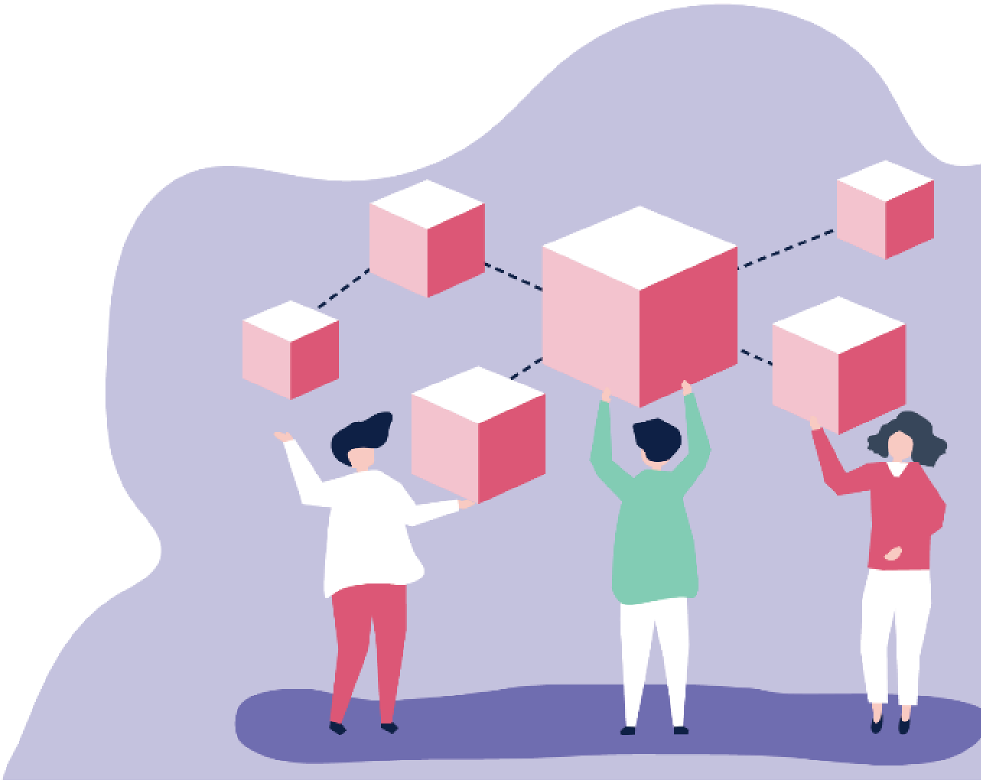
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N° 857223

GATEKEEPER

D8.3 Certification Scheme Strategy and Sustainability Plan

Deliverable No.	D8.3	**Due Date**	31/12/2023
Description	Plan with recommendations for leveraging on certification mechanisms to support GATEKEEPER adoption by the market.		
Type	Report	**Dissemination Level**	PU
Work Package No.	WP8	**Work Package Title**	Standardization and certification mechanisms
Version	1.0	**Status**	Final



Authors

Name and surname	Partner name	e-mail
Adrián Quesada Rodriguez	MI	aquesada@mandint.org
Vasiliki Tsiompanidou	UDGA	vtsiompanidou@udgalliance.org
Renata Radocz	MI	rradocz@mandint.org
Stea Miteva	UDGA	smiteva@udgalliance.org
Cédric Crettaz	UDGA	ccrettaz@udgalliance.org
Sébastien Ziegler	MI	sziegler@mandint.org
Christina Varytimidou	MI	cvarytimidou@mandint.org

History

Date	Version	Change
22/10/2021	0.1	Creation of Table of Content; Sections 1 and 2, introduction of previous research
30/11/2021	0.2	Creation of first draft of section 3
14/02/2022	0.3	Contribution for interoperability certification
22/03/2022	0.4	Section 5
1/04/2022	0.5	First draft of section 6
5/05/2022	0.6	Updates for European Health Data Space Regulation
20/05/2022	0.7	Contribution for interoperability certification, interoperability test specification and interoperability test report
19/12/2023	0.8	Integration of pending sections
23/01/2024	0.9	Internal review complete, submitted for peer review. Integration of peer review results
29/01/2024	1.0	Final version ready for submission

Key data

Keywords	Certification strategy; Interoperability; Data protection; Health data sharing;
Lead Editor	Adrian Quesada Rodriguez – aquesada@udgalliance.org; Vasiliki Tsiompanidou – vtsiompanidou@udgalliance.org; Stea Miteva - smiteva@udgalliance.org
Internal Reviewer(s)	John Farrell – RCSN / Eva Karaglani - HUA

Abstract

The present deliverable presents the main results of GATEKEEPER T8.3, including the project's methodological approach for certification and sustainability, focusing on data protection, medical device provision, Artificial Intelligence (AI) and interoperability solutions. It includes a demand and requirement analysis considering stakeholder inputs on certification for demand identification, and gap analysis.

To ensure the viability of its work, the task leveraged and supported EU-wide initiatives such as the development of the Europrivacy Certification Scheme while connecting with technical certification work undertaken by other GATEKEEPER work packages. Finally, the deliverable presents the solutions developed by the task to cover the identified priorities, including draft certification criteria for AI, and multi-normative compliance assessment for health and data sharing. Additionally, it showcases certification-related solutions developed during the project to ease contractual agreements and self-assessment by relevant parties.

Statement of originality

This deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both.

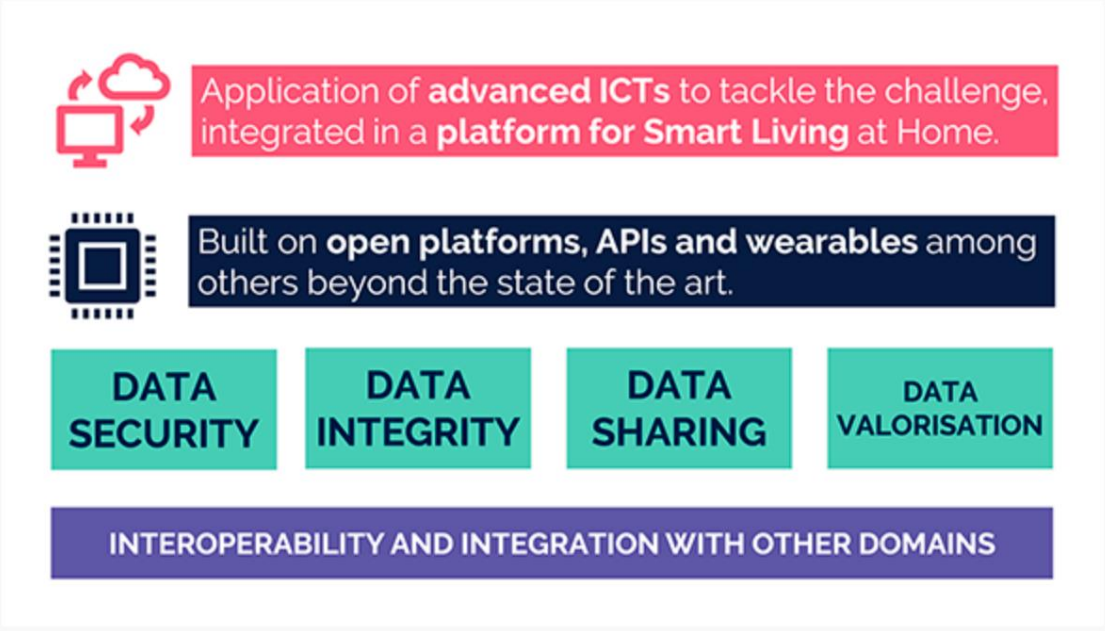
Table of contents

List of tables

List of figures

1 Introduction

GATEKEEPER is a European Multi Centric Large-Scale Pilot on Smart Living Environments. It aims to create a platform, which will allow healthcare providers, businesses, entrepreneurs, and elderly citizens to connect with each other and with the communities they live in. The project envisioned the development of an open, trust-based arena for matching ideas, technologies, user needs and processes, aimed at ensuring healthier independent lives for ageing populations. The platform was designed to be composed of a GATEKEEPER Healthcare Space, a Consumer Space, a Business Space, and an Ecosystem Transition Space. The four spaces are interlinked and were developed to allow smooth interaction and communication between the stakeholders and users of the platform. Figure 1 below showcases the conceptualised data processing-related actions and principles between these spaces.



Application of **advanced ICTs** to tackle the challenge, integrated in a **platform for Smart Living** at Home.

Built on **open platforms, APIs and wearables** among others beyond the state of the art.

Figure 1: Concept for interlinking GATEKEEPER spaces

The figure reflects the crucial importance of the technological platform in GATEKEEPER to manage all data and to apply digital innovation actions. Furthermore, to derive quality data value and stimulate the engagement of stakeholders and particularly end-users, the project needs to build trust. This could be done through various technical or organizational trust-generating mechanisms, which ensure compliant data processing, and thus reduce any potential risks. The current deliverable will focus on certification as such mechanism and will report on the actions undertaken so far to generate relevant certification-related solutions (CRS) to support sustainability and relevance of the project results upon its completion.

1.1 Work Package 8 and Objectives of Task 8.3 on Certification Strategy

GATEKEEPER's Work Package (WP) 8 is dedicated to standardisation and certification mechanisms. The overall objectives of this WP are to identify and analyse relevant standards and standardisation tracks for the project, to support standardisation of the project's technology, and to analyse and support an effective certification strategy to enhance trust in data processing activities carried out by GATEKEEPER's solutions as well as their interoperability. Task 8.3 has a twofold focus on the project:

- Data protection – certification processes that demonstrate compliance;
- Technical interoperability – assessment of technical requirements and solutions to support interoperability tests, validation and potential certification.

Task 8.3 is particularly focused on the development of CRS which address and support needs and requirements of GATEKEEPER stakeholders during and after the project. The successful execution of this task depends on a clearly crafted methodology, which is described in detail in Section 2 of the current document.

1.2 Objectives of Deliverable 8.3

Deliverable 8.3 is the final report of Task 8.3. As per the project's Grant Agreement, the current deliverable is intended to serve as a "plan with recommendations for leveraging on certification mechanisms to support GATEKEEPER adoption by the market". The current version of the deliverable contains the only and final iteration of the certification strategy for GATEKEEPER, to be submitted by the end of the project.

The objectives of the current deliverable are:

1. to interact with key stakeholders and understand their needs and requirements in terms of certification;
2. to compare existing certification solutions;
3. to conduct a gap analysis based on the findings in point 1 and point 2;
4. to recommend a strategy for certification with a clearly defined scope to address identified priority needs;
5. to report on the certification's interoperability based on initial implementation results.

The main certification results of the task reported in this deliverable have already been introduced to the official European Data Protection Seal or have served as baseline for subsequent certification schemes currently under development. Furthermore, the CRS brought forward by this task in collaboration with WP1 are currently being tested and refined by subsequent European research projects.

2 Methodological Approach

The current deliverable follows a step-by-step approach, which is tightly aligned with the goals noted in the description of Task 8.3. As part of this action, the following domains have been considered as potential subjects to certification and CRS development:

- Data protection;
- Medical device provision;
- AI solutions;
- Interoperability solutions.

The deliverable starts by analysing the demand side for certification. In order to understand in-depth the needs and requirements of relevant stakeholders, an interactive workshop with GATEKEEPER's consortium was planned and executed. The workshop enabled consortium partners to express 1) whether they considered certification solutions feasible in their specific domain, 2) what in their specific domain needs certification, and the motivation behind their interest. This interaction was complemented by a digital survey (Appendix A), distributed to the attendees during the workshop. Additionally, consultations were performed in conferences (CPDP, Privacy Symposium, and IAPP Europe meetings) with domain experts external to the consortium to produce a holistic and all-encompassing analysis which supports the certification strategy and the viability of the developed solutions. The results thus enabled the classification and prioritisation of collected outcomes (section 3.3.2).

In parallel, the task carried out regulatory and normative research in alignment and collaboration with WP1, which were reported on the Legal, Ethics and Privacy Protection deliverable. Section 3.2 of this deliverable includes some relevant outputs of this research with regards to relevant frameworks (such as GDPR, Medical Device Regulation and AI Regulation), and particularly those which can be addressed by normative compliance certification solutions. This action served to bring depth to the considered stakeholder/industry requirements while acknowledging the credibility of the proposed mechanisms to support the project's overall goals.

Section 4 of the deliverable examines the current offers in the certification domain. It follows the logic of the regulatory legal research and focuses on available mechanisms for data protection certification, AI certification, and Interoperability certification. This study enables demand and offer comparison (section 5.1) and to identify relevant gaps (section 5.2).

Based on the gap analysis, this deliverable then proposes a certification scheme and solution-development strategy (section 6) for its implementation during and after the project's duration. For cost-efficiency and feasibility, the project leverages previous and existing initiatives, such as the Europrivacy Certification Scheme (developed across various H2020 projects). Additionally, the deliverable makes a connection with relevant technical certification activities carried out by GATEKEEPER's components, and briefly reports on their main results and potential inter-connection with the proposed solutions.

Table 1 below provides a summary of the described methodology, including the actions, the key expected results (KER), methods of verification of the collected results, overall status of the actions by the end of the project.

Table 1: Methodology Overview

Planned Actions	Rationale	Means of verification	Final status
Survey on certification demand	Identify **who** wants to certify **what** and **why**	• Surveys done during the workshop and potential questions can be addressed right away; • Ensuring everyone attending conducts the survey and provide quantitively reliable results.	Achieved
Workshop on certification demand	Identify **who** wants to certify **what** and **why**	• Stimulate an open discussion and among the consortium to stimulate partners to reflect on others' opinions and think through their demand and motivation for certification.	Achieved
Conference consultation on certification demand	Extended view on the certification demand in the concerned domains	• International experts in the concerned domains from both the industry and the academia will reflect on the demand; • Answers may complement the demand analysis and help improve the strategy's sustainability and interoperability.	Achieved
Regulatory and normative research in data protection, MDR, and AI Regulation	Comprehensive list with current and upcoming legal requirements for the domains of interest	• Monitor latest developments, initiatives and opinions by EC, EDPB.	Achieved, reported on Gatekeeper LEPP
Research current certification **offer**	Comprehensive list with available solutions for the domains of interest	• Certification Report	Achieved

Compare offer and demand side	Identify gaps	- Leverage on the extensive internal expertise of UDGA	Achieved
Report on interoperability and technical certification solutions in project	**Report** outcomes; Identify potential areas of improvement	- Reports from Gatekeeper technical partners and interviews (if necessary)	Achieved

3 Demand and Requirement Analysis for Certification and CRS

3.1 Stakeholders and potential beneficiaries

The GATEKEEPER consortium involves 43 organisations, including 8 pilot sites that have extensively tested the project's platform. Among the organisations are large industrial companies, government healthcare providers, research institutes, pioneering in research of active healthy aging, AI and Big Data, big companies and SMEs in the silver economy and IoT based smart environment field, as well as standardisation organisations. The stakeholders interact and connect in four interlinked GATEKEEPER spaces through the shared use of the platform:

The GATEKEEPER Healthcare Space provides a set of services, tools, data, and components for healthcare, complying with health protocols and regulations. It connects with health information systems and records and enables the development of Business-to-Business (B2B) solutions which could provide services to healthcare providers.

The GATEKEEPER Consumer Space provides a set of services, tools and support components that allow integration and interoperability of consumer-oriented solutions, appliances, robots, applications, data, sensors and platforms. It allows to build Business to Consumer (B2C) solutions and services to be used by end users for health or life-style monitoring, as well as integrated with solutions from the Healthcare Space to combine services and provide a holistic health view and monitoring in return.

The GATEKEEPER Business Space provides the adequate ecosystem for small, medium and large companies to develop solutions, services and devices alone or in partnership with other companies following a set of standards to reach end-users (Consumer Space) or health providers (Healthcare Space).

The GATEKEEPER Ecosystem Transaction Space provides a large selection of applications and devices leveraging AI, Big Data, machine learning and IoT technologies; coupled with a variety of smart objects (e.g., wearables, sensors, robots) currently available in the market to support Data Sharing and Value-based healthcare.

When assessing relevant target beneficiaries and applicants of any given certification or CRS developed by the project, the potential composition exceeds the one of the consortium itself, and includes healthcare institutions (hospitals) and third-party service providers.

Furthermore, there is a reciprocal interrelation between the roles of the stakeholders. Firstly, both the solution providers and the healthcare institutions can be certification applicants, and all the identified stakeholder groups (solution providers, healthcare institutions, and even patients[1]) can benefit from the availability of certification and

[1] In the context of this assessment, we will consider patients and citizens under the beneficiary classification although formally they fall under a third-party beneficiary category. This due to them benefitting from the added trust provided by the compliance audits and other certification-related activities while formally remaining disconnected from the certification recipient from an organizational perspective.

associated solutions (either through direct benefits such as enhanced business opportunities, or enhanced availability of trustworthy solutions). Secondly, solution providers often belong to more than one of the abovementioned clusters; this determines a certification disposition to B2B and B2c relations in various fields of interest. The correlation between the stakeholders is exemplified in the Figure below.

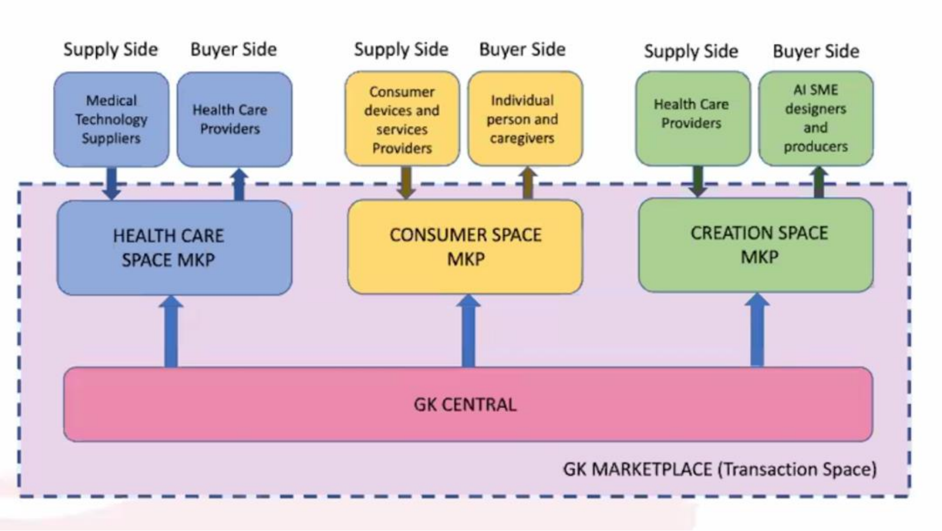


Figure 2: Supply and Demand Side in the GATEKEEPER spaces

Source (Business Cluster Presentation at the 5th Plenary Meeting 24.11.2021)

The preliminary considerations of the role and affiliation of potential certification applicants and beneficiaries have been examined in the certification survey (section 3.3.1.1).

3.1.1 GATEKEEPER Solution Providers

GATEKEEPER solution providers constitute one pillar of potential applicants and beneficiaries of certification. As outlined above, these providers belong to more than one GATEKEEPER space, and, depending on the situations, could also be demanders instead of suppliers. The GATEKEEPER initial ecosystem management plan (D2.1) identifies which producers, prosumers, and providers are interested in providing value on the supply side of the ecosystem/marketplace, usually seeking for opportunities to improve their business and honing their capabilities towards a better performance. Typically, these players produce value that is usually consumed by demand entities. Often the same peer may behave as both consumer and producer in different phases of its relationship with the brand-platform. Like in the case of GK, a hospital supply health care services to patients (consumers) and at the same time "consume" technological services supplied by technology suppliers.

In the case of GATEKEEPER, these are technological companies, technological centres and universities that supply technological assets in the project, as well as hospitals and other health care organisations that provide health care services to patients.

3.1.2 Health Institutions

The organisations participating in the pilots are the prime example of healthcare institutions. Healthcare institutions, including hospitals, clinics or any other entity engaging in the provision of health-related services, both in the private and public sector, constitute a dynamic category of certification applicants and beneficiaries. Given the multitude of data and technological solutions required to provide modernised healthcare services and promote evolution in the field, certification can play a detrimental role to ensure compliance with rapidly developing legal obligations.

3.1.3 PATIENTS

Patients and citizens belong to the "Demand entities", which are interested in "consuming" the value produced in the ecosystem. From all the identified stakeholders in the certification demand research, patients are the only pilar which will only be beneficiary to a certification.

3.2 Regulatory and Normative Basis for Certification

This section will seek to provide a brief introduction to the main legal and normative frameworks which include references to certifications as means to demonstrate regulatory conformity. The contents of this section should be read in conjunction with the associated regulatory assessment presented in the Gatekeeper Legal and Ethical deliverables prepared by WP1.

3.2.1.1 Personal Data Protection Certification

Under the General Data Protection Regulation, certification is optional for controllers (GDPR, Art.42(3)) and can be used as a way to demonstrate compliance (GDPR,2016, Art. 24(3)) and fulfil the key principle of accountability (GDPR, 2016, Art. 5(2)). However, any certification granted does not reduce the responsibility of the controller (GDPR, 2016, Art. 42(4)).

As noted in following sections, all certification work (research, criteria, and recommendations) carried out during the project and CRS developed by Gatekeeper have been aligned with the GDPR's goal to establish pan-European certification mechanisms and data protection seals and marks. Article 42(1) GDPR specifically encourages all Member States, supervisory authorities, the European Data Protection Board (EDPB) and the European Commission (EC) to encourage such efforts. When a scheme owner or a certification body submits EU-wide certification criteria, the competent data protection authority must request the opinion of the EDPB (GDPR, Art. 64(2), that will issue the relevant decision either adopting or rejecting the certification scheme.

Based on the above-described procedure, in October 2022, Europrivacy became the first certification scheme approved by the EDPB as the first Pan-European Data Protection Seal. Europrivacy constitutes a hybrid certification scheme, applicable to all types of data processing activities, while addressing domain- and technology-specific obligations and risks for the data subjects, covering compliance with the GDPR requirements. It is also extendable to other non-EU privacy laws, and it is supervised and continuously updated by an International Board of Experts to address regulatory changes.

3.2.1.2 Medical Devices Regulation Certification Basis

Under the Medical Devices Regulation (MDR), certification is mandatory before being placed on the market, and medical devices need to pass the relevant conformity assessment procedure depending on their classification. Only then they will be allowed to draw up a declaration of conformity with the MDR (MDR, 2017, Arts.19, 10(6)) and affix the CE marking (MDR, 2017, Art. 20). The CE marking must include the identification number of the notified body responsible for the conformity assessment (MDR, 2017, Arts. 20(5). 52).

Under the MDR, each Member State must appoint an authority that will be responsible for the notified bodies (MDR, 2017, Art.35). Article 36 of the MDR details the requirements relating to notified bodies that inter alia include organisational requirements, quality management and sufficient administrative, technical, and scientific personnel that are necessary to fulfil their tasks. In case of subcontractors, these must be verified in advance that they meet all the requirements set under Annex VII and the responsible authority for the notified bodies shall also be informed (MDR,2017, Art. 37).

To become a notified body, a lengthy procedure must be followed, as specified under MDR, Art 39: Initially, an application must be submitted to the authority responsible for notified bodies. Within 30 days the authority must draw up a preliminary assessment report that will then be submitted to the Medical Device Coordination Group (MDCG). Within 14 days upon submission the Commission jointly with the MDCG shall appoint a joint assessment team of three experts (as specified under MDR, 2017, Art 39 (3)). Within 90 days the joint team reviews the submitted documentation. When there are no non-compliances detected, the authority responsible for notified bodies draws up a final assessment report with a recommendation of the scope of designation.

