the action (Part A), List of Work packages, p. 11, T4.1 : "set-up the evaluation protocols, tools and digital facilities to provide virtual testing services based on datasets".

EHDS proposal creates the "HealthData@EU", which is a decentralized infrastructure responsible for making electronic health data available for secondary use in a cross-border context[245].

Concretely, to facilitate the cross-border access to electronic health data for secondary use, EHDS proposal sets up a system in which only *authorised participants* can connect to the platform "HealthData@EU". Several entities can be recognized as "authorised participants"[246].

Among the different authorised participants provided for in EHDS proposal, there are the *national contact points for secondary use of electronic health data*. These national contact points are designated by each Member State. They are responsible for making electronic health data available for secondary use in a cross-border context[247] [248].

Moreover, health-related research infrastructures or similar structures which functioning is based on European Union law and which support the use of electronic health data for research, policy making, statistical patient safety or regulatory purposes are also authorised participants of HealthData@EU[249].

This last hypothesis regarding health-related research or similar infrastructures could be of interest for TEF-Health. It could indeed cover the participation of some partners of TEF-Health as authorised participants to HealthData@EU (notably, hospitals within WP3 and WP4 which provide testing facilities).

When cross-border registries and databases are concerned, the health data access body of the Member State in which the data holder is registered must be competent to decide on the data access applications to provide electronic health data[250]. Each authorized participant shall acquire the required technical capability to connect to and participate in HealthData@EU[251].

The following figure, issued from the European Commission, aims to show the so-called HealthData@EU infrastructure to be created and the various relationship for sharing of health data it will allow.

[245] EHDS proposal, art. 52.
[246] EHDS proposal, art. 52(2) 52(3), 52(4), and 52(5).
[247] EHDS proposal, art. 52(1). EHDS proposal, art. 2 (u) defines 'national contact point for secondary use of electronic health data' as being an "organizational and technical gateway enabling the cross-border secondary use of electronic health data, under the responsibility of Member States".
[248] The national contact point can be the coordinator for the health data access bodies designated when several health data access bodies have been designated by a Member State; see EHDS proposal, art. 52(1); Regarding the coordinator, see *supra*, point 2.2.2.1.
[249] EHDS proposal, art. 52.3.
[250] EHDS proposal, art. 53.1.
[251] EHDS proposal, art. 52.6.