Furthermore, according to Article 8(1) MDR, if medical devices are in conformity with the relevant harmonised standards that are published in the Official Journal of the European Union, there is a presumption of conformity with the MDR. The same presumption applies to common specifications adopted by the European Commission (MDR, 2017, Art. 9(2)). However, it is important to note that thus far, very few harmonised standards have been adapted for the new MDR and published in the OJ, most of which concern the sterilisation of health care products (European Commission,2021b). The table below includes the harmonised standards for which there is a presumption of conformity:

Table 2: Harmonised standards for MDR

Harmonised standards (OJ publication)	Description
EN ISO 10993-23:2021	Biological evaluation of medical devices- Tests for irritation
EN ISO 11135:2014	Sterilisation of health care products- Ethylene oxide
EN ISO 11137-1:2015	Sterilisation of health care products - Radiation
EN ISO 11737-2:2020	Sterilisation of health care products - Microbiological methods
EN ISO 25424:2019	Sterilisation of health care products – Low temperature steam and formaldehyde

The 2022 annual work programme for European standardisation of the European Commission expressly includes the revision of standards and the development of new ones that align with the new MDR and the IVDR, which remains ongoing. Therefore, manufacturers should watch out for publication of any further lists of harmonised standards to benefit from the presumption of compliance with the MDR these provide (European Commission, 2022c). If no harmonised standards exist, common specifications ('CS') may be adopted by the Commission according to the examination procedure of article 5 of Regulation EU No 182/2011. If medical devices are in conformity with these CS, they can still benefit from the presumption of conformity for the requirements these CS cover. Considering that at the moment not many harmonised standards have been published, CS might be an interim option and solve practicalities until harmonised standards become published.

3.2.1.3 Artificial Intelligence Certification Basis

Under the proposed Artificial Intelligence Act (AIA), certification is **mandatory** for all high-risk AI systems. Specifically, before being placed on the market, high-risk systems must inter alia undergo the relevant **conformity assessment procedure** (AIA, Arts. 16(e), 19, 43). Only after such assessment providers can draw a **single declaration of conformity** for both AIA and MDR (AIA, Art 48(3)) and **affix the CE marking of conformity** with AIA as art 49 specifies (AIA, Art. 16(i)).

As the conformity assessment will be aggregated with MDR assessment, the appropriate notified body under the MDR will also conduct this conformity assessment (AIA, Art. 43(3), which will be incorporated into the assessment under the MDR. Among the additional checks that need to be incorporated is the assessment of the quality management system (AIA, Art. 17) and of the technical documentation (AIA, Art 11(2) by the notified body as set out under AIA, Annex VII. If in this assessment the high-risk system is in conformity with all the requirements under ch. 2 of AIA, an ''***EU technical documentation assessment certificate*** *shall be issued by the notified body. The certificate shall indicate the name and address of the provider, the conclusions of the examination, the conditions (if any) for its validity and the data necessary for the identification of the AI system. The certificate and its annexes shall contain all relevant information to allow the conformity of the AI system to be evaluated, and to allow for control of the AI system while in use, where applicable*.'' (Annex VII, s. 4.6)

The declaration of conformity that will then follow will include a statement that this high-risk AI system is in conformity with both AIA and the MDR (AIA, Annex V (4)). The CE marking of conformity must include the identification number of the notified body responsible for the conformity assessment (AIA, Art 49(3)). An interesting element similar to the MDR is also introduced under Art. 40 AIA. According to this, harmonised standards that have been published in the Official Journal of the European Union ''*shall be presumed to be inconformity with the requirements set out under chapter 2 of AIA, which includes all the requirements set out for high-risk systems. The similarities with the MDR continue as Common Specifications for requirements for which no harmonised standard is yet approved are also an option under art. 41 AIA. In this way agility is enhanced, as whenever there is a specific lacuna in the technical standards, the Commission can intervene and approve a CS to fill it*." (Oxford Commission, 2021, p. 9)

3.2.1.4 NIS 2 Directive

Under Article 21 of the NIS2 Directive, Member States will be given the option to require essential and important entities to certify certain ICT products and processes via the European cybersecurity certification schemes adopted pursuant to Article 49 of the Cybersecurity Act. If such cybersecurity certification scheme is not available, ENISA will most likely prepare the candidate scheme (European Commission, 2020c, Art 21(3)).

For the rest ICT products and process that will not be subject to a mandatory certification, the current proposal empowers standardisation and encourages the use of European and internationally accepted standards and specifications relevant to the security of network (European Commission 2020c, Art 22). Therefore, when the NIS2 Directive comes into force in January 2024, a new standardisation opportunity that will cover the gap might need to be assessed, however considering that ENISA will be in charge any gap will probably be gradually covered by the initiatives of the Agency.

3.2.1.5 Cybersecurity Act

Since June 2021, the Cybersecurity Act compliments the NIS Directive and is in force (Cybersecurity Act,2019, Art.69). The Act mainly aims to grant ENISA, the EU agency for cybersecurity, its permanent mandate. Of particular importance for the GATEKEEPER project is the EU-wide certification framework for ICT products, ICT services and ICT processes, which ENISA will lead to resolve the standards fragmentation issue (Cybersecurity Act, 2019, Arts. 46, 57).

Specifically, ENISA will prepare the candidate certification schemes or will review existing European schemes on the basis of a Union rolling work programme that identifies strategic priorities for future European cybersecurity certification schemes and includes a list of ICT products and services capable of benefiting from being included in the scope of a European cybersecurity certification scheme (as this is explained under art. 47).

The security objectives of European cybersecurity certification schemes are indicatively enumerated under Art 52 Cybersecurity Act, and inter alia include security by design and default, identification and documentation of vulnerabilities as well as availability restoration. An important novelty in the certification is the option to include assurance levels (basic, substantial, or high) depending on the intended use of the ICT product, and the probability and impact of an incident. Although new standardisation opportunities thus appear within this Act, since ENISA will be in charge to prepare the certification scheme, at the moment, no gap is envisaged regarding such certification.

3.2.2 Findings

The following figure presents the main avenues for certification as identified in the previous sections:

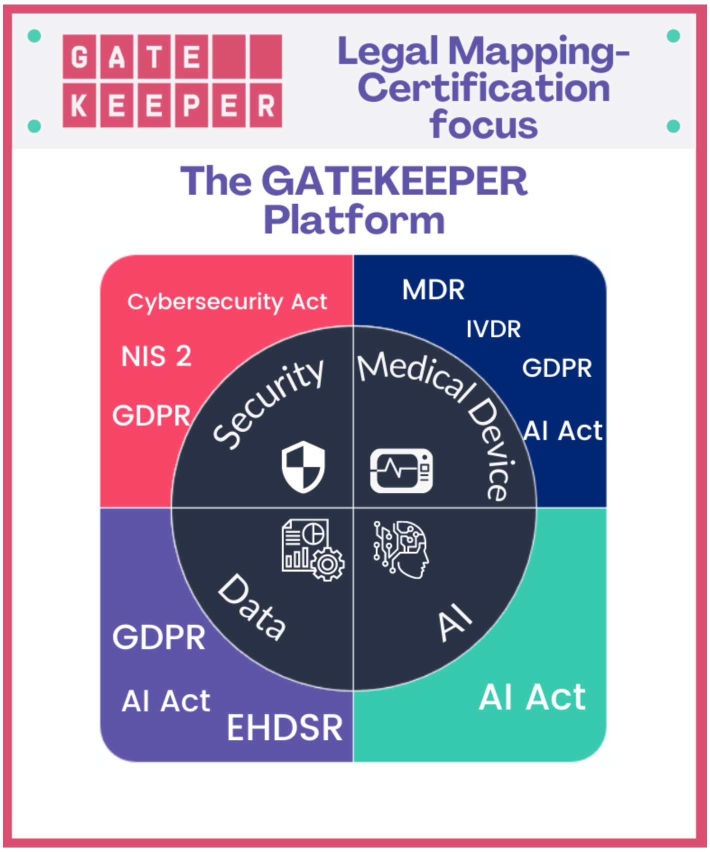


Figure 3: GATEKEEPER LEGAL MAPPING –Focus on Certification opportunities

3.3 Stakeholder Demand and Requirement Identification

Based on the results of the legal analysis, several stakeholder consultations were performed during the project. These consultations included both internal and external experts who provided insights on the main industry demands for both certifications and CRS and served as baseline for the certification strategy.

3.3.1 Stakeholder Consultation Process

Several initiatives for stakeholder consultations were undertaken, to map potentially relevant demand areas for certification and identify important requirements for potential adoption and sustainability. Those initiatives included a workshop on certification demand, an interactive exercise with consortium members for collecting inputs on a Miro Board, as well as a survey, distributed within the GATEKEEPER consortium. To ensure sustainability of the results and confirm the identified gaps in the conducted gap analysis, consultations were further conducted with stakeholders beyond the scope of the project, particularly through participation in diverse events and conferences, such as IAPP Europe conferences, CPDP, and the Privacy Symposium. The following sections will present the main outputs of these activities.

3.3.1.1 Workshop

The "Workshop on Certification Demand" took place during the 5th GATEKEEPER Plenary Meeting and aimed at collecting inputs from all the represented stakeholders both online and onsite. It consisted of several open questions, in order to let the potential certification stakeholders freely reflect on the demand side according to their role in the GATEKEEPER project, their work in the dedicated work packages, the intended outcomes, but also considering the overall goals and interests of the project, its consortium, and its current and future end-users. The members of the consortium were asked dedicated questions regarding certification cornerstones, which they answered by raising their hands, and, optionally, providing additional inputs and suggestions.

Firstly, participants were asked, what the scope of certification should be. The scope of certification is a central element for conformity assessment. A certification can have a very specific scope, or a broadly defined one. Additionally, it can be recognised internationally or only nationally. *Universal certification schemes* are cost-efficient for SMEs but do not assess technology-specific risks. On the other hand, *specialised certification schemes* may be optimal to assess specific categories of data processing, but they are inherently limited and cannot be extended to other categories of data processing. Moreover, they force companies to use diverse certification schemes and requirements with increased costs for SMEs.

As presented in the figure below, most interest (10 votes) was shown in having algorithms as certification scope. Data processing and data spaces are identified as second-important scope of interest (8 votes). The collected inputs allow to conclude that certifying tools and services, as well as datasets are equally of interest for the GATEKEEPER community, but not as important as the certification of algorithms and data processing and spaces. Lastly, based on the outcomes of the consultation, there is no interest in certifying providers.

Figure 4 provides an indication of what is the desired scope of certification. The majority would like algorithms to be certified followed by data processing and data spaces.

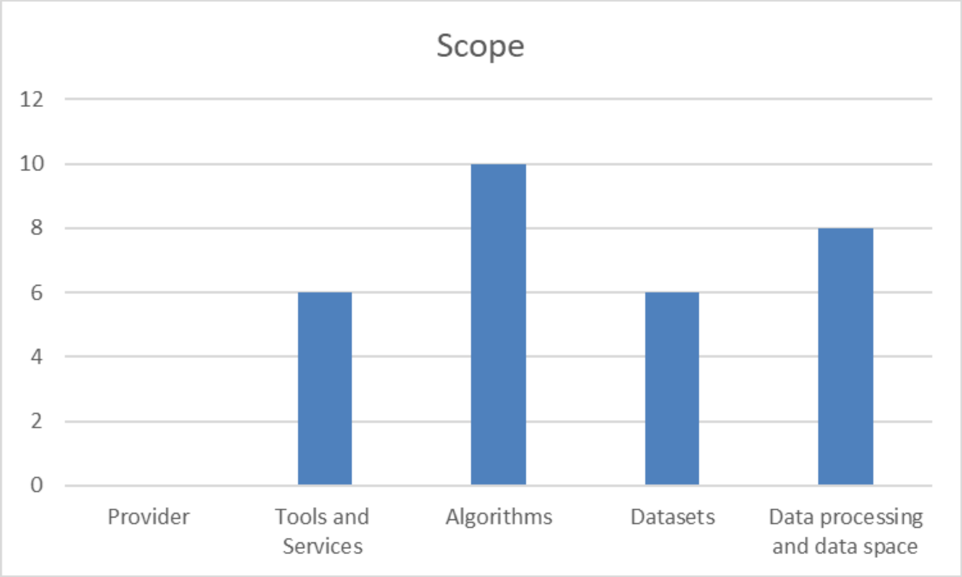


Figure 4: Scope of Certification

Secondly, participants were asked to choose the most important focus of certification. The focus of certification is not the Target of Evaluation (ToE), but rather the goal that will be achieved by obtaining a certification. Most respondents would like to achieve regulatory compliance and then interoperability. An important element is an indication that respondents prioritise long-term goals and needs over short-terms ones, as shown by the fact that the goal to make GATEKEEPER compliant was the least favourable choice.

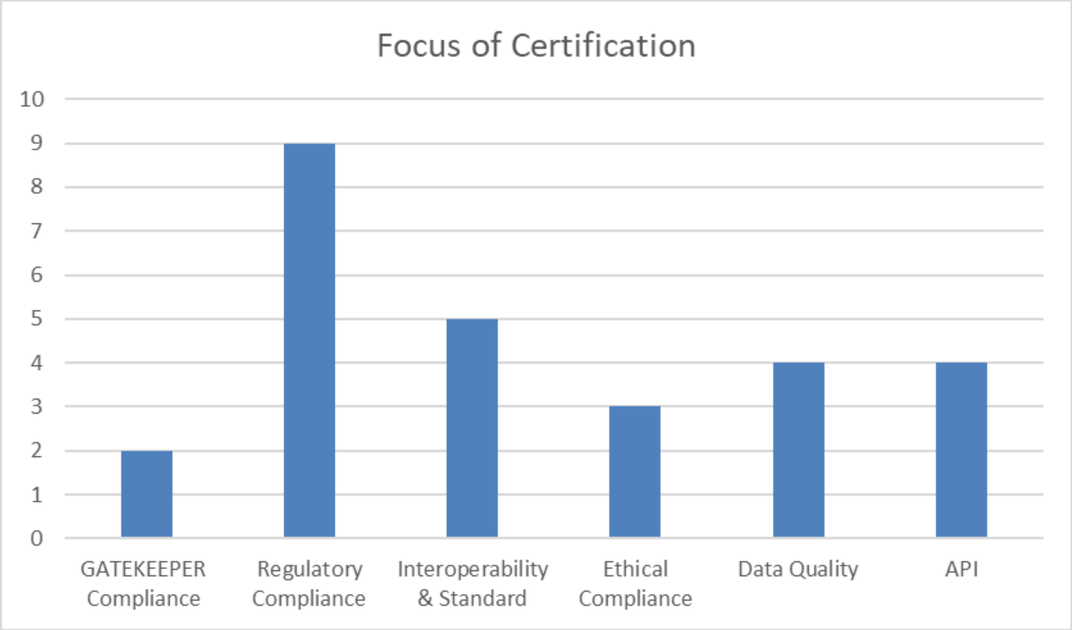


Figure 5: Focus of Certification

Figure 6 shows that the respondents would like to develop a certification for healthcare providers and public authorities.

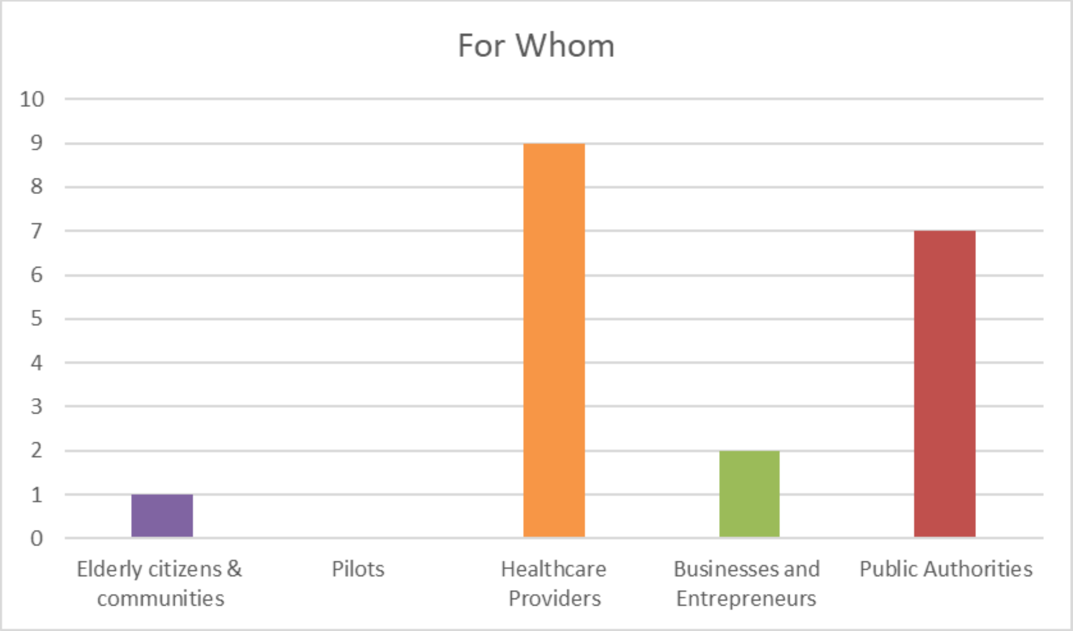


Figure 6: Certification Beneficiaries

In Figure 7, a difference between healthcare providers and public authorities was noticed. While the reason healthcare providers would be interested in certification is regulatory compliance and user acceptance, this changes for public authorities. Risk management seems to be the main reason that makes public authorities interested in such certification, while interoperability is not considered a good reason.

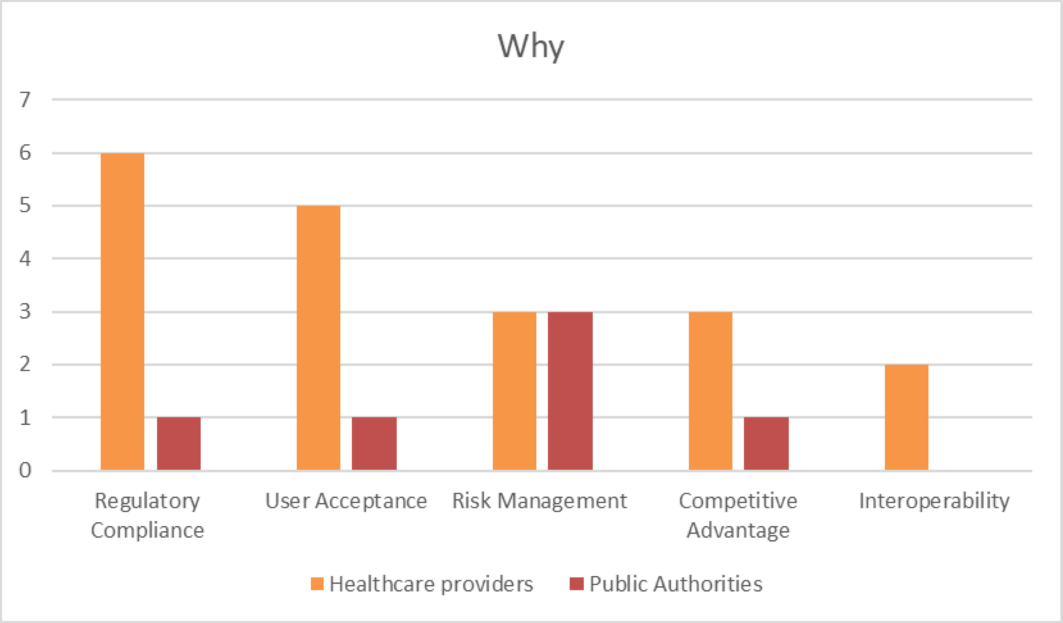


Figure 7: Motivation for Certification

Figure 8 gives an indication that certification demand exists in the GATEKEEPER Creation and Business Space, but not on the Consumer space. Which is in line with the traditional understanding of certification as a fundamentally B2B trust enabler.

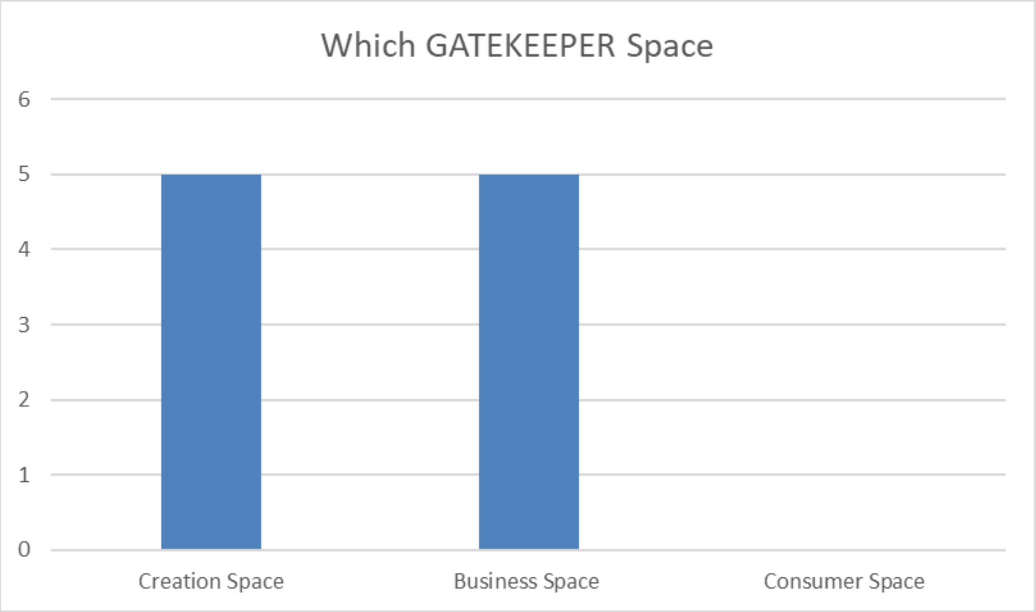
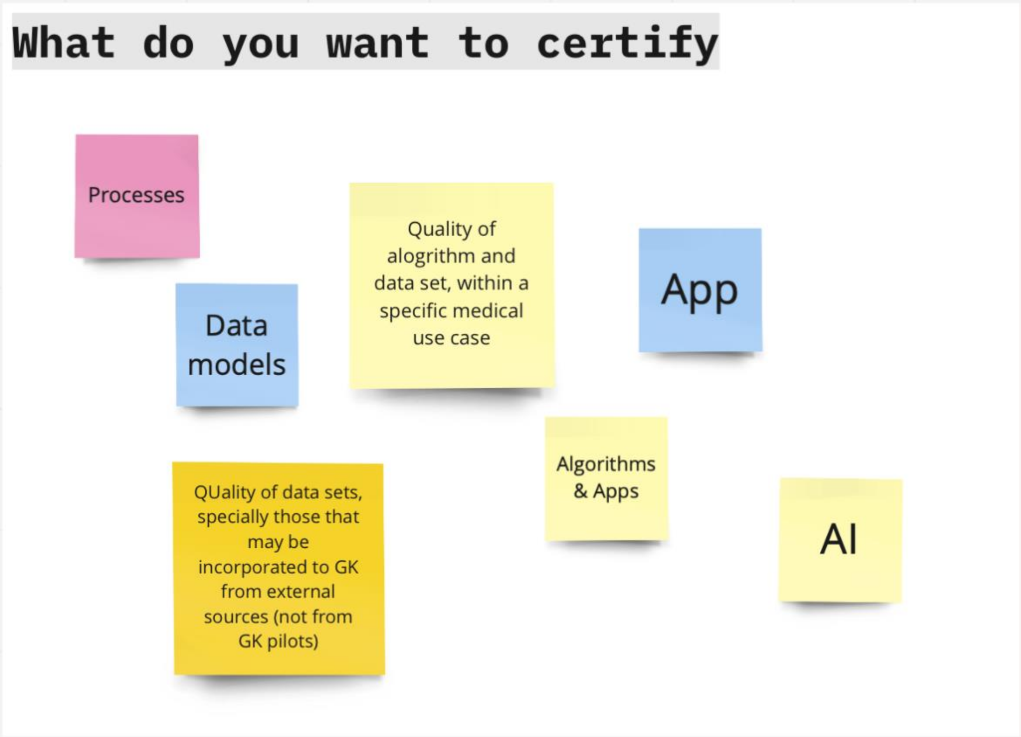


Figure 8: Certification in the GATEKEEPER Spaces

3.3.1.2 Miro Board

Figure 9 from the Miro Board shows an open-ended question to ensure respondents freely expressed their opinion on the certification scope. Quality of datasets, algorithms and apps were mostly referred.



What do you want to certify

Processes

Data models

Quality of alogrithm and data set, within a specific medical use case

App

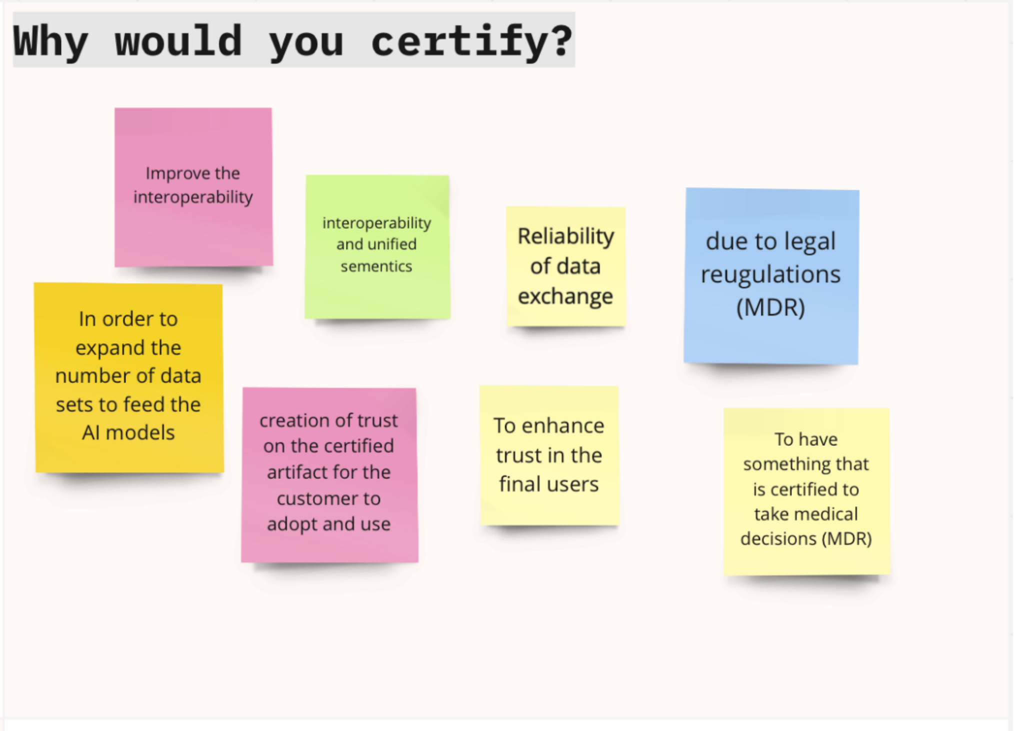
QUality of data sets, specially those that may be incorporated to GK from external sources (not from GK pilots)

Algorithms & Apps

AI

Figure 9: Open-ended question on certification scope

Figure 10 gave the freedom for respondents to freely express their reason behind a possible certification. Interoperability and regulatory compliance were followed by trust and data exchange.



Why would you certify?

Improve the interoperability

interoperability and unified sementics

Reliability of data exchange

due to legal reugulations (MDR)

In order to expand the number of data sets to feed the AI models

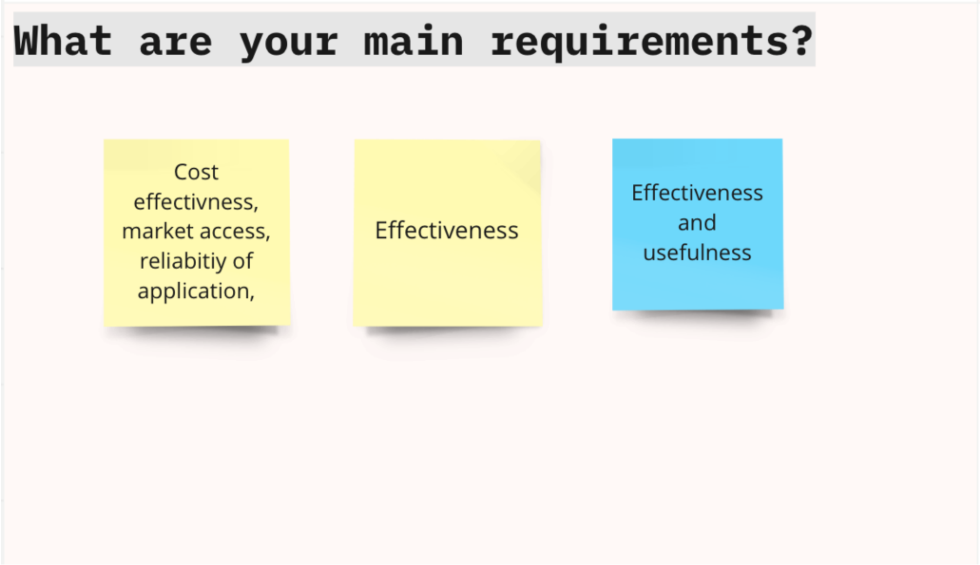
creation of trust on the certified artifact for the customer to adopt and use

To enhance trust in the final users

To have something that is certified to take medical decisions (MDR)

Figure 10: Open–ended question on reasons for certification

Figure 11 shows an indication that effectiveness is the main requirement of respondents while cost effectiveness, reliability and market access where also identified.



What are your main requirements?

Cost effectivness, market access, reliabitiy of application,

Effectiveness

Effectiveness and usefulness

Figure 11: Open-ended question on certification requirements

3.3.1.3 Survey

In addition to the workshop, a survey was conducted amongst internal Gatekeeper stakeholders. The following figure showcases a substantial demand to certify AI algorithms, datasets, data models and applications, with a slightly slower demand to certify open APIs.

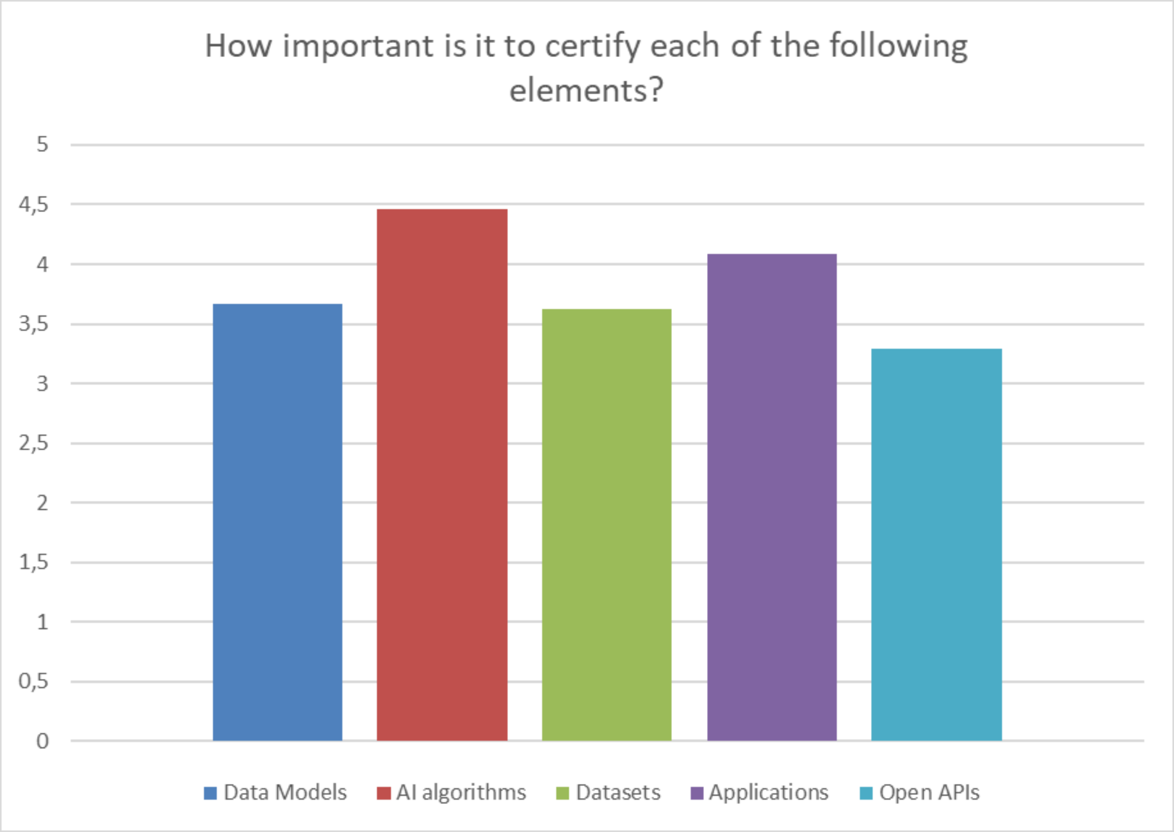


Figure 12: Survey results: Importance of certification for identified elements

In Figure 13, patients' trust and reliability of shared data were the most envisioned benefits from a certification, followed by interoperability and regulatory compliance. Competitive advantage was the least expected benefit from a potential certification.

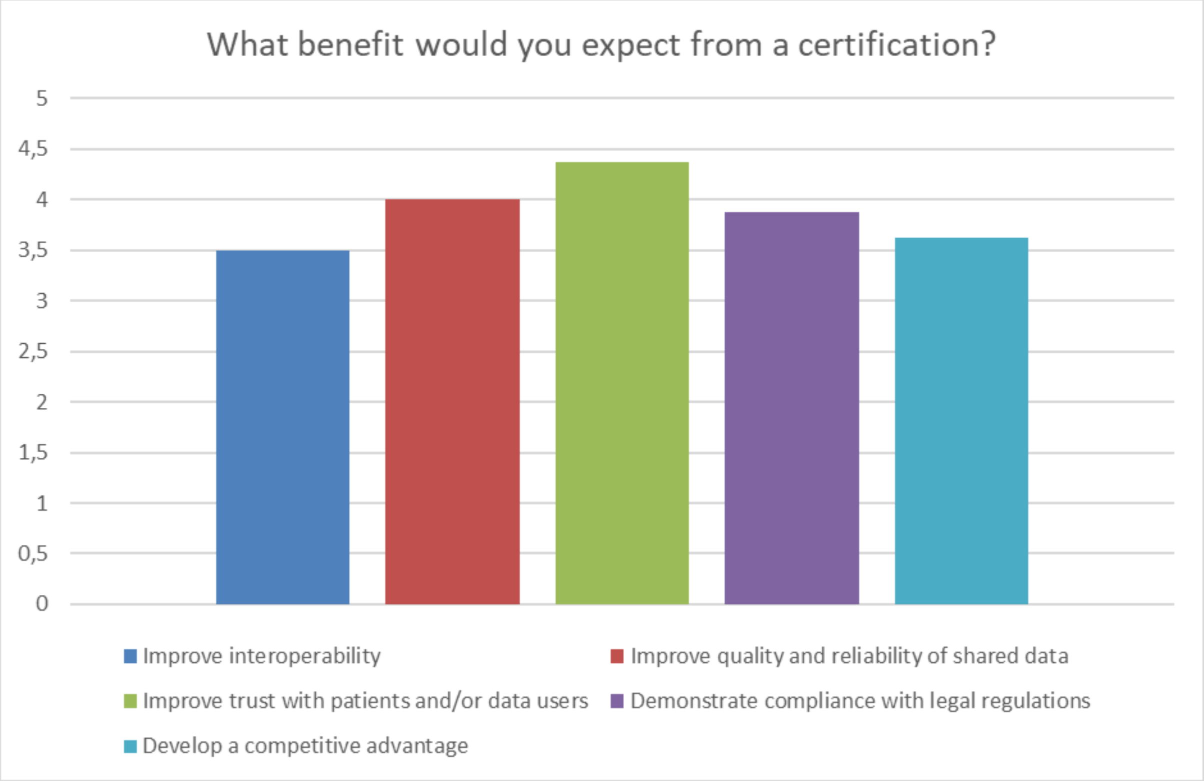


Figure 13: Survey results: Expected benefits from certification

Figure 14 shows a clear prioritisation of reliability and reusability of a certification over cost and automatability.

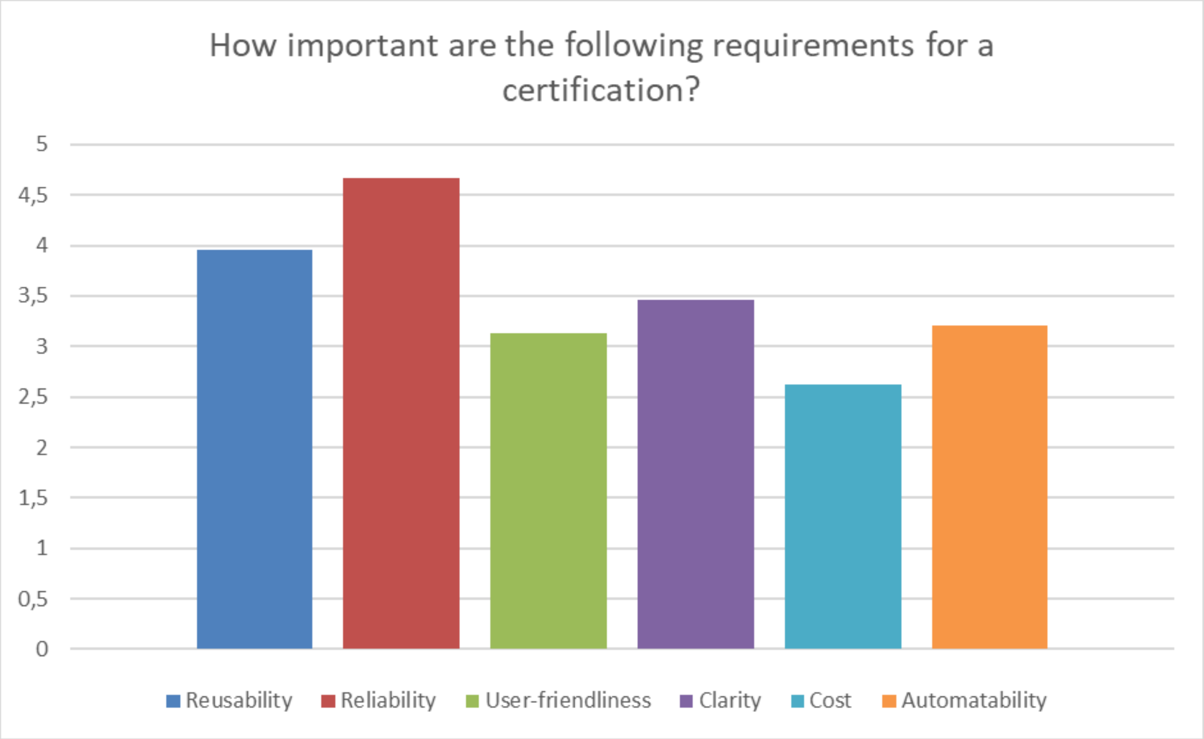


Figure 14: Survey results: Importance of certification for identified elements

Finally, consulted participants consider that all stakeholders would benefit from a certification, but healthcare providers and public authorities would perhaps benefit the most.

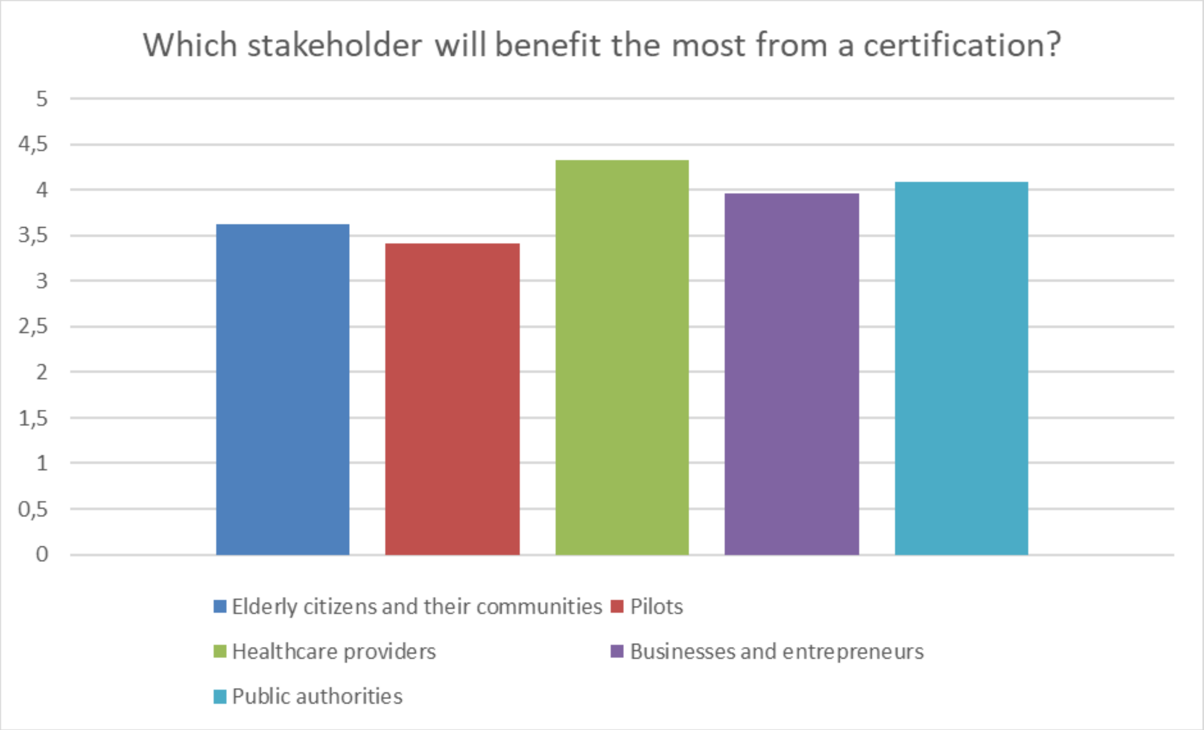


Figure 15: Survey results: Stakeholder benefits from certification

3.3.1.4 Event Consultations

As part of the dissemination and communication activities conducted during the project, participation to several IAPP, CPDP meetings and two editions of the Privacy Symposium was achieved. During each of these, a booth was setup where in addition to information on the project, participants were presented with a survey. The following images showcase the main outputs of this activity.