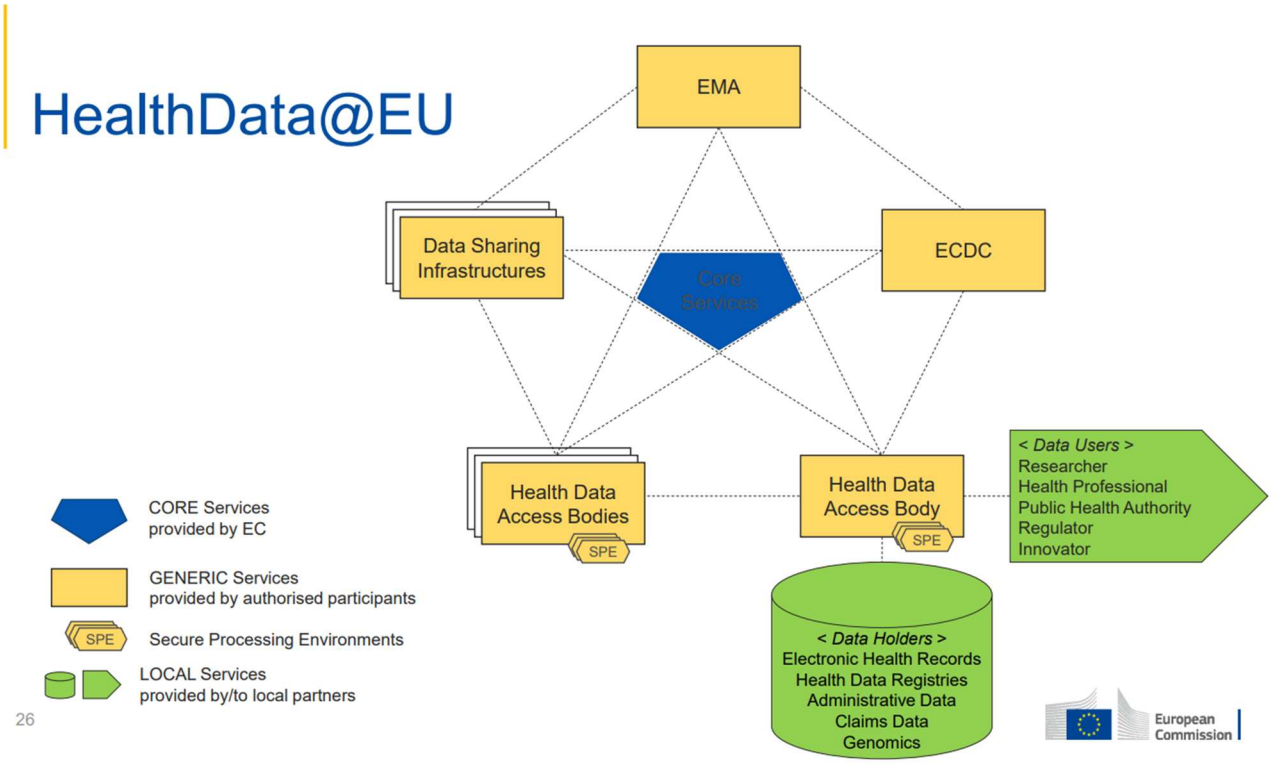


Figure 7 European Health Data Space, Harnessing the power of health data for people, patients and innovation European Commission[252]

This diagram shows how the HealthData@EU should work in practice. Yellow rectangles represent authorised participants which are directly connected at HealthData@EU platform (represented by the blue shape) and who are playing the role of intermediary between, on the one hand, the infrastructure HealthData@EU and, on the other hand, data holders and data users who are based in different Member States. The diagram also includes other European agencies as authorized participants, such as the EMA[253] and the ECDC[254], as they are health-related research infrastructures whose functioning is based on Union Law[255].

[252] European Commission, European Health Data Space, Harnessing the power of health data for people, patients and innovation, slide 26, available on https://www.esante.lu/portal/de/service_project/doc_manager/download.php?&vars=KfuGTISFds4R2dSQeigbHYuY0Yp0qSju1xqY%2AwVftu8, 1st July 2022.

[253] EMA is the acronym of "European Medicines Agency" which is a decentralized agency of the European Union responsible for the scientific evaluation, supervision and safety monitoring of medicines in the EU.

[254] ECDC is the acronym of « European Center for Disease Prevention and Control" which is a decentralized agency of the European Union which aimed at strengthening Europe's defences against infectious diseases.

[255] EHDS proposal, art. 52(4).

Applied to TEF-Health project, it looks that the dataspace to be created by WP4 in the context of the task T4.4.2 could be considered a "data sharing infrastructure". Such data space plays the role of an intermediary that will be connected directly to the infrastructure HealthData@EU[256].

2.2.3 General requirements

2.2.3.1 Obligation of data holders to make data available

Article 33 of EHDS proposal provides that *data holders* have the obligation to put some categories of electronic health data available for secondary use. This article contains a list of fifteen categories of data that must, as a minimum, be made available[257]. Among these categories of data, we can highlight, for example, data impacting on health, electronic health data from clinical trials[258], data from electronic health records (EHRs)[259], …

Some partners of TEF-Health project, are concerned by such an obligation since they hold those categories of data collected and produced during their medical activities, for instance hospitals.

In addition, Article 33 (f) of EHDS proposal provides that "person generated electronic health data, including medical devices, wellness applications or other digital health applications" must be shared by data holders. This requirement will not apply to data holders that qualify as micro enterprises as defined in Article 2 of the Annex to Commission Recommendation 2003/361/EC[260].

It might be of interest in TEF-Health context. Manufacturers of medical devices, such as SMEs using TEF-Health services, could be considered, in some cases, as *data holders* and, as such, could be forced to share health data generated by their medical device.

Article 41 of EHDS proposal contains some general duties that data holders must comply with when they must share electronic health data in the context of EHDS, like, among others, cooperate in good faith with the health data access bodies and communicate to the health data body a general description of the dataset they hold.

Close to the obligation of data holders to make some categories of health data available, health data access bodies must provide information about the available datasets and their

[256] Grant Agreement, Annex 1 – Description of the action (Part A), List of Work packages, p. 11, T4.4.2: "Setting up of a dataspace of health data, where trusted stakeholders can safely merge and use datasets based on high quality consensus standards and practices and incentive mechanisms".
[257] It concerns, for example, the following categories of data: data impacting on health, including social, environmental behavioral determinants of health; relevant pathogen genomic data, impacting human health; human genetic, genomic and proteomic data, person generated electronic health data.
[258] EHDS proposal, art. 33(1) (j).
[259] According to Article 2(2) (m) of EHDS proposal, electronic health records means a collection of electronic health data related to a natural person and collected in the health system, processed for healthcare purposes.
[260] EHDS proposal, art. 33(2); Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (*O.J.*, L 124, 20 May 2003, p.36).

characteristics so that data users can be informed of elementary facts about the dataset and assess their possible relevance for them[261]. For this reason, each dataset should include, at least, information concerning the source, nature of data and conditions for making data available[262].

2.2.3.2 Submission of a data access application by data users

To access electronic health data in the way of secondary use, it is necessary to have a *data permit* granted by a health data access body.

According to Article 45 of EHDS proposal, any natural or legal person may submit a data access application. Data should only be used for specific purposes which are defined in article 34(1) of EHDS proposal. Among these purposes we find the one of "training, testing and evaluating of algorithms, including medical devices, AI systems and digital health applications, contributing to the public health or social security, or ensuring high levels of quality and safety of health care, of medicinal products or of medical devices"[263].

This purpose concerns specifically the object of TEF-Health project. It implies that in case EHDS proposal is adopted, innovators and researchers who are involved in the development of medical devices could submit a data access application to have access to electronic health data hold by data holders (for examples, hospitals) in the case of the development of medical devices involving AI.

Besides, Article 35 contains a list of prohibited purposes. Among them, there is notably the prohibition of taking decisions detrimental to a natural person based on their electronic health data, or the prohibition of taking decisions in relation to a natural person or groups of natural persons to exclude them from the benefit of an insurance contract or to modify their contributions and insurance premiums.

2.2.3.3 Issue of data permits by health data access bodies

When a data access application is submitted, the health data access body concerned must assess whether:

- the application fulfils one of the purposes listed in Article 34(1) of EHDS proposal,
- the requested data is necessary for the purposes listed in the application, and
- the requirements of Chapter IV of EHDS proposal are met[264], notably the respect of the principles of data minimization and purpose limitation[265] [266].

The health data access body has two months to issue or refuse a data permit[267].

---

[261] EHDS proposal, Recital 58; EHDS proposal, ar. 55, 56 and 57.
[262] *Ibid*.
[263] EHDS proposal, art. 34(1) (g).
[264] EHDS proposal, art. 37(1) (a) and 46.
[265] EHDS proposal, art. 44.
[266] EHDS proposal, art. 46(1).
[267] EHDS proposal, art. 46(3).

If all the requirements set out in Chapter IV of EHDS proposal are met, the health data access body will grant the data permit to the data user. On the contrary, the health data access body will refuse all applications that include one or more purposes listed in Article 35 of EHDS proposal or where requirements of EHDS proposal are not met[268].

The health data access body plays a role of an intermediary and must not hold data on his own.

Once the data permit is issued to the data user, the health data access body must immediately request the electronic health data from the data holder[269]. The health data access body has then two months to make the electronic health data available to the data user and, at the same time, the data holder has the obligation to put electronic health data at the disposal of the health data access body within two months from receiving the request from the health data access body[270].

Once the data permit is issued, data users have the right to access and process the electronic health data in accordance with the data permit delivered to them[271]. The data permit must set out general conditions applicable to the data user, notably the types and format of electronic health data accessed, covered by the data permit, the purposes for which data are made available, the duration of the data permit, *etc.*[272].

The following figure aims to describe the various interactions that will be necessary between the data user, the health data access body and the data holder to make the data available to the data user under EHDS proposal.

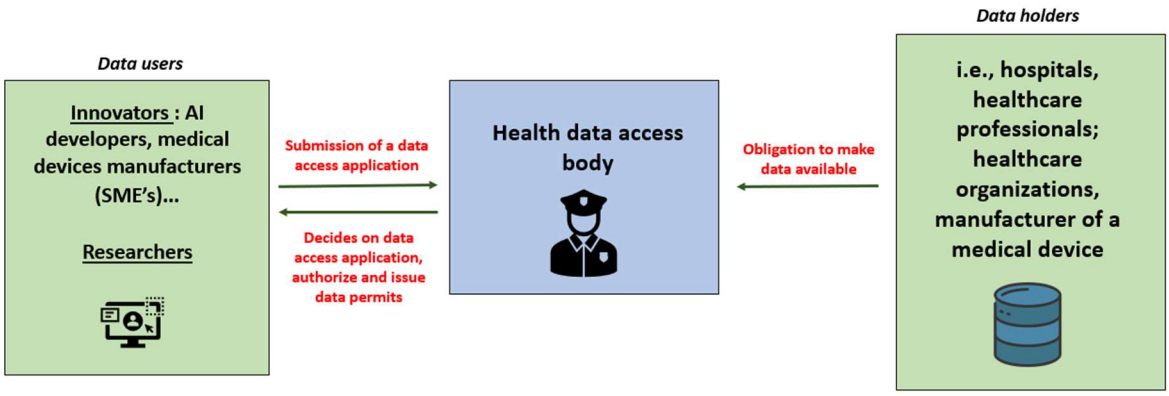


Figure 8 Interactions between data users, data holders, and health data access body

[268] EHDS proposal, art. 46(2).
[269] EHDS proposal, article 46(4).
[270] EHDS proposal, art. 46.4 and art. 41(4).
[271] EHDS proposal, art. 46(7).
[272] All general conditions are listed in Article 46(6) of EHDS proposal.