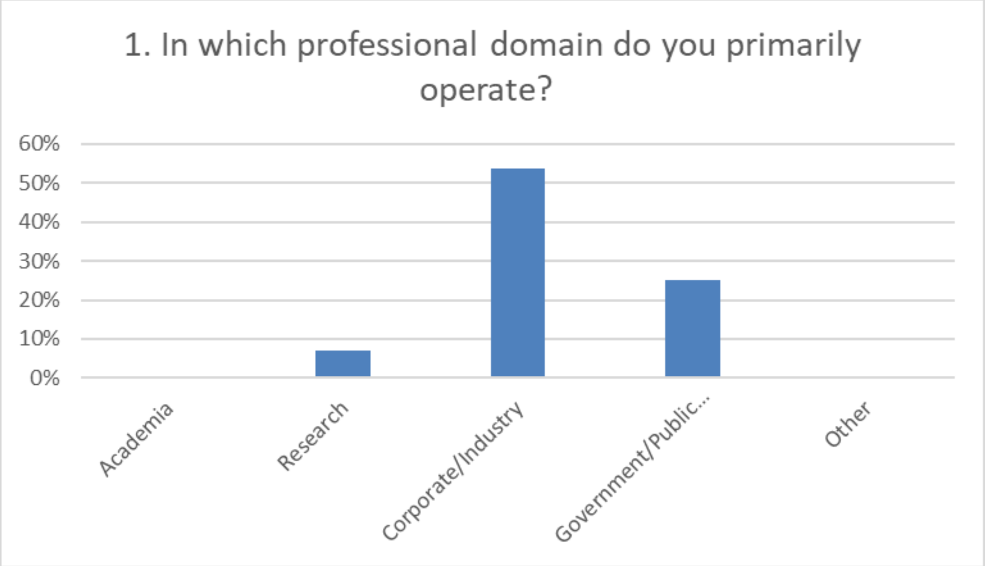


Figure 16: Professional domain of the participant

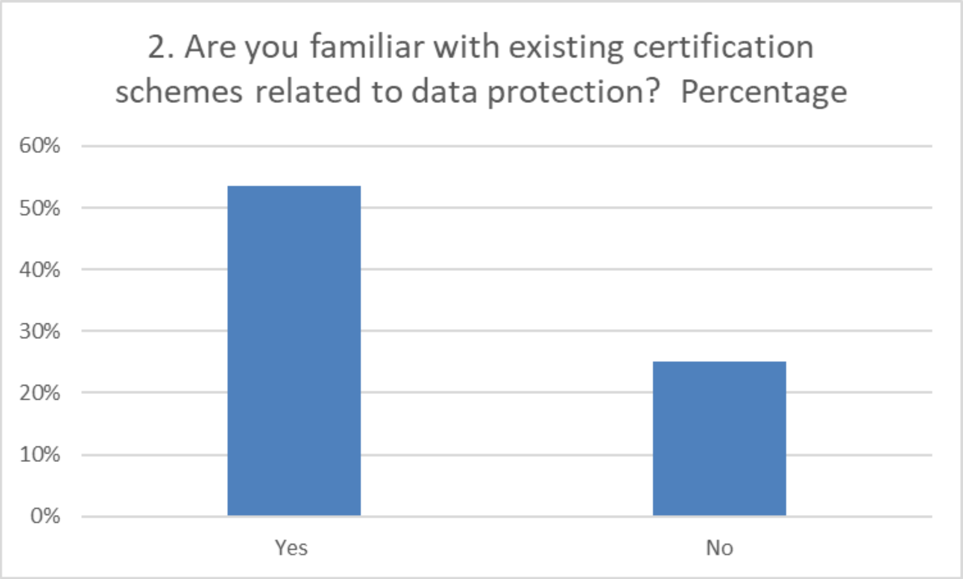


Figure 17: Familiarity with data protection certification

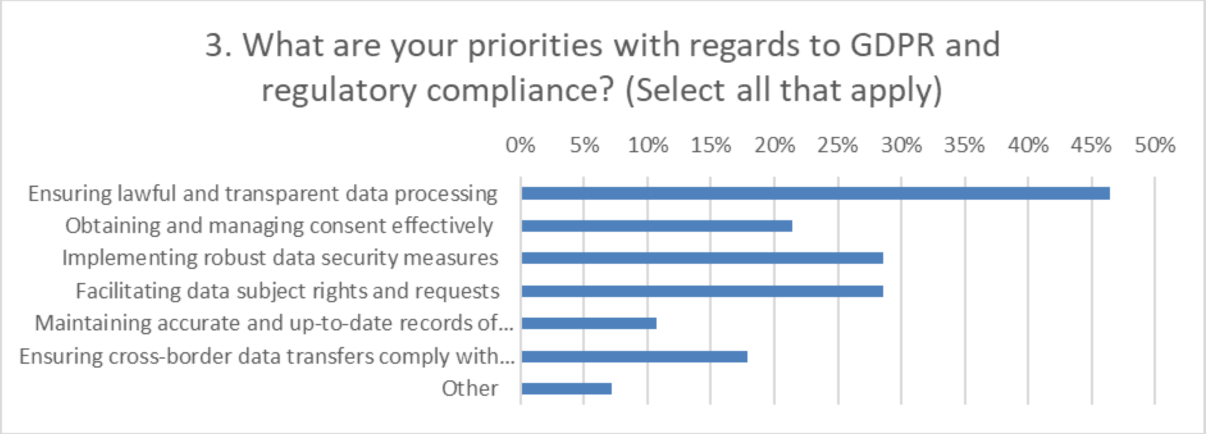


Figure 18: Compliance priorities

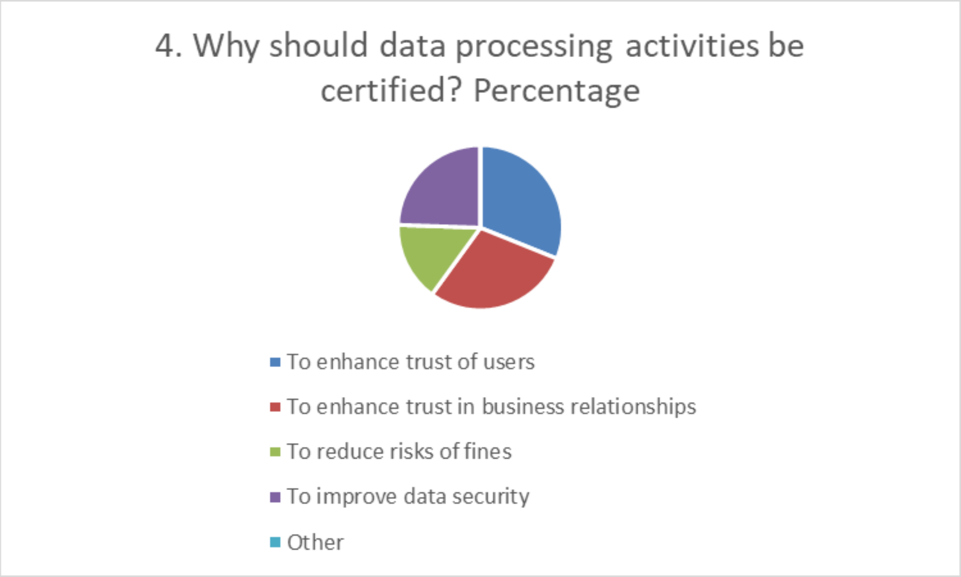


Figure 19: Reasons for processing activity certification

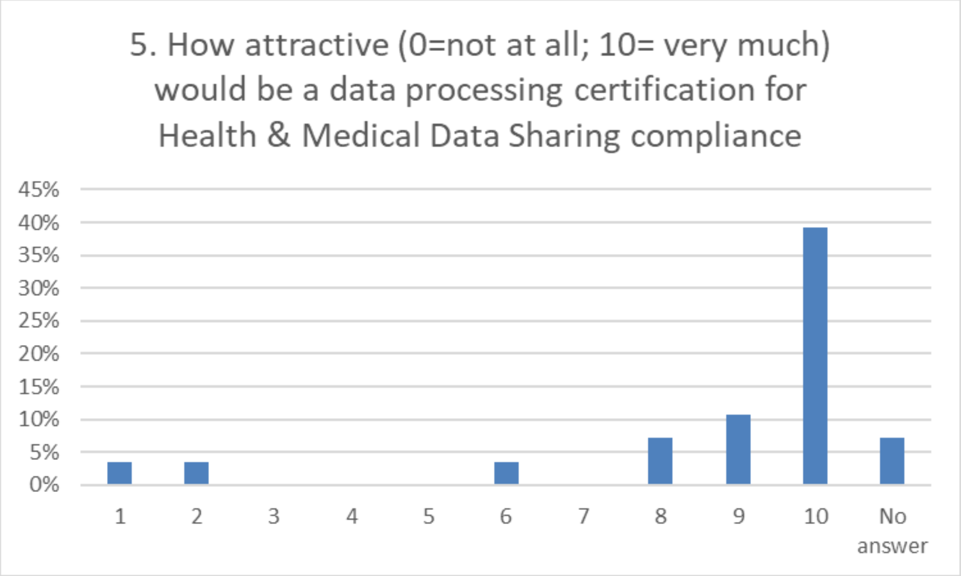


Figure 20: Appeal of health and medical data sharing certification

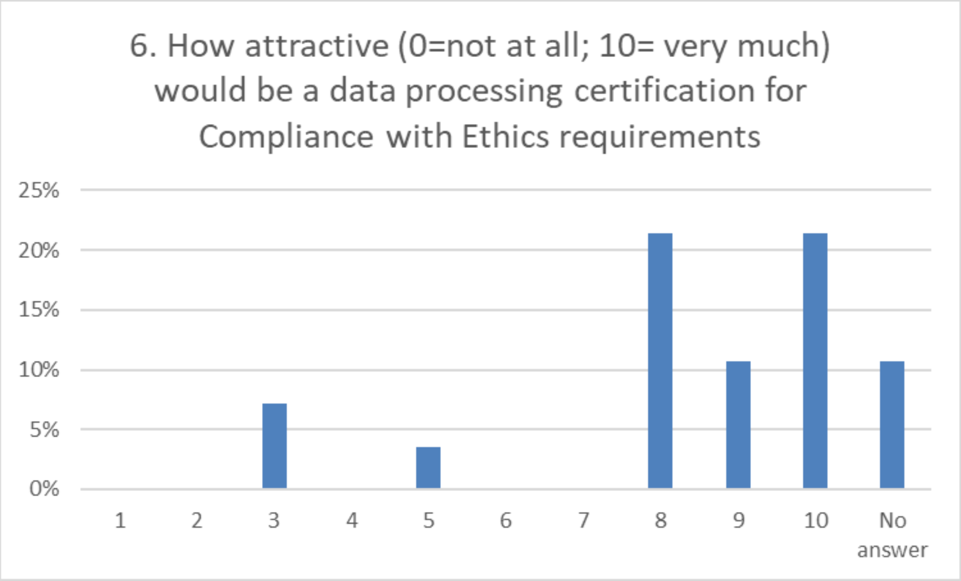


Figure 21: Appeal of ethics certification

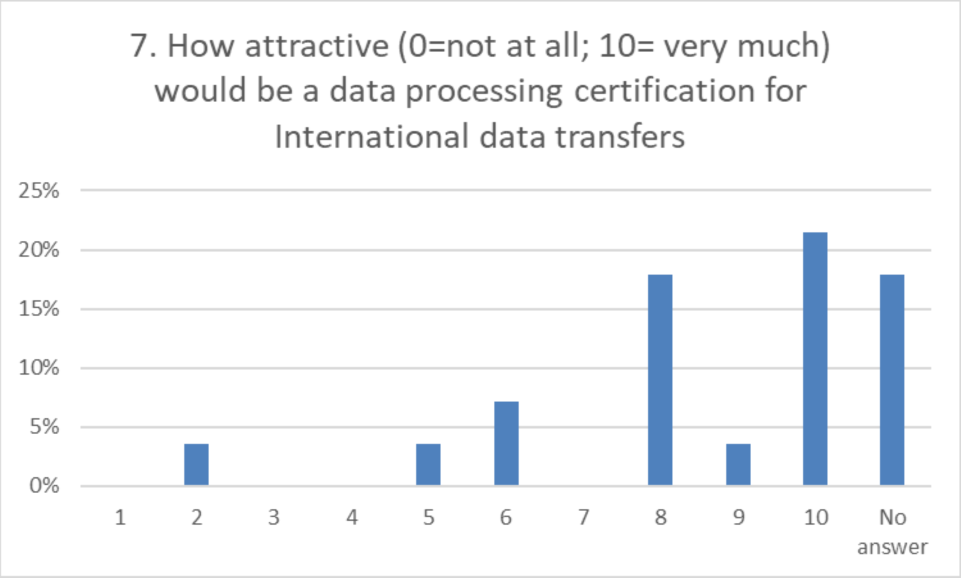


Figure 22: Appeal of international transfer certification

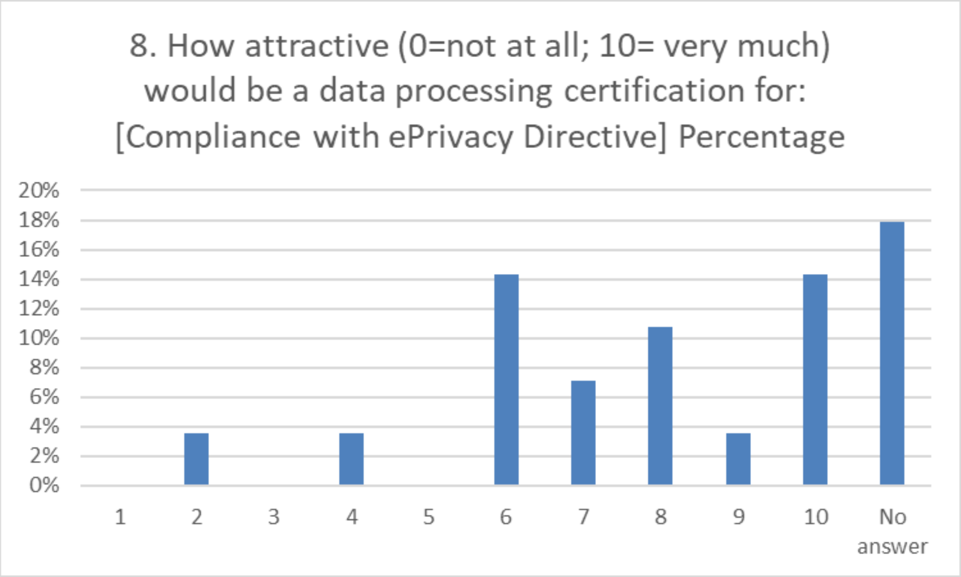


Figure 23: Appeal of ePrivacy certification

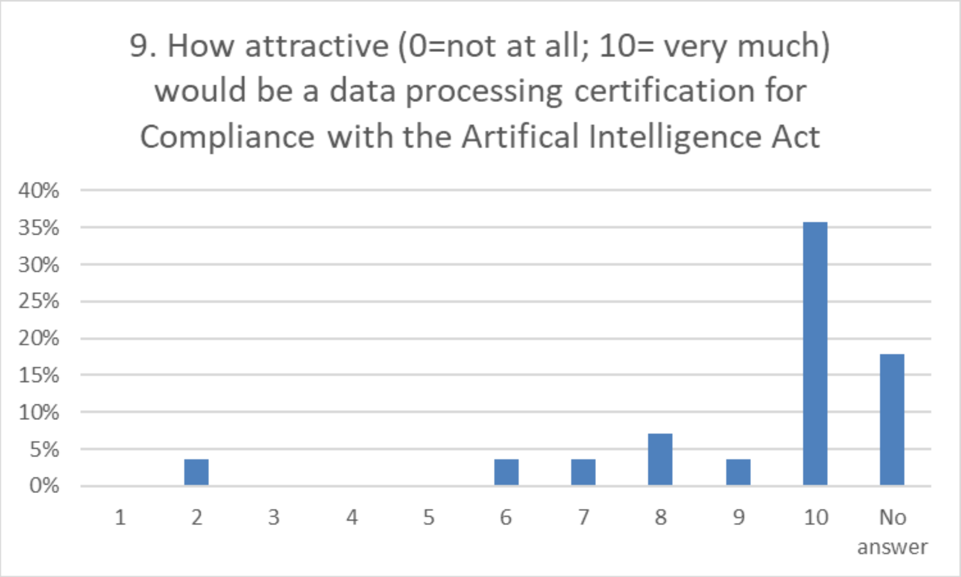


Figure 24: Appeal of AIA certification

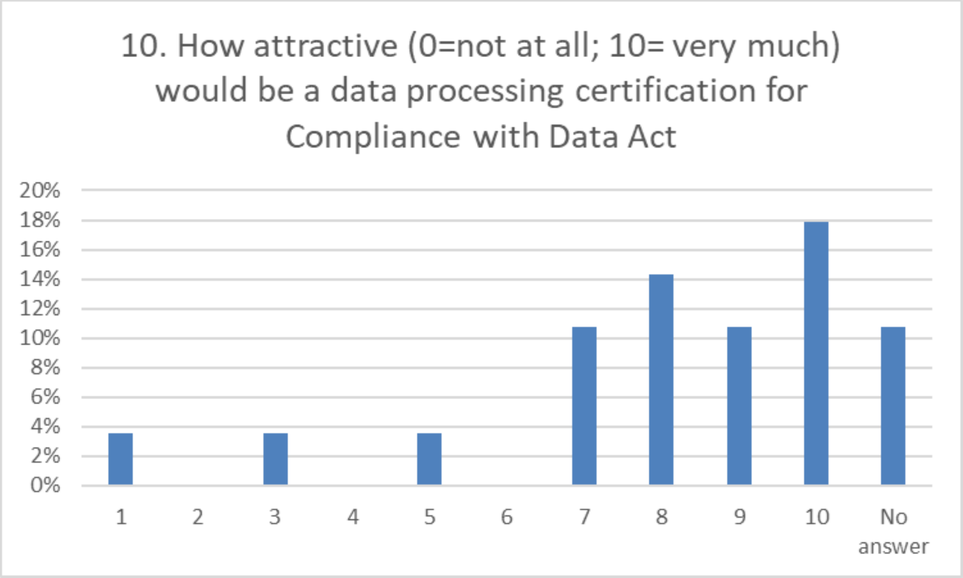


Figure 25: Appeal of Data Act certification

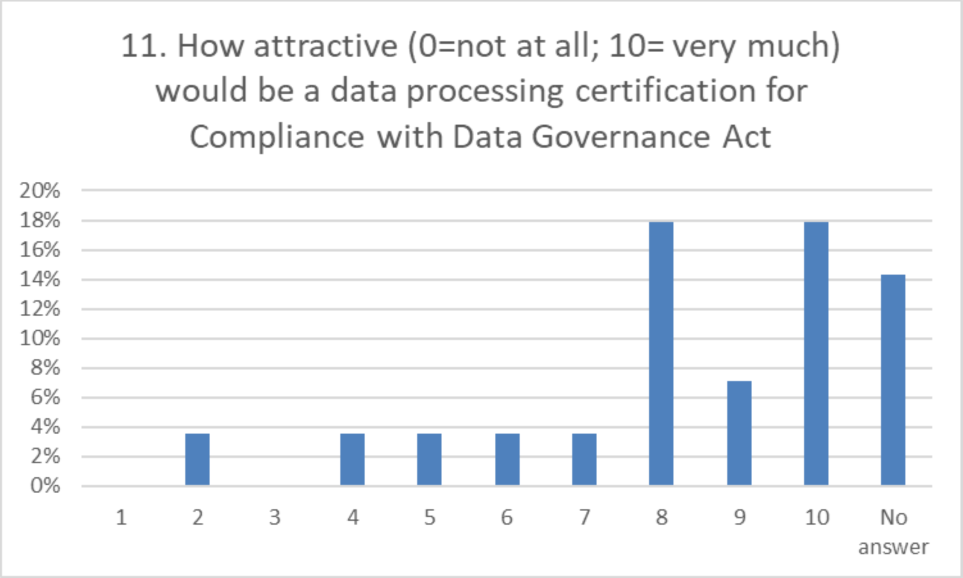


Figure 26: Appeal of DGA certification

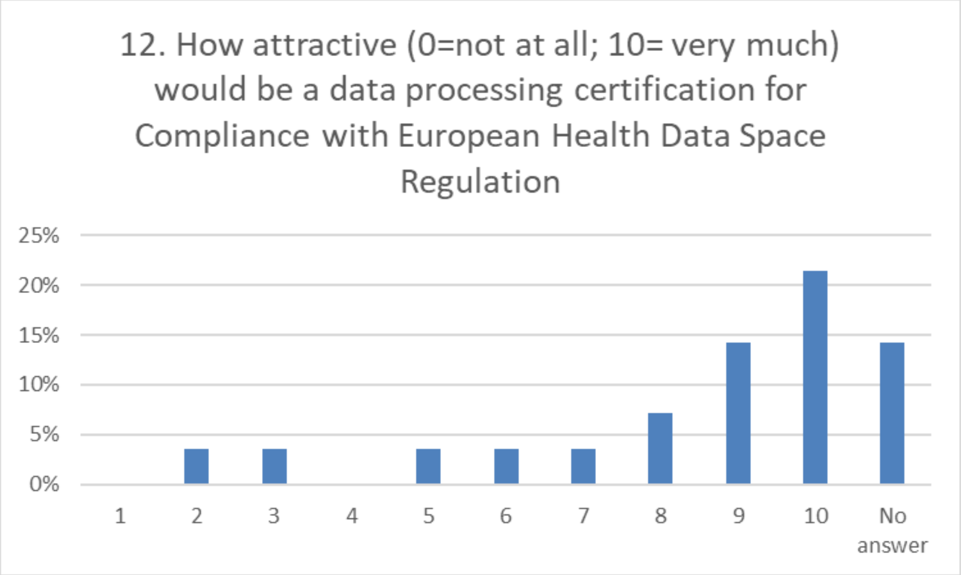


Figure 27: Appeal of EHDS certification

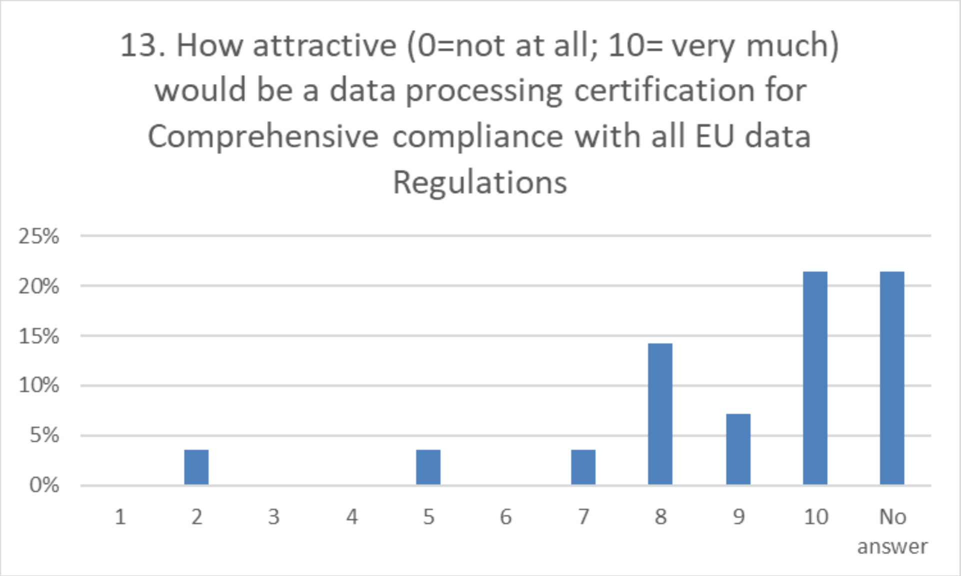


Figure 28: Appeal of comprehensive compliance certification

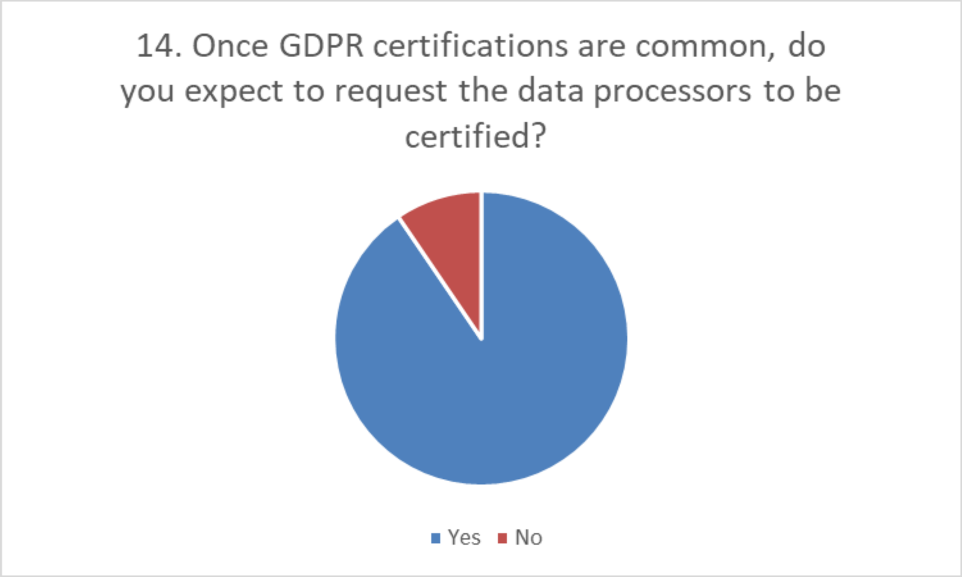


Figure 29: Data processor certification

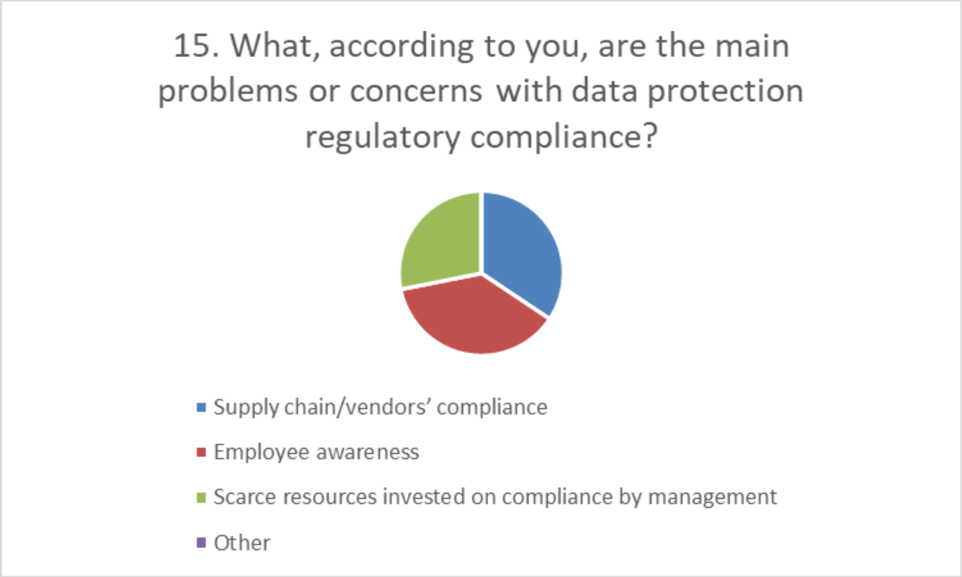


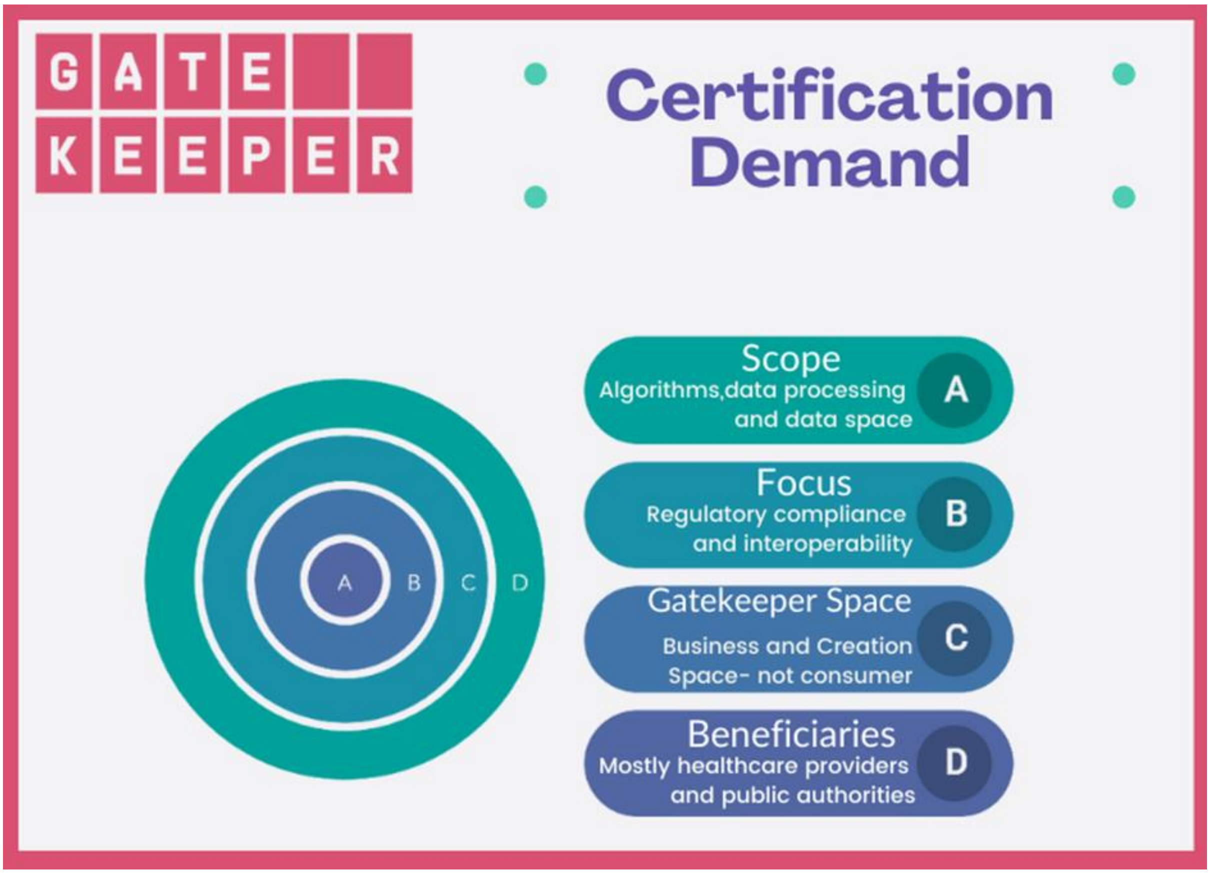
Figure 30: Problems or concerns with regards to data protection compliance

3.3.2 Privacy and Regulatory Compliance Certification/CRS Interest

3.3.2.1 Demand, Motivation, and Interest

All consultation activities noted in the previous sections grated valuable insight on what is the perceived gap and current demand among GATEKEEPER and external stakeholders.