2.2.3.4 Compliance with GDPR – Legal basis for secondary use of sensitive data

Links between EHDS proposal and GDPR

The secondary use of electronic health data tackled in EHDS proposal must also be analysed as a (further) processing of health data (i.e. sensitive data) under GDPR.

It will result in various processings of data by different actors. We can identify at least the two following ones:

1) The processing of data corresponding to the transmission of the data by the data holder to the data access body (to make the data available);
2) The processing corresponding to the access to the data by the data user.

As any processing of data, besides complying with the new rules laid down in EHDS proposal, those processing(s) must be valid according to the principles of the GDPR. Indeed, the secondary use of health data under EHDS proposal will also constitute further processing(s) of data under GDPR[273] (the initial processing could be, for example, the collect of electronic health data by a healthcare professional). Such further processing(s) must be lawful in accordance with both Articles 6 (legal basis for the processing of data) and 9 (possible exemptions from the prohibition of the processing of sensitive data) of the RGPD[274].

This is specified in recital 37 of EHDS proposal.

EHDS proposal as being a basis for justifying the processing of health data despite the prohibition of Article 9 (1) GDPR

Pursuant to this recital 37, EHDS proposal "provides the legal basis in accordance with Articles 9 (2) (g)[275], (h)[276], (i)[277] and (j)[278] of Regulation (EU) 2016/679 [GDPR] for the secondary use of

[273] Regarding the rules applying to further processing, see *supra*, point 1.4.1.2.
[274] See *supra*, point 1.4.2.
[275] The processing is "necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject".
[276] The processing is "necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3".
[277] The processing is "necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy".
[278] The processing "is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject".

health data". In other words, in some precise circumstances, EHDS proposal provides the justification allowing to process health data despite the prohibition of Article 9(1) GDPR for such processing.

All of these legal bases could be interesting in the context of THE-Health, since they concerned research and the medical field. An analysis should be carried out in each case to determine which legal basis is the most appropriate for the particular case.

EHDS proposal as being legal basis for the processing of health data on ground of Article 6 GDPR - concerning the access to sensitive data by data users

At the same time, each person who asks to access electronic health data for secondary use (data applicant) for one of the purposes listed in Article 34 of EHDS proposal must also justify this processing on a legal basis of Article 6 of GDPR.

Two legal bases provided by Article 6 of GDPR could be invoked in this context:

- Article 6(1) (e) of GDPR: the processing is *necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller*.

  In this case, the data applicant should refer to another EU or national law, different from future EHDS regulation, mandating the user to process personal health data for the compliance of his tasks[279].

In TEF-Health context, for certain secondary use concerned, the data users will be the users of TEF-Health services (the SMEs). Since SMEs are not public authorities or will not carry out task in the public interest, they might not benefit from such a basis. Nevertheless, some partners of TEF-Health could be considered as public authorities. In this case, Article 6(1) (e) could be envisaged as legal basis to justify the further processing for secondary use if this purpose is necessary for the performance of a task carried out in the public interest.

- Article 6(1) (f) of GDPR: the processing is *necessary for the purposes of legitimate interests pursued by the controller or by a third party*.

  In this case, EHDS proposal provides the safeguards and data permits issued by health data access bodies define the conditions for the access to data[280].

  For the record, this lawfulness basis cannot be used by public authorities[281].

In the context of TEF-Health, when the processing for secondary use is based on article 6(1) (f) of GDPR, legitimate interests pursued by the controller could be, for example, the development of an innovative device with positive impacts on public health.

[279] EHDS proposal, recital 37.
[280] *Ibid*.
[281] See *supra*, point 1.4.2.1.

On reading the recital 37, it seems that the legal basis should be mentioned and explained in the data access applications submitted by data users.

EHDS proposal as a being legal basis for the processing of health data on ground of Article 6 GDPR - concerning the transmission of sensitive data by data holders

The transmission of health data by data holders also constitutes a further processing that must be funded on a legal basis of Article 6 of GDPR. In this case, data holders can invoke article 6(1) (c) of GDPR (processing is necessary for compliance with a legal obligation to which the controller is subject), since Article 33 of EHDS proposal creates the obligation, for data holders, to make some health data available for secondary use[282].

What about consent?

As we previously explained, EHDS proposal provides other legal bases than consent for the processing of health data for secondary use. The explanatory memorandum of EHDS proposal states that one of the aims of this proposal is precisely to permit a secondary use of health data for researchers, innovators, policy makers and regulators with a trusted governance and at lower costs than relying on consent[283]. Moreover, Article 33 of EHDS proposal – which concerns categories of health data which must be shared by data holders - provides that "where consent of the natural person is required by national law, health data access bodies shall rely on the obligations laid down in this chapter to provide access to electronic health data". By this provision, EHDS proposal sets aside consent as legal basis for processing health data for secondary use.

Nevertheless, if a data subject gives his or her explicit consent to the use of his or her data for secondary purposes that is considered compliant under GDPR[284], it goes without saying that the use of this data will then be legitimate.

[282] Recital 37 of EHDS proposal indeed precises that "for processing of electronic health data held by the data holder pursuant to this Regulation, this Regulation creates the legal obligation in the sense of Article 6(1) point (c) of Regulation (EU) 2016/679 for disclosing the data by the data holder to health data access bodies, while the legal basis for the purpose of the initial processing (e.g. delivery of care) is unaffected".
[283] EHDS proposal, explanatory memorandum, p. 13.
[284] Regarding that point, see *supra*, point 1.4.2.1.

2.3 Data Act proposal

2.3.1 Context and purposes of the regulation

2.3.1.1 Adoption procedure status

The initial Data Act proposal[285] was adopted by the European Commission on 23rd of February 2022[286]. The first reading by the Council and the European Parliament have taken place. The European parliament has made a number of amendments to the European Commission's initial version[287]. European Parliament and Council have then published a provisional agreement on the text on 7th July 2023[288]. On the 9th of November 2023, the European Parliament adopted a legislative resolution on the Data Act[289]. Finally, the 15th November 2023, the European Parliament and the Council have adopted the Regulation[290]. This is the last version adopted of the Data Act and this is the version which is used for this contribution (hereafter the "Data Act").

2.3.1.2 Main purposes of the regulation

The Data Act takes part of the European strategy for data announced in 2020 by the European Commission[291].

The European strategy aims to *regulate and foster data access and use* for seizing the opportunities presented by the digital age and to ensure fairness in the allocation of value from data among actors in the data economy[292]. In this way, the Data Acta aims to encourage and enable greater flow of data. According to article 2(1) of the Data Act, "data" means "any digital representation of acts, facts or information and any compilation of such acts, facts or information, including the form of sound, visual or audio-visual recording; content, or data obtained, generated or collected by the connected product or transmitted to it on behalf of others for the purpose of storage or processing, shall not be covered by the data act proposal"[293]. The data concerned can be personal or not personal. The Data Act aims to encourage data-

[285] Proposal for a regulation on harmonised rules on fair access to and use of data (Data Act), COM(2022) 68 final, 23 February 2022.
[286] *Ibid*.
[287] Amendments adopted by the European Parliament on 14 March 2023 on the proposal for a regulation of the European Parliament and of the Council on harmonized rules on fair access to and use of data (Data Act) (COM(2022)0068 – C9-0051/2022 – 2022/0047(COD)).
[288] Proposal for a regulation on harmonised rules on fait access to and use of data (Data Act), 2022/0047 (COD), 6596/22, 7 July 2023.
[289] European Parliament legislative resolution of 9 November 2023 on the proposal for a regulation oft he European Parliament and oft he Council on harmonised rules on fair access to and use of data (Data Act) (COM(2022)0068 – C9-0051/2022 – 2022/0047(COD)).
[290] Regulation of the European Parliament and oft he Council on harmonised rules on fair access to and use of data and damending Regulation (EU) 2017 and Directive (EU) 2020/1828 (Data Act). This version is not published in the Official Journal yet but cannot be amended anymore.
[291] European Commission, « A European Strategy for Data", COM (2020) 66 final, 19 February 2020 ; A. FERNANDEZ., "the Data Act: The Next Step in Moving Forward to a European Data Space"; *EDPL*., 1/2022, p. 108.
[292]Proposal for a regulation on harmonised rules on fair access to and use of data (Data Act), COM(2022) 68 final, 23 February 2022, explanatory memorandum, pp. 1-2.
[293] Data Act, art. 2(1). The definition is the same as the definition of "Data" in Data Governance Act (see *supra*, point 2.1.3.2).

sharing in all sectors, from business-to-consumer, business-to-business, business-to-government, government-to-business and government-to-government with the adaption of harmonized data-sharing rules[294].