Figure 31 shows the demand based on the closed questions:



Certification Demand

Scope
Algorithms,data processing and data space
A

Focus
Regulatory compliance and interoperability
B

Gatekeeper Space
Business and Creation Space- not consumer
C

Beneficiaries
Mostly healthcare providers and public authorities
D

Figure 31: Certification Demand (closed questions)

Figure 32 shows the demand based on the open-ended questions of the workshop:

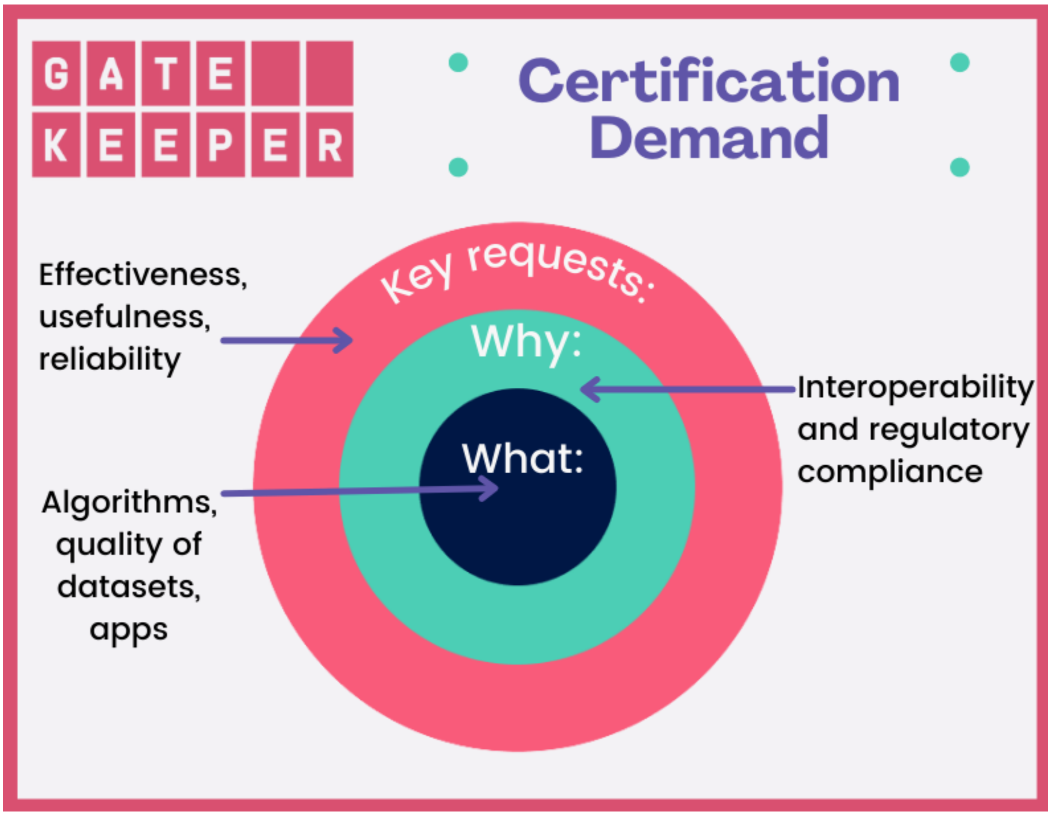

GATEKEEPER
Certification Demand
Key requests:
Why:
What:
Effectiveness, usefulness, reliability
Interoperability and regulatory compliance
Algorithms, quality of datasets, apps

Figure 32: Certification demand (open-ended questions)

In summary, the demand- perceived gap include the following:

Table 3 Privacy and Regulatory Compliance Certification/CRS demand gap

Certification/CRS scope	Algorithms and data spaces
Certification/CRS focus	Regulatory compliance and interoperability
Certification/CRS Aim	Increase users' acceptance and regulatory compliance for health providers and risk management for public authorities
Relevant GATEKEEPER space	Creation and Business Space but not Consumer space
What should be assessed/addressed	Algorithms, quality of datasets and apps
Why should it be assessed/addressed	Regulatory compliance and interoperability
Main requirements of certification/CRS	(cost)-effectiveness, usefulness and reliability
Certification/CRS target prioritisation	Algorithms first followed by datasets and applications
Pursued benefit	Patients' trust and reliability of shared data

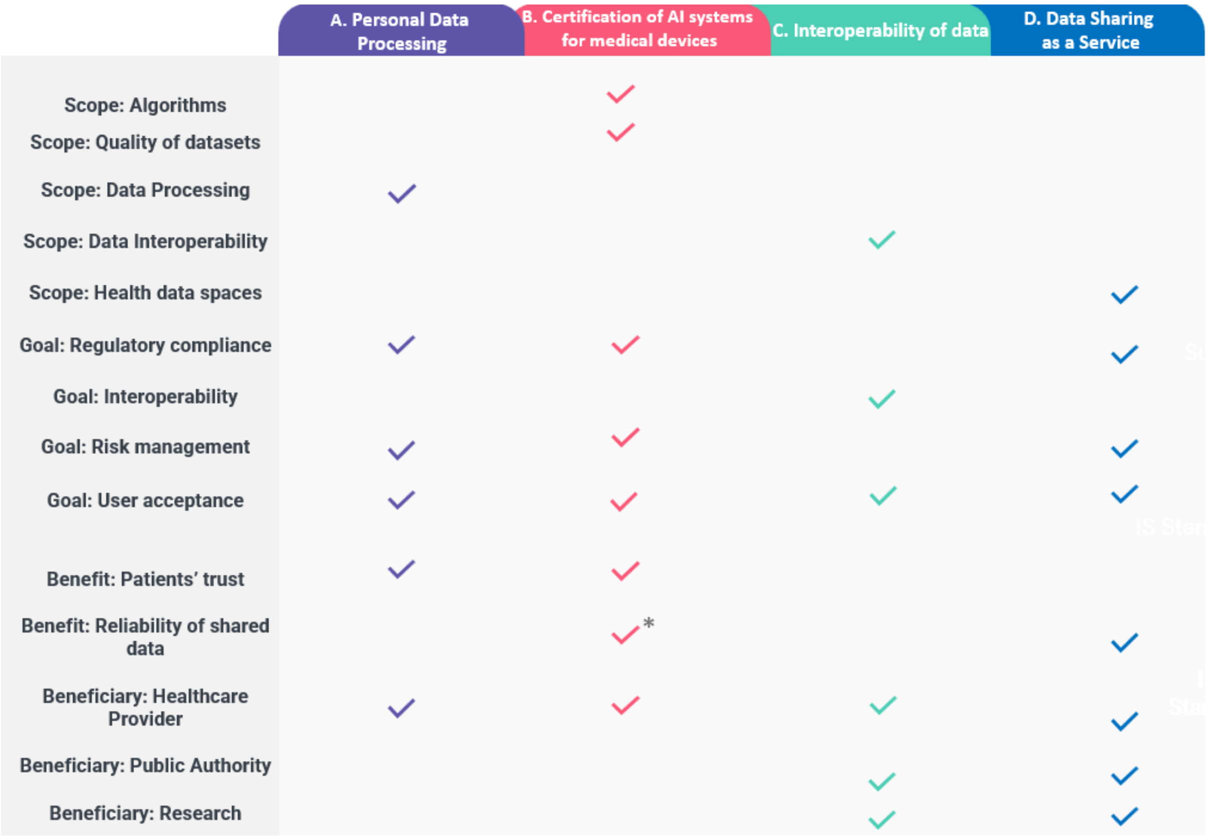
Goal prioritisation	Reliability and reusability of certification over cost and automatability;
Potential Certification/CRS applicants/users	Health providers and public authorities;
Certification Beneficiary	Mainly healthcare providers and public authorities, data subjects and public as third-party beneficiaries.

3.3.2.2 Scope

Based on the demand analysis above, four main categories of interest were identified:

1. Data protection certification and CRS with a focus on health data. These elements would certify personal data processing activities that will take place in the context of similar environments as GATEKEEPER, with a focus on securing processing of special categories of data.
2. Certification and CRS for health data sharing. This scope aims to ensure trustworthy data sharing between public and private entities who will have access to the GATEKEEPER Health Data Space. This certification will aim to ensure that both data providers and data receivers share health data and comply with their relevant legal obligations.
3. Certification and CRS for AI systems with a focus on certifying algorithms and quality of datasets. This certification could also cover in its scope the deployment of AI systems for medical diagnosis (software as a medical device, better known as 'SaMD').
4. Interoperability and trust certification (See Sections 3.3.3, 6 and 7).

The figure below identifies how each scope meets the current demand of the GATEKEEPER stakeholders:



	A. Personal Data Processing	B. Certification of AI systems for medical devices	C. Interoperability of data	D. Data Sharing as a Service
Scope: Algorithms		✓		
Scope: Quality of datasets		✓		
Scope: Data Processing	✓			
Scope: Data Interoperability			✓	
Scope: Health data spaces				✓
Goal: Regulatory compliance	✓	✓		✓
Goal: Interoperability			✓	
Goal: Risk management	✓	✓		✓
Goal: User acceptance	✓	✓	✓	✓
Benefit: Patients' trust	✓	✓		
Benefit: Reliability of shared data		✓*		✓
Beneficiary: Healthcare Provider	✓	✓	✓	✓
Beneficiary: Public Authority			✓	✓
Beneficiary: Research			✓	✓

Figure 33: Certification scope vs. demand

3.3.3 Interoperability Certification Interest

3.3.3.1 Demand, Motivation, and Interest

The carried-out consultations gathered opinions and ideas on interoperability certification from all GATEKEEPER project stakeholders. The analysis of the received feedback during the workshop shows that the interoperability, notably through common standards, is not the hottest topic, but rather a subject of medium importance. The comments collected through Miro demonstrate a need to improve the interoperability and the unified semantics, and to increase the reliability of the data exchanges. The interoperability is also an element to improve reliability during exchanges of data among software components. Finally, the survey illustrates that the interoperability should be achieved through data models used in different kinds of datasets and through Open APIs. The certification is also recognised as a means to improve interoperability.

In the context of the GATEKEEPER project, several standards commonly used in the medical sector are of interest for interoperability certification. The list encompasses:

- HL7 FHIR: Platform specification defining a set of capabilities used across the healthcare process in all jurisdictions and in different contexts. De facto, HL7 FHIR is the outstanding standard from HL7 and globally employed.
- HL7 CDA R2.0: Document markup standard specifying the structure and semantics of clinical documents. These documents are exchanged among healthcare providers and patients. This standard is also the reference standard for the documents exchanged in the European Cross-Borders services named MyHealth@EU.

- IPS HL7 FHIR Implementation Guide: Describes how to represent an International Patient Summary (IPS) within the HL7 FHIR standard. An IPS document is in fact an electronic health record extract containing essential healthcare information about a patient. The IPS dataset is specified in the EN/ISO 27269 standard. This guide is a central piece of the IPS standard ecosystem, and Global Digital Health Partnership (GDHP) and G7 initiatives have adopted a reference implementation based on this guide.
- IPS HL7 CDA R2.0 Implementation Guide: As with the IPS HL7 FHIR Implementation Guide, describes how to represent an IPS within the HL7 CDA R2.0 standard. It is also an important element of the IPS standard ecosystem.
- IPA HL7 FHIR Implementation Guide: Specification describing how an application acting on the behalf of a patient can access information about the patient from a clinical record system using an API based on FHIR. IPA means International Patient Access.
- POCD HL7 FHIR Implementation Guide: Defines the use of FHIR resources to convey measurements and supporting data from acute care point-of-care medical devices (POCD). This standard is used by qualified professionals to receive data from systems of electronic medical records, clinical decision support and medical data archiving.
- PHD HL7 FHIR Implementation Guide: Defines the use of FHIR resources to convey measurements and supporting data from communicating Personal Health Devices (PHD). The standard is used to receive data from systems of electronic medical records, clinical decision support and medical data archiving. The communication is managed by a Personal Health Gateway (PHG) which converts the data from the PHD and uploads them into the medical systems. Basically, a PHG is implemented the content of this guide when translating PHD data into FHIR resources.
- Smart App Launch: This implementation guide describes a set of foundational patterns based on OAuth 2.0 for client applications to authorise, authenticate and integrate with systems based on FHIR.
- HL7 CDS Hooks, as known as HL7 FHIR IG: This specification describes the RESTful APIs and interactions to integrate Clinical Decision Support (CDS) between CDS clients and CDS services. A CDS client can be typically an Electronic Health Record (EHR) system or another health information system.
- HL7 Consumer Mobile Health Application Functional Framework (cMHAFF), Release 1: Standard used to assess the foundational characteristics of mobile applications. These characteristics include the security, the privacy, the data access, the data export, the transparency and the disclosure of conditions. The approach presented in this standard is customer-centric and based on lifecycle principles.
- HL7 Health Services Platform (HSP) Marketplace, Release 2: This specification presents the Marketplace API used to orchestrate the exchange of health services and executable knowledge.
- HL7 Privacy and Security Logical Data Model, Release 1: It builds upon the following standards:
  - Composite Security and Privacy Domain Analysis Model (CSP-DAM).
  - Privacy and Security Architecture Framework.

  - ISO/IEC 10181-3:1996 Access Control Framework.
  - ISO 22600-3 Privilege Management Access Control.
  - ISO 23903 Health informatics – Interoperability and integration reference architecture – Model and framework.
- HL7 Healthcare Privacy and Security Classification System (HCS), Release 1: Used for interoperable exchanges of security metadata to ensure that only authorised users access protected health information.

The four last standards, namely HL7 cMHAFF, HL7 HSP Marketplace, HL7 Privacy and Security Logical Data Model, and HL7 HCS do not directly address the interoperability of the data but are more focused on the interoperability of the data access, taking into account all the aspects linked to the security and the privacy for protected health data.

Furthermore, a final report was published by the European Commission with the title "eHealth, Interoperability of Health Data and Artificial Intelligence for Health and Care in the EU; Lot 1 – Interoperability of Electronic Health Records in the EU (2020)"[2]. This report presents the situation for the development of interoperable Electronic Health Record (EHR) systems in 2020 in the European Union, Norway, and United Kingdom. A survey was used to collect the inputs from 58 independent country experts and official government representatives. In terms of interoperability, the report shows interoperable EHRs are not yet achieved in Europe.

The semantic interoperability is applied by over two-thirds of study countries through clinical terminology standards for diagnosis, medications, and billing. For data concerning the immunisation and allergies, only half of study countries have made the clinical terminology standards mandatory. The implementation of clinical terminology servers has not yet started in most European countries. In fact, only around one-third of the countries are using SNOMED CT or LOINC for medical terminologies. In the end, a minority of European countries have already implemented eHealth Digital Service Infrastructures (DSIs).

The technical interoperability is implemented in two-thirds of study countries and permits to access patient summaries and ePrescriptions services through an online portal. A limited number of European countries are able to exchange patient summaries and ePrescriptions across their borders. Some countries have not yet defined an architecture for their Electronic Health Record (EHR) system. Some other countries have deployed EHR systems which are not routinely used. The situation is in fact different from country to country in terms of deployment of EHR systems. In Europe, there is not yet clearly structured electronic health data. Reasons include an absence of training for the healthcare staff and for auditing the quality of the electronic health data.

The report highlights that several aspects should be taken into account to realise the interoperability of EHR systems across the whole of Europe:

[2] European Commission, eHealth, Interoperability of Health Data and Artificial Intelligence for Health and Care in the EU, Lot 1 – Interoperability of Electronic Health Records in the EU (2020), https://digital-strategy.ec.europa.eu/en/library/interoperability-electronic-health-records-eu

- Legal: National legislations should allow the access and sharing of electronic health data.
- Financial and organisational measures: Interoperability should be promoted and supported by sufficient and efficient means.
- Security and access: Electronic identification and cybersecurity should be put in place in an appropriate way.
- Semantic interoperability: International standards should be applied by each European country and their usage is mandatory also at the national level.
- Technical interoperability: The exchange of electronic health data, such as patient summaries and ePrescriptions, should be possible through interoperable services and solutions across Europe.

These aspects are in fact key factors to succeed in the interoperability of EHR systems in Europe. Currently, the fastest technical manner is to establish common standards and digital infrastructures. An interoperability certification also provides good means to ensure that these standards are properly applied in the digital infrastructures dedicated to health. The availability of interoperable clinical data will also trigger more advanced health research, personalised medicine, genome sequencing, and Artificial Intelligence (AI). Indeed, these domains require a lot of data provided by different sources across Europe. It will not be possible to implement in an efficient way European initiatives, such as the European 1+ Million Genomes (1+MG) or the Genome of Europe (GoE), without the interoperability of electronic health data.

3.3.3.2 Scope

Based on the feedback received from the different types of GATEKEEPER stakeholders, the interoperability of data provided through the HL7 standard family is the most important topic to be addressed by a potential interoperability certification. The scope of an eventual interoperability certification would mainly focus on the interoperability of the data representing through the HL7 FHIR formats. The aspects linked to security and privacy could however be handled by the data protection certification already mentioned in this deliverable.

4 Offer Side Analysis

4.1 Data protection-related standards and certification options

This section seeks to present the main options when considering data protection standards for certification of compliance. It builds on the work of GATEKEEPER T8.1 and its deliverables.

4.1.1 ISO/IEC

ISO/IEC 27000 series is a family of international standards for Information security, cybersecurity and privacy protection. On top of this, **ISO/IEC 27701** builds on both ISO/IEC 27001 and 27002 including a set of additional requirements and guidance dedicated to the establishment, implementation, maintenance, and continuous improvement of Privacy Information Management Systems (PIMS). Although this voluntary certification partially covers some of the obligations contained in the GDPR, this standard by itself cannot make the GATEKEEPER assets GDPR compliant as it only establishes requirements for the management system, but not for the processing of activities (subject scope of the GDPR). Additionally, it is not eligible for recognition under Article 42 of the GDPR, as its main certification scope (PIMS) is out of the scope of the GDPR. More specifically, the EDPB Guidelines state not only that management systems or "governance processes" cannot receive a certification under Art. 42(1) GDPR, but this includes certification of persons managing them as well (EDPB, 2018b, p.13).

In addition, the terminology used by ISO/IEC 27000 and 27701 is different from the one in the GDPR, namely, ISO standards typically refer to personal identifiable information rather than personal data. Moreover, according to the GDPR, the drafting of certification requirements and the certification process are closely monitored by the data protection authorities. For instance, a data protection authority is entitled to refuse the issuance (GDPR, ART 58(2)) of the certification when the conditions of issuance are not met by the certified entity. It is also entitled to withdraw a certification when the conditions of issuance are no longer met (GDPR, art 42(7)). Thus, ISO privacy standards' approach differ significantly from the one enshrined under the GDPR (Eric Lachaud, 2020).

What is more, the ISO/IEC 27701 takes a risk-based approach. Each candidate entity will have to comply with the data protection requirements set in the standard depending on the context and level of risk identified in each data processing. This risk management process aims to identify and mitigate security risks associated with the loss of confidentiality, integrity, and availability (ISO/IEC 27005: 2018, Subclause 3.2.). Although the GDPR also takes a risk-based approach, the CIA triad is not the only element that is taken into consideration. Rather a more general identification and mitigation of threats on data subjects' rights and freedoms are also considered. Under the GDPR, data protection is seen as a fundamental right that needs to be balanced with the rest of fundamental rights enshrined under the EU Charter (GDPR, recitals 1, 4). The EDPB has also pointed out the difference between industry standards that focus on security while the GDPR is "*directed at the protection of fundamental rights of natural persons"* (EDPB, 2018a, p. 16). Other relevant ISO standards include ISO/IEC 29134:2017 Information technology — Security techniques — Guidelines for privacy impact assessment, the ISO/IEC 29184:2020 that focuses on consent, openness, transparency and notice, ISO/IEC 27018:2019 Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors, ISO/IEC 27555:2021 Information security, cybersecurity and privacy protection — Guidelines on personally identifiable information deletion, ISO/IEC

27002:2022 Information security, cybersecurity, and privacy protection – Information security controls, and ISO/PC 317 Consumer protection: privacy by design for consumer goods and services, which is currently under development. However, these standards only focus on a few specific requirements resulting in a significantly narrower scope, and they are not supervised by the data protection authorities. It should also be noted that by design, ISO standards are applicable worldwide, thus a perfect alignment with the GDPR can never be achieved. What is more, when it comes to national laws of Member States that deviate from the GDPR, the ISO standards cannot be extended to cover these requirements as well, causing significant practicalities to the controllers.

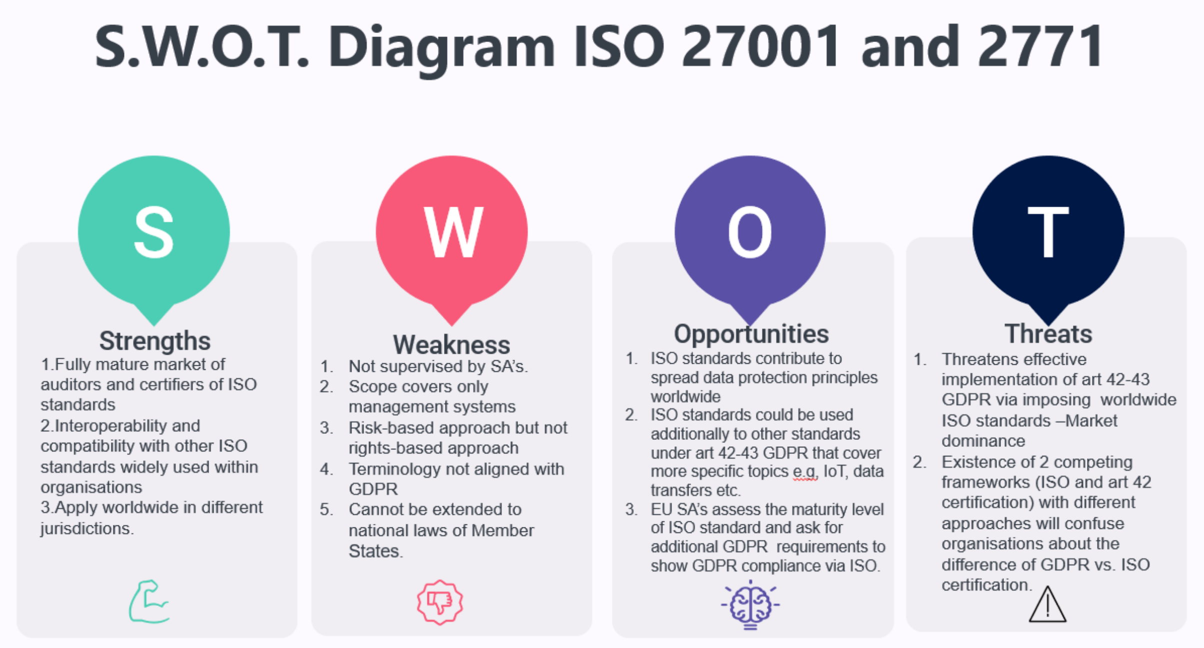
The above does not imply that ISO standards cannot be utilised for certification. However, considering the inherent differences between the certification scheme under the GDPR and the current use for ISO standards, it is highly unlikely that relevant ISO standards can directly become an approved certification scheme under the GDPR without significant modifications. This in practice might lead to two simultaneously existing certification frameworks that have different approaches and different market power. Considering that ISO standards are available worldwide and already well-known to organisations, the market dominance of ISO would be hard to disrupt, unless organisations realise the different approach and advantages a certification under the GDPR will bring.