The Data Act aims notably to *regulate the large amount of data generated and collected by connected products*, i.e., physical products that are able to communicate those data via an electronic communications service, a physical connection, or on-device ("Internet of things", hereinafter "IoT")[295]. In this way, the main objective of the Data Act is to *enable users of connected objects to access and use the data generated by these connected products*. Chapter II of the Data Act, called "business to consumer and business to business data sharing", aims to achieve this objective by setting up a right of access for users of connected products and for recipients of data.

In this way, the analysis of Data Act is relevant in the context of TEF-Health project on two levels: First, because it could give *manufacturers and researchers* access to data generated and collected by other products already put on the market. Those data are important for the development of new products. Moreover, it contains certain requirements that must be considered by manufacturers at the product manufacturing stage (accessibility by design). Those rules are contained in chapter II of the Data Act ("business to consumer and business to business data sharing").

Secondly, because it contains requirements that must be considered by some partners of the Consortium during some of their tasks, notably in the context of building data spaces. Those rules are contained in chapter VI and chapter VIII of the Data Act ("switching between data processing services" and "interoperability")[296].

Only those chapters will be analyzed in this contribution. As these chapters deal with conditions and concepts that may differ from one another, they will be analyzed separately.

2.3.2 Business to consumer and business to business data sharing (right to access)

One of the main aims of the proposal is to create a new right to access to data, previously not covered by specific legislative acts of the EU, by giving users - who could be consumers (B2C) and professionals (B2B) - access to the data generated by the connected products they use[297].

[294]Proposal for a regulation on harmonised rules on fair access to and use of data (Data Act), COM(2022) 68 final, 23 February 2022, explanatory memorandum, p. 2.
[295] Data Act, recital 14.
[296] According to Annex I of the Grant Agreement, WP4 is in charge of building a dataspace of health data (T4.4.2 "Setting up of a TEF dataspace of health data, where trusted stakeholders can safely share, merge and use datasets based on high quality consensus standards and practices and incentive mechanisms"); Grant Agreement, Annex 1 – Description of the action (Part A), List of Work packages, p. 11.
[297] A. FERNANDEZ., "the Data Act: The Next Step in Moving Forward to a European Data Space"; *EDPL*., 1/2022, p. 108.

This objective stems notably from the fact that data generation is the result of the actions of at least two actors:

- the designer or the manufacturer of a product, who may in many cases also be a provider of related services, and
- the user of that product[298].

2.3.2.1 *Scope and actors involved*

Scope

Article 1(1) of the Data Act provides that the regulation lays down harmonized rules on making product or related service data (b) available to the user of that connected product or related services (a).

a. *Products or related services*

According to recital 14 of the Data Act, "connected products that obtain, generate or collect, by means of their components or operating systems, data concerning their performance, use or environment and that are able to communicate that data via an electronic communication service, a physical connection or on-device should be covered by this regulation *with the exception of prototype*". In other words, this regulation should apply to connected products placed on the market in the EU and thus does not concern connected products in development stage[299].

Medical devices with AI are considered as being such products as they are likely to generate and collect data concerning their performance, use or environment[300]. The exception for prototypes implies that the Data Act should not directly apply to medical devices which are in development in the context of TEF-Health project. Indeed, as TEF-Health project aims to help manufacturers in the process of testing and certification of medical devices, the services it will offer will take place before the putting on the market of the concerned medical devices, when the medical devices are still at the state of prototype.

The right of access also concerns related services which are connected to a connected product at the time of a purchase, rent or lease in such a way that the absence of those services would prevent the product from performing one or more of its functions[301]. Such related services involve the exchange of data between the connected product and the service provider and should be understood as explicitly linked to the operation of the product's function[302]. These related services may themselves generate data of value to the user independently of the data collection capabilities of the product with which they are interconnected. On the contrary, services which

[298] Data Act, recital 6.
[299] According to Article 2(21) of the Data Act proposal, "making available on the market" means any supply of a product for distribution, consumption or use on the Union market in the course of a commercial activity, whether in return for payment or free of charge".
[300] Data Act, recital 14.
[301] Data Act, recital 17.
[302] *Ibid*.

do not impact the operation of the connected product and do not involve the transmitting of data or commands to the product by the service provider should not be considered as related services[303].

b. Product data and related services data

The right of access concerns data generated during the use of a product or related services. It concerns both product data and related services data.

- *Product data* are defined as "data, generated by the use of a connected product, that the manufacturer designed to be retrievable, via an electronic communication service, a physical connection or on-device-access, by a user, data holder or a third party, including, where relevant, the manufacturer"[304];

- *Related services data* are defined as "data representing the digitization of user actions or events related to the connected product, recorded intentionally by the user or as a by-product of the user's action, which is generated during the provision of a related service by the provider"[305].

Recital 14a of the Data Act gives some examples of this kind of data. According to this recital, the notion should include data on the use of a product generated by a user interface or via related services. "It should not be limited to the information that such action happened but should also include all data that the product generates as a result of such action, such as data generated automatically by sensors and data recorded by embedded applications, including applications indicating hardware status and malfunctions. This should also include data generated by the product or related services during times of inaction by the user, such as when the user chooses to not use a product for a given period of time and keep it in stand-by or even switched off, as the status of a product or its components".

It is important to mention that some of these data could be covered by trade secret, according to directive 2016/943[306]. In this situation, data holders should be able to require the user, or third parties of the user's choice, to preserve the confidentiality of data considered as trade secret[307]. To that end, data holders should identify trade secrets prior the disclosure, and should have the possibility to agree with the user, or third parties of the user's choice, on appropriate measures to preserve their confidentiality[308].

[303] *Ibid*.
[304] Data Act, art. 2(15).
[305] Data Act, art. 2(16).
[306] Directive (EU) of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, *J.O.*, L 157/1, 15th June 2016.
[307] Data Act, recital 31.
[308] Data Act, recital 31 and art. 4.6.

Actors involved

In TEF-Health context, among the different actors involved in the right of access established by the Data Act, the following ones will be at stake:
Manufacturers of connected products and providers of related services placed on the market in the EU, irrespective of their place of establishment. It would be TEF-Health users' (the SMEs) which will develop medical devices with AI, which could be connected product in the sense of the Data Act proposal.
Data holder[309] , who is a natural or legal person who has accessed data from the connected product and have the obligation to make data available to a data recipient or a user. It could concern a manufacturer once the connected product is put on the market, when it generates and collects data.
The user of a connected product who is a legal or natural person that owns a connected product or to whom temporary rights to use that connected product have been contractually transferred, or that receives related services[310]. More generally, it could concern patients who may use a connected medical device. In the specific context of TEF-Health project, it could also concern hospitals and healthcare professionals who will use connected medical devices in their professional activities, as, for example, for diagnostic assistance.
Third party to whom data is made available, is a natural or legal person, *an enterprise, a research organization or a not-for-profit organization or an* entity acting in a professional capacity[311]. It could concern TEF-Health Consortium or at least certain partners of the Consortium (research institutes, notably) who need specific data to achieve their tasks, but also TEF-Health users (the SMEs) which need specific data of other connected medical devices to test and develop a new medical device with AI.

2.3.2.2 Impact for TEF-Health project

Concerning the manufacturers (TEF-Health users – the SMEs) – Accessibility by design

Article 3 of the Data Act contains several obligations concerning the obligation to make data from connected products or generated during the provision of related services *accessible to the user*.

Among those obligations, one is particularly relevant in the context of TEF-Health project: the obligation, for the manufacturer of a connected product, to respect the principle of "accessible by design and by default". It implies that manufacturers have the obligation to design their connected products in such a manner that data they collect, generate or otherwise obtain, which are accessible to data holders or data recipients are, by default free of charge to the user, and easily, securely accessible[312]. They also have to ensure that, where relevant and technically

[309] According to article 2, (13) of data act, data holder means "a natural or legal person that has the right or obligation, in accordance with this Regulation, applicable Union law or national legislation adopted in accordance with Union law, to use and make available data, including, where contractually agreed, product data or related service data which it has retrieved or generated during the provision of a related service". ".
[310] Data act proposal, art. 2(13).
[311] Data act proposal, recital 33.
[312] Data act, art. 3.1.

feasible, data are directly accessible to it, in a comprehensive, structured, commonly used and machine-readable format[313].

This obligation to make data accessible to the user implies that manufacturer of a medical device based on AI must think about this point from the first step of the development of his product in order to design it from the outset in a way that permits the user to access the data of the device.

Concerning the users and data recipients - Access to product data and related services data

a. Access to product and related service data by the users

Users would be able to request access to their data by means of a simple request by electronic means whenever technically feasible[314]. Where data cannot be directly accessed by the user from the product, the data holder should make them available to the user without undue delay, free of charge and, where applicable, continuously and in real time[315].