However potential opportunities that will utilise the market strength of ISO standards might arise. This inter alia includes the chance an organisation would adopt an ISO standard and be issued a certification under art 42 GDPR on a specific subject scope (for instance Internet of things, AI, children's data) that the ISO standard does not cover and is of interest. In this way, the art. 42 GDPR certification will supplement ISO standards without overlaps, leveraging GDPR certification by cooperating with ISO and targeting its mature audience. This is aligned with EDPB guidance on the certification criteria that should consider ISO standards and be interoperable with these (EDPB 2018, p.16).

In addition, data protection authorities in charge of approving criteria of certification (GDPR, Arts. 58 (3)(f),42(5)) could ask organisations that already have adopted relevant ISO standards to additionally comply with specific requirements under the GDPR and depending on the extent of their compliance, assurance levels for ISO standards that show the GDPR maturity level could be integrated. The Cybersecurity Act, already includes assurance levels for the European Certification Scheme which ENISA will lead (Cybersecurity Act, 52(1)). Although this envisioned maturity assessment will not lead to a new certification *per se*, organisations will then have the option to include a 'basic', 'substantial 'or 'high' GDPR assurance level in their ISO certification that shows that this particular certification activity is partially compliant with the GDPR, following the additional criteria/requirements the EDPB or the data protection authority will require for each assurance level. This might open the doors for making GDPR compliance and standardisation widespread across the globe, again via utilising the strengths of ISO standards. However, for the latter opportunity, potential amendments to the GDPR on the powers of data protection authorities might be necessary.

As far as the British Standards are concerned, the **BS10012:2017** +A1:2018-Personal Information Management System standard came as a response to the GDPR, and it provides a best "*practice framework for a personal information management system that is aligned to the principles of the EU GDPR. This specific standard has the benefit of aligning with both the GDPR terminology and simultaneously being consistent with ISO Standards. In terms of scope, it outlines the core requirements organisations' need to consider when collecting, storing, processing, retaining or disposing of personal records related to individuals"* (BSI, Personal information management). BS 10012 is thus better aligned with the GDPR and DPA 2018, whereas ISO 27701 avoids aligning itself with any specific data protection regime. However, the scope of this standard is still narrower than the GDPR as it still applies only to PIMS.

Below is a compact SWOT analysis for ISO standards on data protection followed by a brief listing of relevant standard for medical devices.



S.W.O.T. Diagram ISO 27001 and 2771

Strengths

1.Fully mature market of auditors and certifiers of ISO standards
2.Interoperability and compatibility with other ISO standards widely used within organisations
3.Apply worldwide in different jurisdictions.

Weakness

1. Not supervised by SA's.
2. Scope covers only management systems
3. Risk-based approach but not rights-based approach
4. Terminology not aligned with GDPR
5. Cannot be extended to national laws of Member States.

Opportunities

1. ISO standards contribute to spread data protection principles worldwide
2. ISO standards could be used additionally to other standards under art 42-43 GDPR that cover more specific topics e.g, IoT, data transfers etc.
3. EU SA's assess the maturity level of ISO standard and ask for additional GDPR requirements to show GDPR compliance via ISO.

Threats

1. Threatens effective implementation of art 42-43 GDPR via imposing worldwide ISO standards –Market dominance
2. Existence of 2 competing frameworks (ISO and art 42 certification) with different approaches will confuse organisations about the difference of GDPR vs. ISO certification.

Figure 34: SWOT analysis for ISO 27001 and 27701 Standards

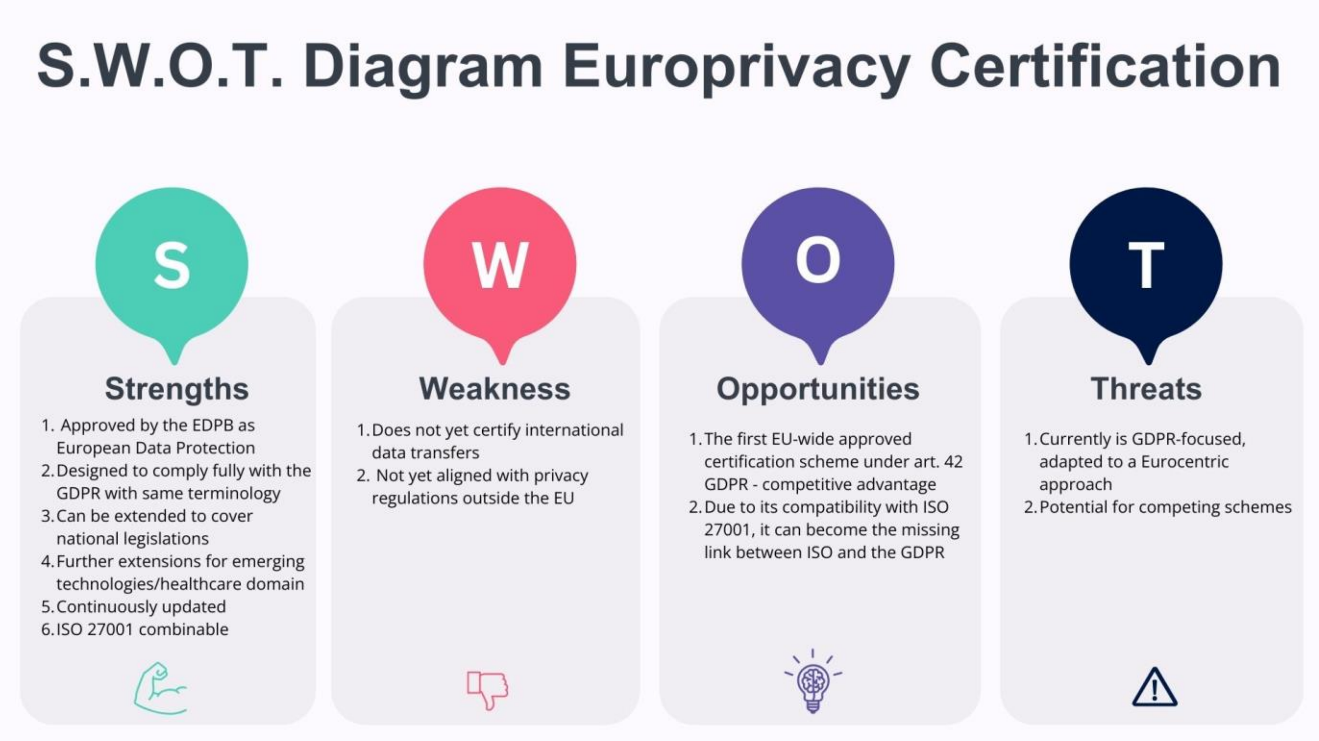
4.1.2 ECCP/Europrivacy

Europrivacy is a European Data Protection Seal, an EU-wide certification scheme that assesses and certifies the conformity of personal data processing activities with the GDPR. It combines various methodologies, such as documentation review, sampling analysis, technical tests, inspections, and interviews. It was developed through the European Research Programme Horizon 2020, co-financed by the European Commission and the Swiss Ministry for Research and Education. The scheme was originally developed by Archimede Solutions SARL, which was the original Scheme Owner. The role and functions of the Scheme Owner have now been transferred to the European Centre for Certification and Privacy (ECCP) in Luxembourg.

As a GDPR-specific certification, Europrivacy does not have the weaknesses ISO standards have. It uses identical terminology with the GDPR, it can be extended to emerging technologies (e.g., artificial intelligence) domains (e.g., healthcare) and to national laws of Member States. It has also been developed in consultation with national supervisory authorities, while it is continuously updated by the European Centre for Certification and Privacy and its International Board of Experts in data protection.

Another important advantage of Europrivacy is that it is interoperable with ISO standards and can be easily combined with complementary management system certifications, such as ISO/IEC 27001 or 27701. The certification itself is also aligned with the applicable ISO/IEC 17065 and 17021-1 principles.

Considering the SWOT analysis for ISO standards at 4.1.1 above, one can easily understand the difference of the Europrivacy certification and the rest of available ISO standards, but also the opportunities that arise if we combine these two different standardisation frameworks. If Europrivacy is combined with ISO or other international standards then significant gaps that exist in ISO standards are also covered (scope, national laws, domain, terminology), providing to successful applicants a holistic compliance not only with the GDPR but also beyond its scope through the ISO standards. Especially as the EDPB has approved the certification scheme and endorsed it under art 42 GDPR, the Europrivacy scheme is now supervised by DPAs, resolving one more weakness of ISO standards. On the other side, the Europrivacy scheme will also benefit from this combination as the competitive advantage it brings to the mature audience of ISO standards will facilitate its entrance into the market and offer a strong boost in comparison with other potential competitors that may become certified under art. 42 GDPR.



S.W.O.T. Diagram Europrivacy Certification

S

Strengths

1. Approved by the EDPB as European Data Protection
2. Designed to comply fully with the GDPR with same terminology
3. Can be extended to cover national legislations
4. Further extensions for emerging technologies/healthcare domain
5. Continuously updated
6. ISO 27001 combinable

W

Weakness

1. Does not yet certify international data transfers
2. Not yet aligned with privacy regulations outside the EU

O

Opportunities

1. The first EU-wide approved certification scheme under art. 42 GDPR - competitive advantage
2. Due to its compatibility with ISO 27001, it can become the missing link between ISO and the GDPR

T

Threats

1. Currently is GDPR-focused, adapted to a Eurocentric approach
2. Potential for competing schemes

Figure 35: SWOT Analysis for Europrivacy

4.1.3 HL7

HL7 provides a comprehensive framework and related standards for the exchange, integration, sharing and retrieval of electronic health information that supports clinical practice and the management, delivery, and evaluation of health services. For the GATEKEEPER project, the most relevant standards and implementation guides are presented in the table below:

Table 4: HL7 relevant standards

Current Available Standards	Description	Territorial Application /publication status

HL7 FHIR	HL7 FHIR is a platform specification that defines a set of capabilities use across the healthcare process, in all jurisdictions, and in lots of different contexts, including health care data exchange	Universal Globally used. It is the HL7 outstanding standard.
HL7 CDA R2.0	The HL7 Version 3 Clinical Document Architecture (CDA®) is a document markup standard that specifies the structure and semantics of "clinical documents" for the purpose of exchange between healthcare providers and patients.	Universal Globally used. Reference standard for the document exchanged in the European Cross-Borders services (MyHealth@EU)
International Patient Summary (IPS) HL7 FHIR Implementation Guide	Implementation Guide describing how to represent an IPS by using HL7 FHIR. An International Patient Summary (IPS) document is an electronic health record extract containing essential healthcare information about a subject of care. The IPS data set is specified in the EN/ISO 27269 standard.	Universal Standard For Trial Use One of the standards constituting the IPS standard ecosystem. Reference implementation adopted by the GDHP[3] and the G7[4] initiatives
International Patient Summary (IPS) HL7 CDA R2 Implementation Guide	Implementation Guide describing how to represent an IPS by using HL7 CDA R2.	Universal Standard For Trial Use One of the standards constituting the IPS standard ecosystem.
International Patient Access (IPA) HL7 FHIR Implementation Guide	This specification describes how an application acting on behalf of a patient can access information about the patient from a clinical records system using a FHIR based API.	Universal Standard For Trial Use Ballot

[3] Global Digital Health Partnership (GDHP) https://gdhp.nhp.gov.in/home/index/our-work

[4] See G7 declaration https://www.g7uk.org/g7-health-ministers-meeting-communique-oxford-4-june-2021/

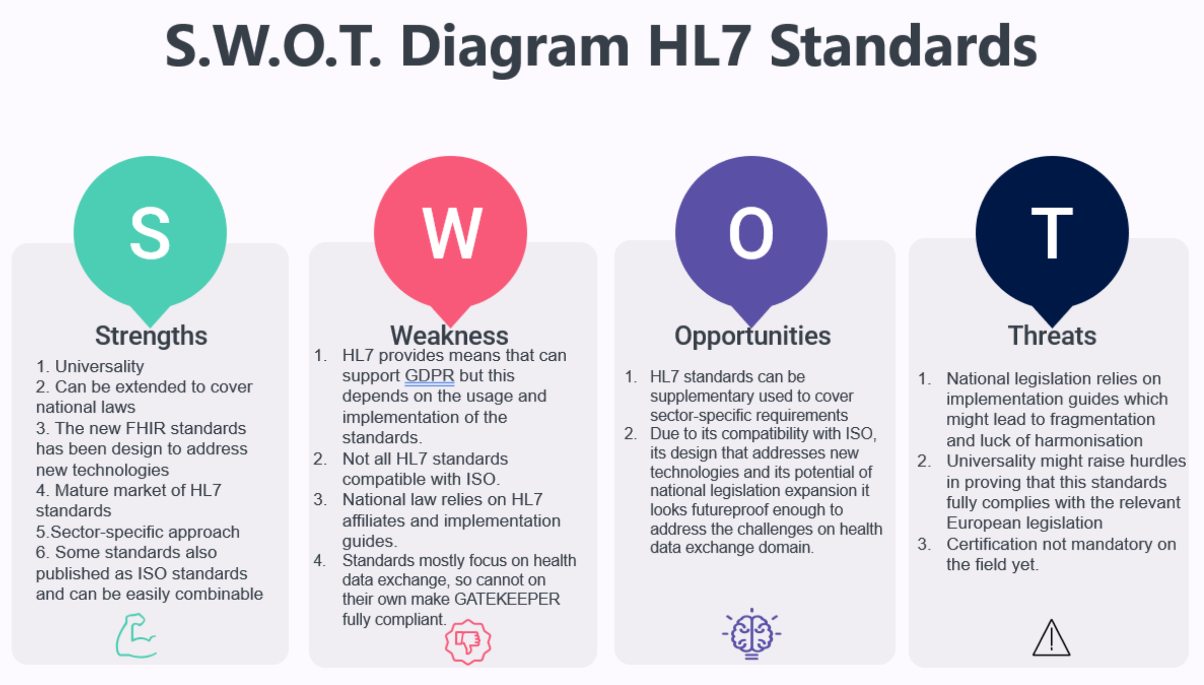
Point-of-Care Device (POCD) HL7 FHIR Implementation Guide	This Implementation Guide defines the use of FHIR resources to convey measurements and supporting data from acute care point-of-care medical devices (PoCD) intended for use by qualified professional to receiving systems for electronic medical records, clinical decision support, and medical data archiving for aggregate quality measurement and research purposes.	Universal Standard For Trial Use Ballot
Personal Health Device (PHD) HL7 FHIR Implementation Guide	This Implementation Guide defines the use of FHIR resources to convey measurements and supporting data from communicating Personal Health Devices (PHDs) to receiving systems for electronic medical records, clinical decision support, and medical data archiving for aggregate quality measurement and research purposes. In most cases there is a Personal Health Gateway (PHG) that handles the PHD communications. The PHG translates the PHD data to the appropriate form and uploads it to the receiving systems. Uploads generated by Continua compliant PHGs shall use this implementation guide when transforming the PHD data to FHIR resources.	Universal Standard For Trial Use Ballot
SMART App Launch	This implementation guide describes a set of foundational patterns based on OAuth 2.0 for client applications to authorise, authenticate, and integrate with FHIR-based data systems.	Universal Standard For Trial Use
HL7 CDS Hooks (HL7 FHIR IG)	The CDS Hooks specification describes the RESTful APIs and interactions to integrate Clinical Decision Support (CDS) between CDS Clients (typically Electronic Health Record Systems (EHRs) or other health information systems) and CDS Services.	Universal Standard For Trial Use

HL7 Consumer Mobile Health Application Functional Framework (cMHAFF), Release 1	Standard against which a mobile app's foundational characteristics - including security, privacy, data access, data export, and transparency/disclosure of conditions - can be assessed. Lifecycle, customer-centric approach	Universal Standard For Trial Use
HL7 Health Services Platform (HSP) Marketplace, Release 2	The Marketplace API specification serves as a building block for orchestrating the exchange of such services and executable knowledge. Products deployed in an enterprise architecture are constituent building blocks in a larger information technology (IT) ecosystem. The deployment and runtime characteristics of each individual building block as well as underlying infrastructure naturally vary across organisations, requiring each service deployment to be further tailored to local IT needs.	Universal Standard For Trial Use
HL7 Privacy and Security Logical Data Model, Release 1	The HL7 Privacy and Security Logical Data Model builds upon the Composite Security and Privacy DAM, the Privacy and Security Architecture Framework and other foundational security standards including ISO/IEC 10181-3:1996 Access Control Framework, ISO 22600-3 Privilege Management Access Control, and ISO 23903 Health informatics — Interoperability and integration reference architecture – Model and framework.	
HL7 Healthcare Privacy and Security Classification System (HCS), Release 1	Enables interoperable exchange of security metadata to ensure that only authorised users access protected health information.	

The HL7 Standards are developed through an open consensus-based process. Some of these standards are adopted by authorities, but in general there is no supervisory authority that monitors them, and the certification is voluntary. As far as the interplay with ISO is concerned, some HL7 standards are published also as ISO standards, e.g., CDA so in such cases these can be easily combined with other ISO standards as well.

A significant advantage of these standards is that they are universally applicable, and no market disruption is necessary. The new FHIR standard has been designed to address new technologies, while national legislation can be considered through the HL7 affiliates that publish implementation guides.

Regarding data protection, **the HL7 standards do not aim for data protection certification**. However, depending on the standard, means to support compliance with some of the GDPR requirements could be provided. This implies that if combined with other data protection standards, HL7 standards can facilitate compliance with the GDPR.



S.W.O.T. Diagram HL7 Standards

S

Strengths

1. Universality
2. Can be extended to cover national laws
3. The new FHIR standards has been design to address new technologies
4. Mature market of HL7 standards
5.Sector-specific approach
6. Some standards also published as ISO standards and can be easily combinable

W

Weakness

1. HL7 provides means that can support GDPR but this depends on the usage and implementation of the standards.
2. Not all HL7 standards compatible with ISO.
3. National law relies on HL7 affiliates and implementation guides.
4. Standards mostly focus on health data exchange, so cannot on their own make GATEKEEPER fully compliant.

O

Opportunities

1. HL7 standards can be supplementary used to cover sector-specific requirements
2. Due to its compatibility with ISO, its design that addresses new technologies and its potential of national legislation expansion it looks futureproof enough to address the challenges on health data exchange domain.

T

Threats

1. National legislation relies on implementation guides which might lead to fragmentation and luck of harmonisation
2. Universality might raise hurdles in proving that this standards fully complies with the relevant European legislation
3. Certification not mandatory on the field yet.

Figure 36: SWOT Analysis for HL7 Standards

4.1.4 NIST Certification

The National Institute of Standards and Technology (NIST) is now part of the U.S. Department of Commerce. Aiming at promoting U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology, the NIST standards territorially mostly focus on the US. Among others it provides standards for AI, cybersecurity, and health & bioscience. However, the NIST standards do not take into account any European legislation and it seems inappropriate for GATEKEEPER to rely on these. For instance, the Privacy Framework complies only under the relevant US privacy laws (CCPA/CRPA) and does not use the GDPR terminology. The same applies for the cybersecurity framework, which focuses on federal government compliance (for instance SP 800-213A-IoT Device Cybersecurity Guidance for the Federal Government). However, NIST certification might be beneficial in a potential extension of GATEKEEPER in the US. In addition, standards for AI systems are currently being developed. In particular, NIST is developing a framework to better manage risks to individuals, organisations, and society associated with AI. The NIST Artificial Intelligence Risk Management Framework (AI RMF or Framework) will be voluntary and aims to make the design, development, and use of AI products trustworthy.

4.2 AI Certification

As already analysed above, the proposed AI Act sets specific requirements regarding high-risk systems. Although standards continue to be developed to adapt to these new requirements, below is a current overview of the published (in bold) or under development international standards and their alignment with the AI Act requirements that have been considered in the context of GATEKEEPER WP8's activities. These can be found below alongside a table mentioning the relevant standards for Medical Devices. In addition to these tables, a summary of each standard can be found in Appendix B.

Table 5: Standards vs AI Act's Obligations

Requirement	Standards	Description
Data governance	1. **ISO/IEC 25024:2015** 2. ISO/IEC AWI 5259 3. ISO/IEC 24668	1. **Systems and software Quality Requirements and Evaluation (SQuaRE) Measurement of data quality** 2. Data Quality for AI (ML) 3. Process Management framework for Big Data analytics
	4. IEEE P7002 5. IEEE P7003 6. IEEE P7006 7. IEEE P2801 8. IEEE P2807 9. IEEE P2863	4. Standard for Data Privacy Process 5. Algorithmic Bias Considerations 6. Personal Data AI Agent working group 7. Quality Management of Datasets for Medical Artificial Intelligence 8. Framework of Knowledge Graphs 9. Organisational Governance of Artificial Intelligence
	10. ETSI DES/eHEALTH-008 11. ETSI DGR/CIM-007-SEC 12. ETSI DGR/SAI-002 13. ETSI TR 103 674	10. eHEALTH Data recording requirements 11. Context Information Management (CIM); Security and Privacy 12. Securing Artificial Intelligence (SAI); Data Supply Chain Security 13. Introduction of AI into IoT systems and, particularly, into the oneM2M architecture.
	1. ISO/IEC DTS 4213.2 2. ISO/IEC CD 24029-2 3. ISO/IEC DIS 23894	1. Artificial Intelligence-Assessment of machine learning classification performance

Risk management system	4. ISO/IEC AWI TR 5469	2. Assessment of the robustness of neural networks 3. Artificial intelligence - Risk Management System 4. Functional Safety of AI Systems
	5. IEEE P 7009 6. IEEE P2863	5. Standard for Fail-Safe Design of Autonomous and Semi-Autonomous Systems 6. Recommended Practice for Organisational Governance of Artificial Intelligence
Technical documentation **And** **Record-keeping**	1. **ISO/IEC 24372:2021** 2. ISO/IEC DTR 24368 3. ISO/IEC AWI TR 5469 4. ISO/IEC CD 5338 5. ISO/IEC DIS 24668	1. **Overview of computational approaches for AI systems** 2. Overview of ethical and societal concerns 3. Functional safety and AI systems 4. AI system life cycle processes 5. Process management framework for big data analytics
	6. IEEE P7001 7. **IEEE P7000-2021** 8. IEEE P2801 9. IEEE P2863	6. Transparency of Autonomous Systems 7. **IEEE Standard Model Process for Addressing Ethical Concerns during System Design** 8. Recommended Practice for the Quality Management of Datasets for Medical Artificial Intelligence 9. Recommended Practice for Organisational Governance of Artificial Intelligence
	10. **ETSI DGR/SAI-002**	10. **Data Supply Chain Report**
Transparency obligations	1. **ISO/IEC TR 24028:2020** 2. ISO/IEC AWI TS 6254	1. **Overview of trustworthiness in artificial intelligence** 2. Objectives and approaches for explainability of ML models and AI systems

	3. IEEE P7001 4. IEEE P7012 5. IEEE P7009 6. IEEE P2863	3. Transparency of Autonomous Systems 4. Standard for Machine Readable Personal Privacy Terms 5. Standard for Fail-Safe Design of Autonomous and Semi-Autonomous Systems 6. Recommended Practice for Organisational Governance of Artificial Intelligence
Human oversight	1. IEEE P7006 2. IEEE P7014 3. IEEE P2863 4. **IEEE P7000-2021**	1. Standard for Personal Data Artificial Intelligence (AI) Agent 2. Standard for Ethical considerations in Emulated Empathy in Autonomous and Intelligent Systems 3. Recommended Practice for Organisational Governance of Artificial Intelligence 4. **IEEE Standard Model Process for Addressing Ethical Concerns during System Design**
Accuracy, robustness and cybersecurity	1. **ISO/IEC TR 24028:2020** 2. **ISO/IEC 24027:2021** 3. **ISO/IEC TR 24029-1:2021** 4. **ISO/IEC 20547-4:2020** 5. ISO/IEC AWI TR 5469	1. **Overview of trustworthiness in artificial intelligence** 2. **Bias in AI systems and AI aided decision making** 3. **Assessment of the robustness of neural networks** 4. **Information technology — Big data reference architecture — Part 4: Security and privacy** 5. Functional safety and AI systems
	6. **ETSI DGR SAI 005** 7. **ETSI DGR SAI 002** 8. ETSI DGR SAI 001 9. ETSI DGR SAI 003 10. ETSI DGR/CIM-007-SEC 11. **ETSI TS 103 327**	6. **Securing Artificial Intelligence (SAI); Mitigation Strategy Report** 7. **Securing Artificial Intelligence (SAI); Data Supply Chain Security** 8. Securing Artificial Intelligence (SAI); AI Threat Ontology 9. Securing Artificial Intelligence (SAI); Security Testing of AI 10. Context Information Management (CIM); Security and Privacy 11. **Smart Body Area Networks (SmartBAN);**

		Service and application standardised enablers and interfaces, APIs and infrastructure for interoperability management
	11. IEEE/P 2802 12. IEEE/P 7003 13 IEEE/ P 7002	11. Standard for the Performance and Safety Evaluation of Artificial Intelligence Based Medical Device: Terminology 12. Algorithmic Bias Considerations 13. Draft Standard for Data Privacy Process
Quality Management system	1. ISO/IEC CD 25059 2. ISO/IEC FDIS 38507 3. ISO/IEC CD 42001 4. ISO/IEC AWI TS 5471	1. SQuaRE-Quality model for AI systems 2. Governance implications of the use of artificial intelligence by organisations 3. AI Management System 4. Quality evaluation guidelines for AI systems
	5. IEEE P/2801 6. IEEE P2863	5. Recommended Practice for the Quality Management of Datasets for Medical Artificial Intelligence 6. Recommended Practice for Organisational Governance of Artificial Intelligence
	7. ETSI TR 103 749	7. INT Artificial Intelligence (AI) in Test Systems and Testing AI models

Table 6 Relevant standards for medical devices

Current Available Standards	Description
ISO 20417:2021	Information to be supplied by the manufacturer
ISO 15223-1:2021	Symbols to be used with information to be supplied by the manufacturer
ISO 14971:2019	Medical devices — Application of risk management to medical devices
ISO/TR 20416:2020	Post-market surveillance for manufacturers

IEC 62304:2006 (reviewed in 2021)	Medical device software — Software life cycle processes
IEC 82304-1:2016 (reviewed in 2020)	Health software - General requirements for product safety
ISO/TS 82304-2:2021	Health and wellness apps. Quality and reliability
ISO 13485:2016 (reviewed in 2020)	Quality management systems. Requirements for regulatory purposes
IEEE P2621	MEDICAL DEVICES CYBERSECURITY

4.3 Interoperability certification

4.3.1 OTA/F-Interop

The F-Interop project was a European Horizon 2020 project providing online interoperability and performance test tools to support emerging technologies from research to standardisation and market launch. These online tools are intended to accelerate the standardisation processes and the developments of ICT products. Indeed, thanks to the remote access to tools, there is no longer a need to travel to realise tests; furthermore, the costs and time required to travel are eliminated. Different kinds of testing tools are available on the online platform:

- Online interoperability tests and validation tools;
- Remote compliance and conformance tests;
- Scalability tests;
- Quality of Service (QoS) tests;
- Online privacy test tools.