In the context of TEF-Health, it could give access to hospitals or healthcare professionals to data generated or collected by medical devices with AI used in the context of their professional activities and hold by data holders, for example manufacturers of those medical devices.

Nevertheless, Article 4.12 of the Data Act provides that where the user is not the data subject whose personal data is requested, any personal data generated by the use of a product or related service, including data derived and inferred from that use, must only be made available where there is a valid legal basis under Article 6 of GDPR and, if it concerns sensitive data, the conditions of Article 9 of GDPR[316]. It implies that hospitals or healthcare professionals who want to access personal data of a patient generated by a medical device they are using in the context of their professional activities, will have to have a legal basis in the sense of GDPR for this treatment.

b. Access to product data and related service data by a third-party (data recipient)

The significant innovation with the Data Acta is the creation of *the right, for a user, to ask the data holder to share data with third parties*[317]. The request must be addressed to the data holder by the user or by a party acting on behalf of a user.
According to recital 39 of Data act, “the third party may use the data to develop a new and innovative connected product or related service but not to develop a competing connected product”.

This right to share data with third party could be a great opportunity for SMEs (third parties) in the context of TEF-Health project to access data produced by other medical devices with AI which are already put on the market and used by hospitals (users), in a view of developing new innovative medical devices with IA.

[313] *Ibid*.
[314] Data Act, art. 4.1.
[315] Data Act, art. 4.1.
[316] Regarding the lawfulness of the processing, see *supra* 1.4.2.
[317] Data Act, art. 5.1.

c. *Links with GDPR*

The data access right provided by the Data Act would overlap and interfere with other regulations, notably with GDPR[318]. Regarding this point, Article 1.5of the Data Act provides that this future regulation is without prejudice of GDPR. In practice, these two regulations should be applied in parallel, and GDPR compliance seems to be a condition to lawfully invoke the right to access of the Data Act proposal[319]. As explained above, users and third parties are authorized to access personal data concerning other data subject only if they can invoke a legal basis under Article 6 of GDPR[320].

More specifically, the Data Act proposal explicitly addresses the interference with right to portability provided by Article 20 of GDPR[321]. The Data Act provides that the right to access data it provides complements the right provided under Article 20 of GDPR which provides for a right for data subjects to receive personal data concerning them[322]. In this view, the right to access of the Data Act differs from the right to portability in several ways. In one way, the right of access is less broad than the right to portability of GDPR because it only concerns data generated from the use of a connected product or related service. In another way, it is broader than the right to portability of GDPR because it concerns both personal and non-personal data and applies regardless of the legal basis for the processing[323].

2.3.3 Switching between data processing services and interoperability (chapter VI and chapter VIII)

The Data Act aims to make it easier to switch between providers of data processing services, in particular by *increasing data portability*. Once again, this right of portability is broader than the portability right laid down in Article 20 GDPR. The aim is to make the market more competitive and guarantee further resilience for users of data processing services[324].

In this view, the Data Act lays down certain essential requirements for interoperability, for example[325] :

- The dataset consent, use restrictions, licenses, data collection methodology, data quality and uncertainty shall be sufficiently described, where applicable, in a machine-readable format, to allow the recipient to find, access and use the data;

---

[318] S. GEIREGAT., "The Data Act: Start of a New Era for Data Ownership?" p. 24, available on: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4214704, 27 September 2022. Data act proposal, recital 7.
[319] *Ibid.,* p. 24.
[320] Data Act, art. 4.12.
[321] Data Act, recital 35.
[322] Data Act, recital 35. Article 20 of GDPR provides that: "The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured commonly used and machine-readable format [...]".
[323] Data Act, recital 35; S. GEIREGAT., "The Data Act: Start of a New Era for Data Ownership?", *op. cit.*, p. 24.
[324] Data Act, recital 78.
[325] Data Act, art. 33.

- The data structures, data formats, vocabularies, classifications schemes, taxonomies and code lists, where available, shall be described in a publicly available and consistent manner;

- ...

Participants within data spaces that offer data or data services to other participants in data spaces, should comply with those requirements[326].

It is fundamental to have this point in mind during the *development of a medical device with AI*, to implement those requirements from the first stage of development of the device to ensure the interoperability of the data produced by the device. This point is also important concerning the *elaboration of health data spaces in the context of TEF-Health project*. For example, in the context of the realization of the task T4.4.2: "setting up of a dataspace of health data", which aims to create a data space "where trusted stakeholders can safely share, merge and use datasets based on high quality consensus standards and practice and incentive mechanisms"[327].

[326] Data Act, art. 33.3.
[327] Grant Agreement, Annex 1 – Description of the action (Part A), List of Work packages, p. 11.