These testing tools were designed first of all for the Internet of Things (IoT), in particular to test devices using protocols and standards, such as oneM2M, 6TiSCH and Web of Things. These standards are respectively supported by ETSI, IETF, and W3C. New testing tools can be added to the F-Interop platform as additional tool extensions, notably for new protocols and standards to be tested in real conditions.

After the end of the Horizon 2020 F-Interop project, a legal entity named Online Testing Association (OTA) was created to maintain the F-Interop platform. The URL to reach out the F-Interop platform and its testing tools is https://www.finterop.eu/.

In the context of the GATEKEEPER project, one of the initially identified options was the potential addition of a new extension to test the interoperability of the Electronic Health Records (EHRs) based on the HL7 standard family. Indeed, the utilisation of the F-Interop platform could accelerate the research and the development of new products and services designed around HL7, ensuring the interoperability among the different solutions based on the HL7 standard family.

4.3.2 ONC Health IT Certification Program

The Office of the National Coordinator for Health Information Technology (ONC)[5] is a federal American entity in charge of promoting and supporting the adoption of health information technology. In particular, the exchanges of health information through standards are very encouraged by the ONC. The ONC Health IT Certification Program[6] is based on ISO/IEC and NIST standards such as:

- ISO/IEC 17011 Conformity assessment - Requirements for accreditation bodies accrediting conformity assessment bodies
- ISO/IEC 17025 Testing and calibration laboratories
- ISO/IEC 17065 Conformity assessment - Requirements for bodies certifying products, processes and services
- ISO/IEC 17067 Conformity assessment - Fundamentals of product certification and guidelines for product certification schemes
- NIST Handbook 150 National Voluntary Laboratory Accreditation Program - Procedures and General Requirements
- NIST Handbook 150-31 NVLAP Healthcare Information Technology Testing

The interoperability is of course also covered by the ONC Health IT Certification Program. There are two types of certifications:

- ONC-ATL (ONC-Authorised Testing Laboratory): A laboratory certified ONC-ATL can perform ONC testing.
- ONC-ACB (ONC-Authorised Certification Body): A certification body certified ONC-ACB can provide certification decisions and conduct the surveillance of the ONC certifications.

So, if a developer would like to certify their health information technology solution in the context of the ONC Health IT Certification Programme, they should first contact a laboratory certified ONC-ATL. The laboratory will perform the tests on the health IT solution. When all the tests are passed, the developer will receive the certification from a certification body certified ONC-ACB. At the end, the health IT solution will be registered into the CHPL (Certified Health IT Product List)[7] monitored by the ONC-ACB certification bodies.

The interoperability of HL7 FHIR is tested with the Inferno open-source tool developed by OMC and MITRE[8]. The Inferno tool has its own website: https://inferno.healthit.gov/. There are basically two versions of Inferno:

[5] ONC website: https://www.healthit.gov/

[6] ONC Health IT Certification Program: https://www.healthit.gov/topic/certification-ehrs/about-onc-health-it-certification-program

[7] CHPL website: https://chpl.healthit.gov/#/resources/overview

[8] MITRE website: https://www.mitre.org/

- ONC Programme Edition: This version is used to prepare the health IT solution to the certification.
- Community Edition: This version is addressed to all the developers working with HL7 FHIR to test their solution in the context of their own use cases, without any link to the certification.

Both versions are available from the Inferno website or directly from GitHub. Independently of Inferno, there are around 250 repositories on GitHub about HL7 FHIR testing. For instance, we can find the FHIR test cases at https://github.com/FHIR/fhir-test-cases and Crucible at https://github.com/fhir-crucible/crucible. The Crucible application permits to test a HL7 FHIR implementation against a FHIR server.

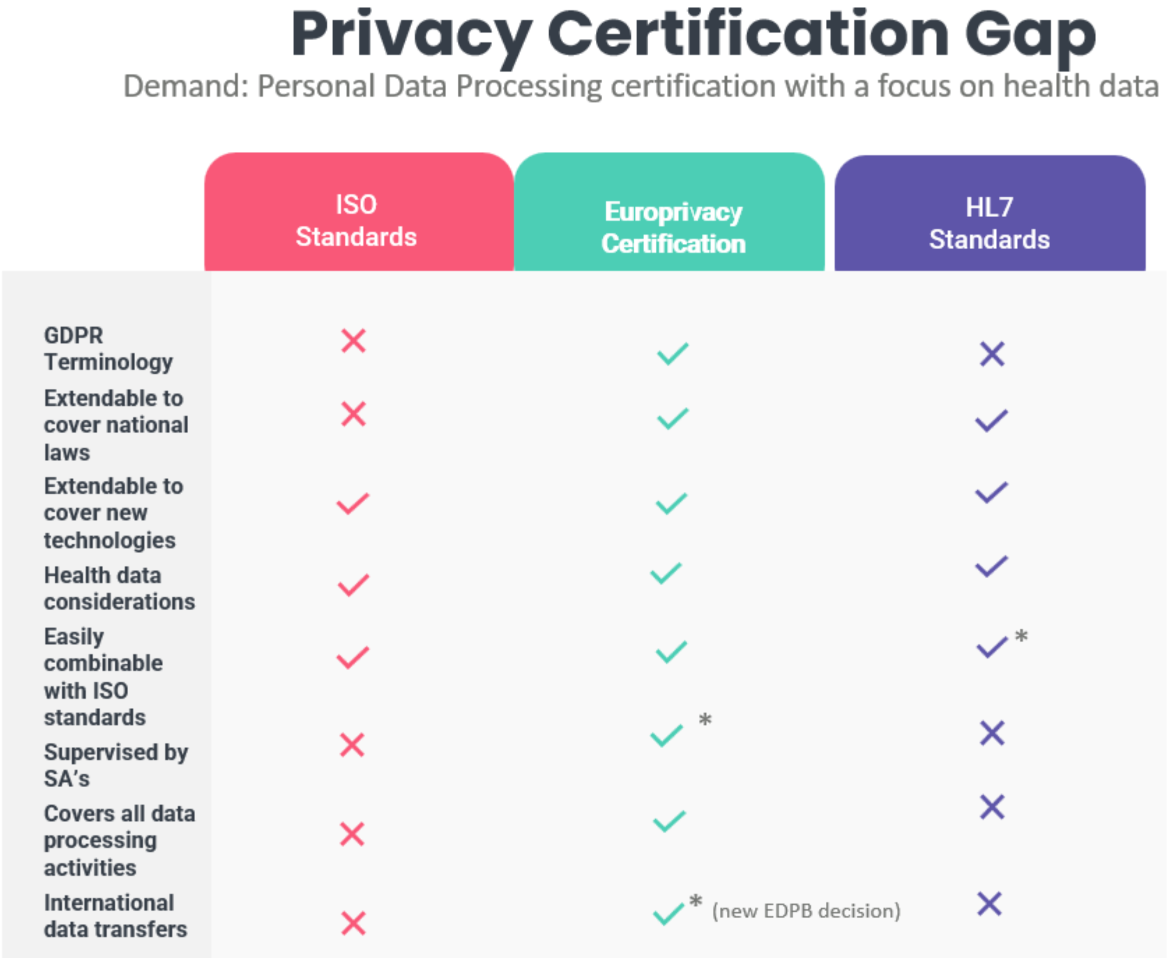
5 Gap Analysis and Priority Definition

5.1 Demand and offer comparison

In order to identify gaps, a comparison of the current demand and existing standardisation offers or those being developed is necessary. Considering the current demand identified via the survey and workshop in section 3 and the current offer in section 4, the actual gaps can then be identified as shown in the matrixes below.

5.1.1 Privacy Certification Gap

As already explained in section 3, a certification on personal data processing would cover the current stakeholder demand on data protection and enable healthcare providers to minimise risks and comply with the GDPR while patients' trust would be enhanced in regard to their right to personal data protection. Considering the offer analysis (and SWOT analysis) in section 4.1 the current comparative table of the demands and offer is provided:



Privacy Certification Gap

Demand: Personal Data Processing certification with a focus on health data

	ISO Standards	Europrivacy Certification	HL7 Standards
GDPR Terminology	✗	✓	✗
Extendable to cover national laws	✗	✓	✓
Extendable to cover new technologies	✓	✓	✓
Health data considerations	✓	✓	✓
Easily combinable with ISO standards	✓	✓	✓*
Supervised by SA's	✗	✓*	✗
Covers all data processing activities	✗	✓	✗
International data transfers	✗	✓* (new EDPB decision)	✗

Figure 37: Privacy Certification Gap

From the figure above, it can be said that at the moment of publication of this deliverable only the Europrivacy certification could serve to demonstrate compliance of personal data processing activities occurring during the GATEKEEPER project fully compliant with the GDPR (however this was not yet settled at earlier stages of the project and this led to the development of criteria extensions as reported in Section 7.1), with the only exception of certification for international data transfers, which is still under discussion at EDPB level.

The Europrivacy certification is the only one among these three models that is fully aligned with the GDPR, can be easily extended to focus on both national legislation on health data and new and innovative technologies like AI, and can make GATEKEEPER GDPR compliant aside from the international data transfers. Considering that some of the GATEKEEPER pilots are not based within the EU (although no data transfers were performed among them and the EU-based pilots), and that the Europrivacy certification scheme has been designed to include international data transfers, during the project, it was considered worthwhile to explore whether a certification extension that could cover at least international data transfers regarding these specific countries could be also explored.

This being considered, an additional avenue of work was deemed relevant in the shape of the specification of tailored criteria considering multiple relevant regulatory frameworks for their use in healthcare and innovative technologies, as described below.

5.1.2 Health Data Sharing Certification Gap

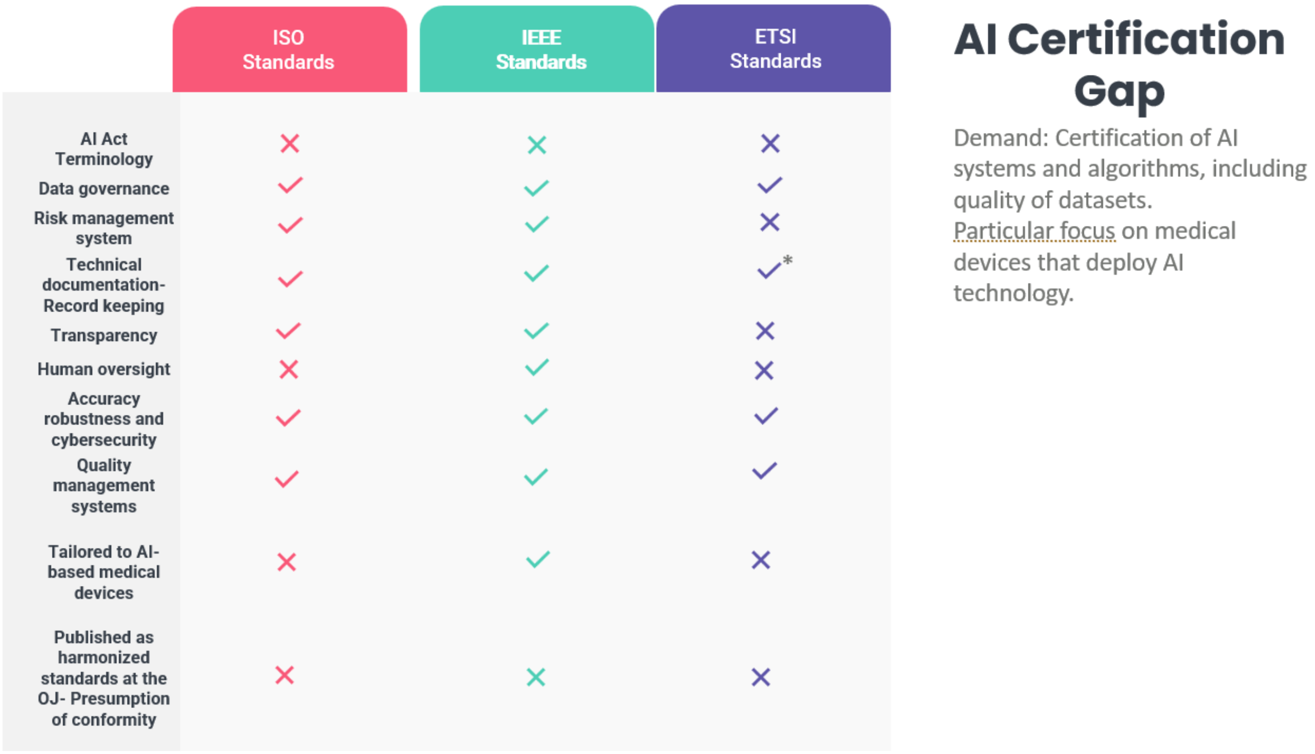
Another important gap that is identified is the absence of a certification mechanism for health data sharing. Considering that GATEKEEPER did not only process personal data but also data that cannot indirectly identify natural persons, and that data was shared among various stakeholders, addressing this gap was deemed to be important.

Both data receivers and data providers must fully comply with the relevant applicable legislation (GDPR, Data Act, Data Governance etc) and in practice create a trustworthy data sharing framework where each party can share and re-use health data with confidence that no legislation is violated. This data-sharing framework will result in de facto promoting a data-driven economy and allow research centres, public authorities, and healthcare providers to have access to the GATEKEEPER data space and facilitate innovation.

Considering that the European Data Strategy aims at this, although not mandatory under any legislation, a data-sharing certification (or at least a self-assessment tool) would be very useful and enable various stakeholders to trust each other (European Commission, European data strategy - Making the EU a role model for a society empowered by data). The European Commission is currently developing a legislative proposal for a European Health Data Space "*to harness data for better healthcare, better research and better policy making to the benefit of patients*" (European Commission, 2020f). Although the legislative proposal was only published during the project's lifetime and has not yet been approved, it builds upon the Data Governance Act, the Data Act and the GDPR with specific sectoral measures that inter alia will enable access and sharing of health data for healthcare delivery purposes as well as enable access to reuse data for research purposes (European Commission 2022 d).

Therefore, an identification of the qualification requirements of health data sharing in general was considered to be a valuable contribution towards the implementation of such legislative framework and would be the start of a mapping exercise of its interplay with the GDPR, Cybersecurity Act, Data Act, Data Governance Act etc. that could potentially benefit policymakers to better address the challenges and gaps of this proposed legislation.

5.1.3 AI certification gap



	ISO Standards	IEEE Standards	ETSI Standards
AI Act Terminology	✗	✗	✗
Data governance	✓	✓	✓
Risk management system	✓	✓	✗
Technical documentation-Record keeping	✓	✓	✓*
Transparency	✓	✓	✗
Human oversight	✗	✓	✗
Accuracy robustness and cybersecurity	✓	✓	✓
Quality management systems	✓	✓	✓
Tailored to AI-based medical devices	✗	✓	✗
Published as harmonized standards at the OJ- Presumption of conformity	✗	✗	✗

AI Certification Gap

Demand: Certification of AI systems and algorithms, including quality of datasets. Particular focus on medical devices that deploy AI technology.

Figure 38: AI Certification Gap

From the table above, it is evident that at the moment there is no available standard that is tailored to the requirements the AI Act poses and aligns with its terminology. However, key players in the standardisation market have already published some standards that aim to achieve similar goals with the AI Act obligations, and more standards are constantly being developed.

In addition, no certification mechanism that will lead to the mandatory CE marking of conformity exists for now. The major reason for this serious gap is because the AI Act is not yet in force, and the final text was only recently approved (November 2023). Consequently, there is no notified body that has been assigned with the task to conduct the conformity assessments under the AI Act. The current gap in AI certification is also evident considering that no harmonised standard is published yet in the Official Journal of the European Union, thus no presumption of conformity can occur. If one tries to focus on AI certification for medical devices the gap deepens more as at the moment very few standards have or are being developed for such cause.

The above gaps are very important and need to be filled not only because without certification, no high-risk device that deploys AI for medical diagnosis can enter the EU market, but also because as a result this could stifle innovation and delay the data-driven economy the EU aspires to lead globally (European Commission 'European data strategy-Making the Eu a role model for a society empowered by data).

Additionally, as soon as the AI Act enters into force, the demand for AI certification will increase rapidly (as happened with the GDPR) and the AI providers will be ready and willing to pay for such certification (mature market). However, it is foreseeable that administrative hurdles will delay the adoption of such certification by relevant authorities and (Europrivacy, the first GDPR Data Protection Seal was approved five years after the regulation's entry into force).

While GATEKEEPER WP8 has developed an initial set of criteria to address the AIA, focus on this action was not deemed a sensible choice for various reasons: Firstly, the AI Act will not be in force until the GATEKEEPER project ends. This practically means that even if a high-level certification mechanism is proposed, changes in the final AI Act were foreseeable and impeded consensus on the criteria prior to this deadline.

In summary, although demand for an AI certification is realistically foreseeable after the AI Act enters into force, activities on this front were not thought of as a priority action. (see Section 5.2). This being said, the need for a tailored certification that focuses on AI systems used for medical diagnosis continues to be explored by relevant partners in the project in alignment with various SDOs.

5.1.4 Interoperability Certification Gap

The feedback received from the different stakeholders is showing that the following standards from the HL7 standard family should be implemented by the solutions and services to ensure the interoperability with electronic health records (EHRs):

- HL7 FHIR
- HL7 CDA R2.0
- IPS HL7 FHIR Implementation Guide
- IPS HL7 CDA R2.0 Implementation Guide
- IDA HL7 FHIR Implementation Guide
- POCD HL7 FHIR Implementation Guide
- PHD HL7 FHIR Implementation Guide
- HL7 CDS Hooks
- Smart App Launch

This means that the solutions and services using the above set of HL7 international standards should be certified for the interoperability based on their specification. In this section, a gap analysis concerning the interoperability certification is realised, notably by examining existing tools facilitating the interoperability for HL7 standards.

A list of testing tools usable to assess the interoperability of HL7 services or solutions was compiled:

- Inferno ONC Program Edition: https://github.com/onc-healthit/inferno-program
- Inferno Community Edition: https://github.com/onc-healthit/inferno
- FHIR Test Cases: https://github.com/FHIR/fhir-test-cases
- Crucible: https://github.com/fhir-crucible/crucible

The table below illustrates the support of each required HL7 standards by the testing tools:

Table 7: HL7 standards vs testing tools

Standards	**Inferno ONC Program Edition**	**Inferno Community Edition**	**FHIR Test Cases**	**Crucible**

HL7 FHIR	Yes	Yes	Yes	Yes
HL7 CDA R2.0	No	No	No	No
IPS HL7 FHIR Implementation Guide	Yes	Yes	Yes	Yes
IPS HL7 CDA R2.0 Implementation Guide	No	No	No	No
IDA HL7 FHIR Implementation Guide	Yes	Yes	Yes	Yes
POCD HL7 FHIR Implementation Guide	Yes	Yes	Yes	Yes
PHD HL7 FHIR Implementation Guide	Yes	Yes	Yes	Yes
HL7 CDS Hooks	Maybe	Maybe	Maybe	Maybe
Smart App Launch	Yes	Yes	No	Yes

The table reveals that there are no testing tools covering all the different standards and related implementation guides. This means that a combination of different testing tools should be used to cover the most important aspects of the interoperability in HL7 FHIR. It is also possible to create a testing tools suite based on the HL7 FHIR open-source components hosted on GitHub at https://github.com/orgs/HL7/repositories. In this case, the testing tools suite can be customised in function of the use cases and needs of the HL7 solutions to be tested and certified.

The HL7 SDO has a higher-focus on the certification of people working with HL7 standards than on the certification of the products, solutions and services implementing the family of HL7 standards. Indeed, there are currently four kinds of HL7 certifications listed on the official HL7 website at https://www.hl7.org/certification/:

- HL7 Version 2 certification: This certification is intended for the people interested in the chapter "Control" of the HL7 Version 2 standard. So, this certification requires strong knowledge of HL7 Version 2 specifications, the related implementation guides, the messages, their formats and their contents.
- HL7 Version 3 certification: This certification requires the expertise and proficiency on the HL7 Reference Information Model (RIM).
- HL7 Clinical Document Architecture (CDA): This certification is given to people using clinical documents based on CDA, typically health information on patients. It

requires strong knowledge of the CDA specification and the implementation guides.

- HL7 FHIR Proficiency Certification: This certification is the combination of the three previous certifications. Different aspects of HL7 FHIR need to be clearly understood by the certification candidates: FHIR concepts and principles, FHIR exchanges, FHIR conformance and implementation, the security, the maintenance and finally, the licensing.

Additional information on interoperability and trust can be found in section 6.1 and in the relevant deliverables of WP4.

5.2 Options and Priority Identification

Considering the current gaps, stakeholder interests, and the alternative solutions that are under development, the figure below summarizes the main options (priority actions) considered during the GATEKEEPER project to bring value to upcoming digital health platforms that will be developed within the EU.

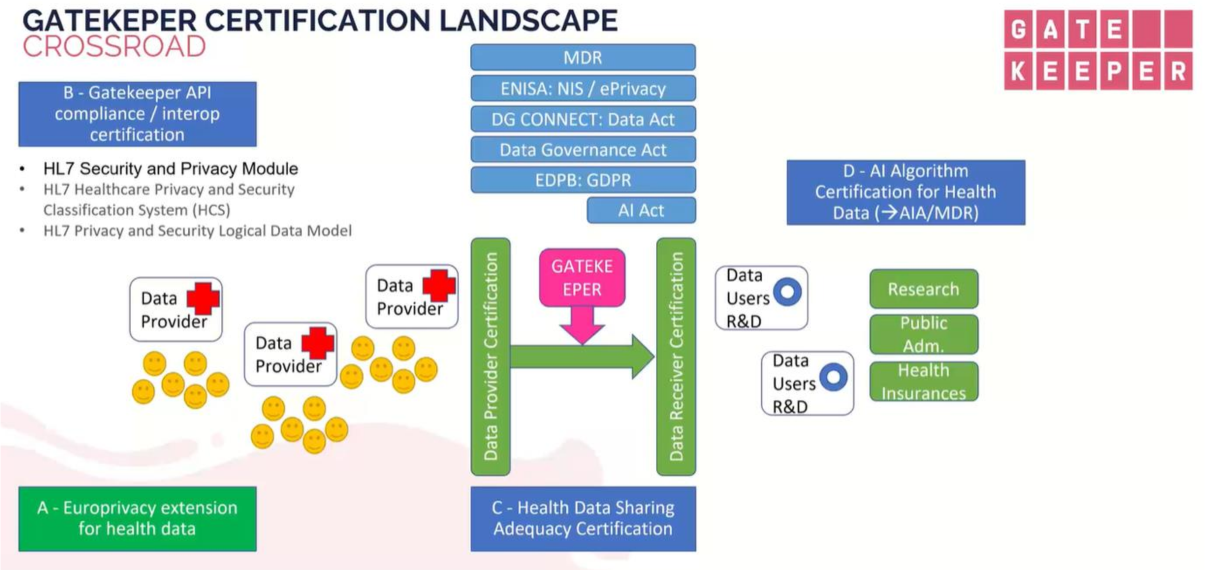

GATEKEPER CERTIFICATION LANDSCAPE
CROSSROAD
GATE KEEPER
B - Gatekeeper API compliance / interop certification
HL7 Security and Privacy Module
HL7 Healthcare Privacy and Security Classification System (HCS)
HL7 Privacy and Security Logical Data Model
MDR
ENISA: NIS / ePrivacy
DG CONNECT: Data Act
Data Governance Act
EDPB: GDPR
AI Act
D - AI Algorithm Certification for Health Data (→AIA/MDR)
Data Provider
Data Provider
Data Provider
Data Provider Certification
GATEKEEPER
Data Receiver Certification
Data Users R&D
Data Users R&D
Research
Public Adm.
Health Insurances
A - Europrivacy extension for health data
C - Health Data Sharing Adequacy Certification

Figure 39: GATEKEEPER: Certification landscape

As all identified work avenues managed to address demand/offer gaps and overall priorities, additional effort was necessary to evaluate priority actions considering technical/organizational limitations associated to the time constraints of the GATEKEEPER project and their short to mid-term feasibility.

This is the case for option B, where an examination was performed considering WP4 activities (see Chapter 6) on interoperability and the GATEKEEPER trust authority (See D2.8). In their work, WP4 and associated tasks provided a robust technical solution which covers most of the project needs on the subject of technical certification and trust generation, and their concluding recommendations provided further arguments to support the need for strengthening ethical and legal opportunities for data sharing (best addressed options A and C in Figure 38). In the case of option D, the pace of EU legal framework development (where the final text of the Act was only approved in November 2023) meant that while a draft of the criteria for an AI certification was proposed for consideration to ECCP (See Section 7.3), no consensus has been reached yet regarding their viability.

For these reasons, GATEKEEPER T8.3 identified options A and C as priority actions to be addressed, as the demand was proven to exist and the main regulatory requirements are relatively stable. For both these options, the EDPB's approval of the Europrivacy certification scheme (including GATEKEEPER e-health criteria) has been fundamental, as it ensured viability of the proposed approach and provided a baseline scheme model and requirement framework for its adaptation towards health data and innovative technologies. Work performed on these options and associated CRS developments is reported in Chapter 7.

6 Interoperability and Trust Report

6.1 Interoperability

In the context of the GATEKEEPER project's activities, HL7 released a GATEKEEPER Implementation Guide, which is an important development in the field of health data interoperability. This guide is designed to facilitate the use of HL7 standards, specifically within the scope of the GATEKEEPER project, by providing detailed mappings and specifications for various HL7 resources.

One of the key aspects of the GK FHIR IG is the detailed description of the `Practitioner` resource profile. This profile includes mappings for different data elements within the HL7 framework, ensuring that the practitioner's information is accurately and consistently represented across different systems. These mappings cover various attributes like identifier, name, telecom, address, gender, birth date, qualifications, and communication preferences, among others. The guide also includes terminological bindings to ensure consistency in the representation of languages, names, gender, qualifications, and communications.

In addition to the Implementation Guide, HL7 offers a notable certification output of relevance to the GATEKEEPER project. Indeed, a professional certification, designed to acknowledge individuals who have demonstrated their expertise and proficiency in using HL7 standards, is recommended for the developers using the FHIR standard in their new products and solutions. The list of professional certifications offered by HL7 is also available in the section 5.1.4 "Interoperability Certification Gap" of this document.

Towards the implementation of HL7 FHIR (Fast Healthcare Interoperability Resources) testing for products or solutions, two steps are basically needed (and could potentially be of relevance to an eventual certification):

1. A test specification which is formulated by a test script following the guidelines and principles of HL7 FHIR.
2. A test report with a structure defined by the HL7 FHIR specification. The test report provides all the information collected after the execution of the test script. It permits to the developers to determine if their initial implementation is correct towards the HL7 FHIR standards.

The HL7 FHIR specification follows a modular approach, meaning that HL7 FHIR components can be added or removed in function of the needs and predefined use cases of the final end-users, the test scripts can be specifically written to ensure the compliance and the interoperability inside a specific medical FHIR infrastructure.

This chapter discusses how to create scripts specifying the tests to be executed in a FHIR environment. These scripts can be used for the certification of FHIR products or solutions and were integrated on WP4 activities and as part of the Gatekeeper FHIR Implementation Guide.

6.1.1 Interoperability test specification

Scripts specifying the tests are intended to be executed against the implementation of FHIR servers and clients. They are part of the quality reporting and testing provided by the FHIR Implementation Support Module to the developers working on FHIR compliant solutions. The Implementation Support Module contains the specific documentation for the FHIR implementers, tools easing the implementation and reference implementations under the form of libraries. Furthermore, reference servers are also available for the developers and testers of FHIR clients. Some links to the FHIR community channels are also published.

The test scripts are usually composed by four parties or sections:

1. A list of resources used in the tests.
2. The procedures to set up the tests.
3. The tests suite to be executed.
4. The procedures undertaken after the execution of tests.

The test scripts permit to the developers to validate workflows in the different use cases, to determine the compliance of servers and clients to the FHIR specification and to assess that several FHIR implementations are compatible and interoperable. Different elements can be evaluated through the test scripts such as the operations realised by the servers, the exchange of datasets between FHIR components, the requests and the corresponding answers. At the end of the day, the test scripts should verify the correct behaviour of an implementation based on the FHIR specification.

The methodology accompanying the FHIR test scripts should improve the interoperability among FHIR applications implemented through servers and clients. The interactions between the servers and the clients are realised by RESTful APIs. The formats of the data exchanged through the RESTful APIs during the tests are XML or JSON, with the corresponding MIME types "application/fhir+xml" or "application/fhir+json". The test scripts are themselves written in XML or JSON or Turtle. Terse RDF Triple Language, shorten to Turtle, is a file format used in the context of Resource Description Framework (RDF) and represents the data as semantic triples. For information, a semantic triple is composed by a subject, a predicate and an object. Test scripts encompass assertions whose results give the final outcome of a test as failed or succeed. For instance, the assertions allow the testing of HTTP error codes beginning by 4xx or 5xx.

The following table presents all the properties to be incorporated in a FHIR test script. More detailed information about the content of the test scripts can be found at https://build.fhir.org/testscript.html. Some examples of test scripts are available at https://build.fhir.org/testscript-examples.html.

Table 8: Test script properties

Name	Description
url	Global unique URI (Uniform Resource Identifier) of the test script.
identifier	Additional identifier of the test script.
version	Version of the test script.
name	Machine-readable name of the test script.
title	Human-readable name of the test script.
status	Status of the test script. Possible values: • Draft • Active • Retired

	- Unknown
experimental	Boolean value signifying that the test script was written for testing purposes.
date	Date when the last change was made in the test script
publisher	Name of the author of the test script. It can be a person or an organisation.
contact	Contact details of the author of the test script.
description	Description of the test script.
useContext	For which context the test script was written.
jurisdiction	Optional jurisdiction for which the test script was made. The jurisdiction can encompass the ISO 3166 code for a country or for a country subdivision or for a region.
purpose	Objective of the test script.
copyright	Restrictions for the publication and/or the utilisation of the test script.
origin	Sender of a message. The origin is composed by the two following attributes: • index: Index of the sender, starting at 1. • profile: Two possible values: FHIR-Client or FHIR-SDC-FormFiller. The FHIR-SDC-FormFiller is a FHIR client acting as a Structured Data Capture Form Filler.
destination	Receiver of a message. The destination is composed by two attributes: • index: index of the receiver, starting at 1. • profile: Four values are possible: ○ FHIR-Server ○ FHIR-SDC-FormManager ○ FHIR-SDC-FormReceiver ○ FHIR-SDC-FormProcessor.
metadata	Describe the capability of the FHIR server to assess. The metadata contain a “link” attribute and a “capacity” attribute. The “link“ attribute is composed by a URL to the specification and by a description. The “capability” attribute is formed by the following elements: • required: Boolean value meaning if the capability is mandatory.

	• validated: Boolean value signifying if the capability is validated. • Description: Description of the capability. • origin: Index of the origin server. • Destination: Index of the destination server. • link: Link to the FHIR specification. • capabilities: Description of the application or component.
scope	Information on the artifact to be tested by the script. Three attributes are available: • artifact: The artifact itself. • conformance: Three values are possible: required, optional or strict. • phase: Phase of development, three values available: unit, integration or production.
fixture	Resource used by the test script. This property has got three attributes: • autocreate: Boolean value meaning whether the resource is automatically created during the setup phase of the test. • Autodelete: Boolean value signifying whether the resource is automatically erased at the end of the test. • resource: Reference to the resource under the form of a URI.
profile	Reference to the validation profile
variable	Placeholder for the elements to be evaluated. A variable contains these attributes: • name: Name of the variable. • defaultValue: Default value of the variable. • description: Description of the variable. • expression: Expression of the variable in the FHIRPath language. • headerField: Name of the HTTP header field. • hint: Indication for the default value of the variable. • Path: Path expressed with the XPath language (for XML) or with the JSONPath language (for JSON). • sourceId: Reference or identifier to the resource.

setup	Operations to be undertaken before the start of the test. This property is composed by an attribute named "action". An action is in fact an operation; indeed, the attribute "action" is composed by: • operation: Operation performed before the beginning of the test. More information available in the table "Details of operation". • assert: Assertion to be done for the above operation. More information available in the table "Details of assert".
test	The test to be executed by the script. It is composed by: • name: Name of the test. • description: Description of the test. • action: Operation to be made in the test. The attribute "action" basically contains: o operation: The operation of the test. More information available in the table "Details of operation". o assert: The assertion of the test. More information available in the table "Details of assert".
teardown	The operations to be realised after the conclusion of a test. This property is composed by the "action" attribute which contains itself the "operation" attribute. More information on the "operation" attribute available in the table "Details of operation".

The following table explains the "operation" attribute:

Table 9: Details of operation

Name	**Description**
type	Type of the operation, defined in an operation code.
resource	Type of the resource, expressed in a URI.
label	Label of the operation.
description	Description of the operation.
accept	MIME type for the acceptation, including the charset.
contentType	MIME type for the content, including the charset.
destination	Index of the server answering to the request.
encodeRequestUrl	Boolean value meaning whether the URL of the request is encoded or not.
method	HTTP methods. Possible values are delete, get, options, patch, post, put and head.

origin	The index of the server sending the request.
params	The parameters included in the request path.
requestHeader	HTTP header. A HTTP header is composed of course by: • field: Name of the HTTP header. • value: Value of the HTTP header.
requestId	Identifier of the resource doing the request.
responseId	Identifier of the resource answering.
sourceId	Identifier of the resource doing HTTP PUT and POST requests.
targetId	Identifier of the resource making http GET requests.
url	The URL of the request.

The following table presents the details of the “assert” attribute:

Table 10: Details of assert

Name	**Description**
label	Label of the assertion.
description	Description of the assertion.
direction	Request or answer, so two values possible: request or response.
compareToSourceId	Identifier of the resource to be evaluated.
compareToSourceExpression	Expression in the FHIRPath language to be evaluated against the resource.
compareToSourcePath	Expression in the XPath language (for XML) or in the JSONPath language (for JSON) to be evaluated against the resource.
contentType	MIME type to be compared with the HTTP “Content-Type” header.
expression	Expression in the FHIRPath language.
headerField	Name of the HTTP header field.
minimumId	Identifier of the resource providing the minimum content.
navigationLinks	Boolean value indicating if a validation of the navigation links is necessary or not.

operator	A code representing an operator. The possible values are equals, notEquals, in, notIn, greaterThan, lessThan, empty, notEmpty, contains, notContains and eval.
path	Expression in the XPath language or in the JSONPath language.
requestMethod	HTTP methods. The possible values are delete, get, options, patch, post, put and head.
requestURL	The URL of the request to be compared.
resource	Type of the resource.
response	Code of the response. The possible values are okay, created, noContent, notModified, bad, forbidden, notFound, methodNotAllowed, conflict, gone, preconditionFailed and unprocessable.
responseCode	HTTP response code to be compared.
sourceId	Identifier of the resource.
stopTestOnFail	Boolean value indicating whether the execution of the test is immediately stopped when an assertion is failing.
validateProfileId	Identifier of the validation profile.
value	Value to be compared.
warningOnly	Boolean value indicating whether the assertion is creating only a warning in case of an error.

6.1.2 Interoperability test report

This section describes the test reports compiled after the execution of tests using the FHIR test scripts presented in the previous chapter. Basically, a FHIR test report is summarising the results of a FHIR test script which the execution has finished. In consequence, the test report is defined based on the test script and can be generated in three different formats: XML, JSON and Turtle, like the test script.

The test report encompasses three sections:

- Setup: Operations done before the start of the test suite.
- Tests: The tests themselves, executed automatically by the test script.
- Teardown: The final operations undertaken when all the tests have finished.

Each section lists the actions, namely the operations and the assertions, realised during the execution of a whole test script.

The results are expressed through result codes which are defined as:

- Pass
- Skip
- Fail

- Warning
- Error

The structure of a test report is presented in the following table with all the possible properties and related attributes:

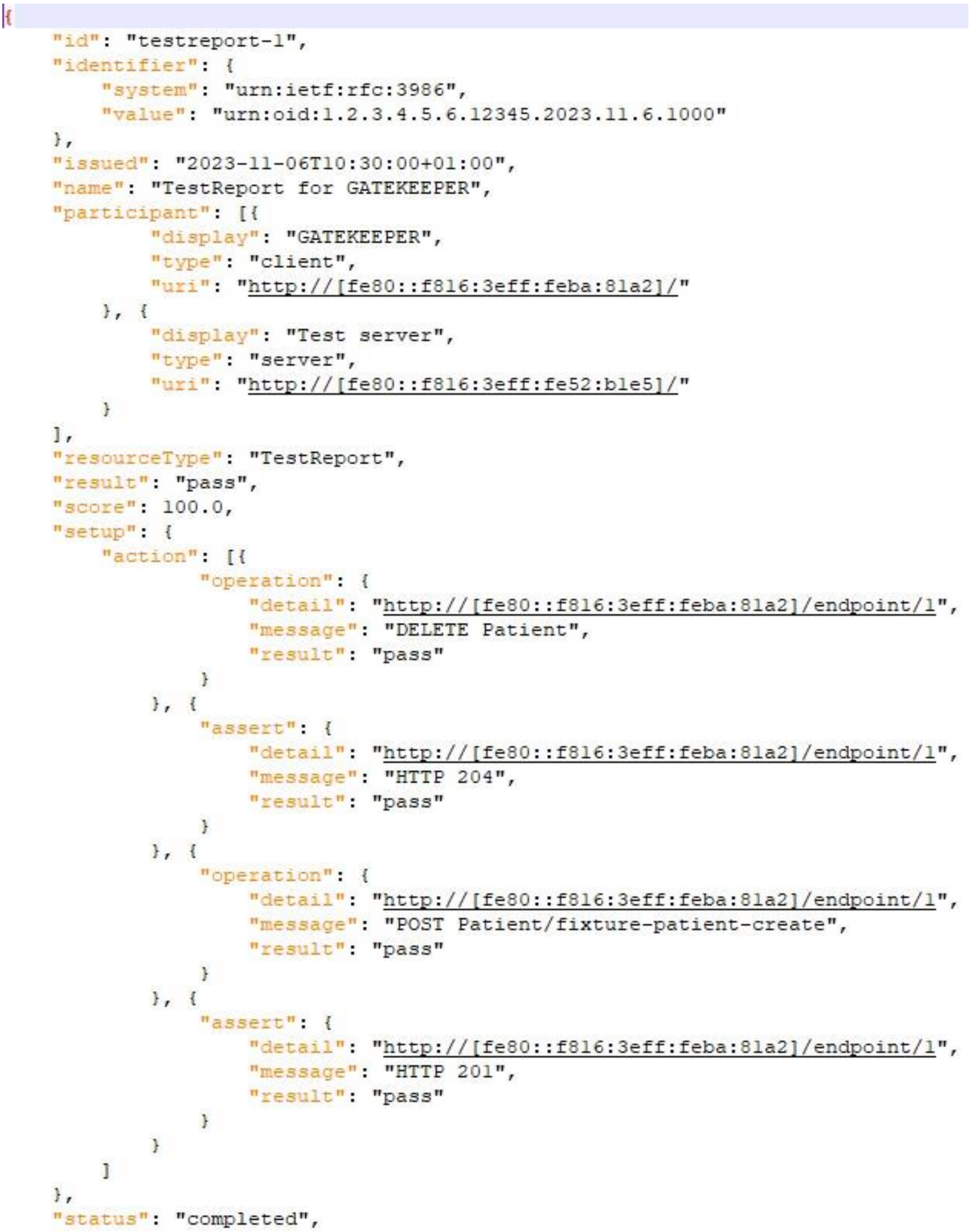
Table 11: Test report properties

Name	**Description**
identifier	Identifier of the test report.
name	Name of the test report.
status	Status of the test report. The following values are possible: • completed • in-progress • waiting • stopped • entered-in-error
testScript	URL of the test script for which the test script is reporting the results.
result	The final result of the test. Three values possible: • pass • fail • pending
score	Score corresponding to the percentage of passed tests.
tester	Name of the author of the test report. The author can be a person or an organisation.
issued	Date when the test script was executed and the corresponding test report generated.
participant	Component participating to the execution of a test. There are three attributes: • type: The type of participant which can have one of these values: test-engine, client or server. • uri: The URI/URL of the participant. • display: Name of the participant to be displayed.
setup	The results of the operations made during the setup of the tests. A setup is composed by an action at least. For each action, there are an operation and an assert. The "operation" attribute and the "assert" attribute are both composed by:

	• result: The result of the operation or assertion. The possible values are pass, skip, fail, warning and error. • message: A message or comment related to the result. • detail: Link to the details of the result.
test	Test from the test script. It is composed by the following attributes: • name: Name of the test. • description: Description of the test. • action: Action which is an operation or an assert. More details on operation and assertion can be found in the corresponding tables previously mentioned in this document.
teardown	Results concerning the operations realised at the end of the tests. An "action" attribute is present at least, with an operation performed at least.

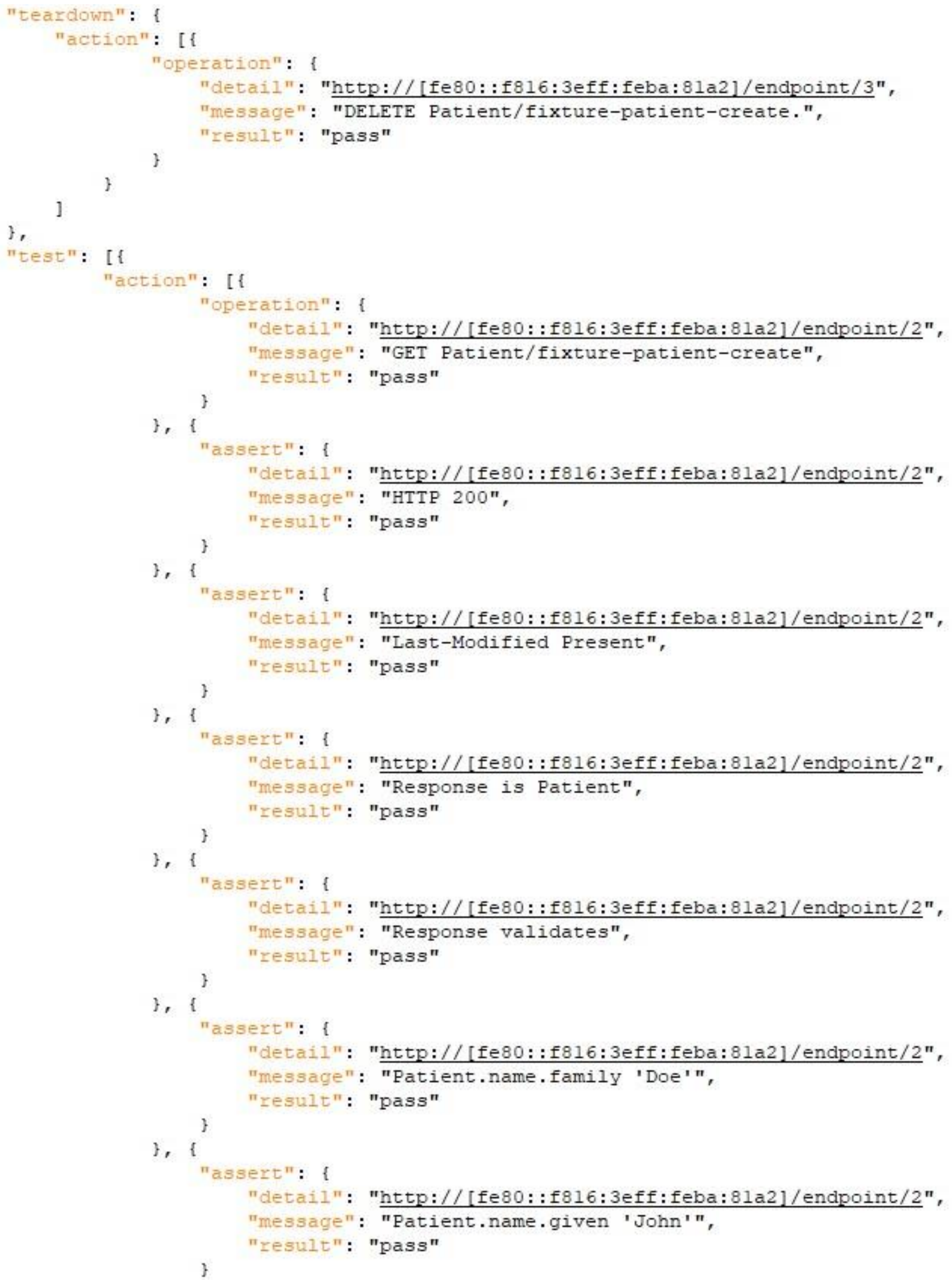
More detailed information concerning the test reports is available online at https://build.fhir.org/testreport.html.

The following figures shows an example of a test report using the JSON format:



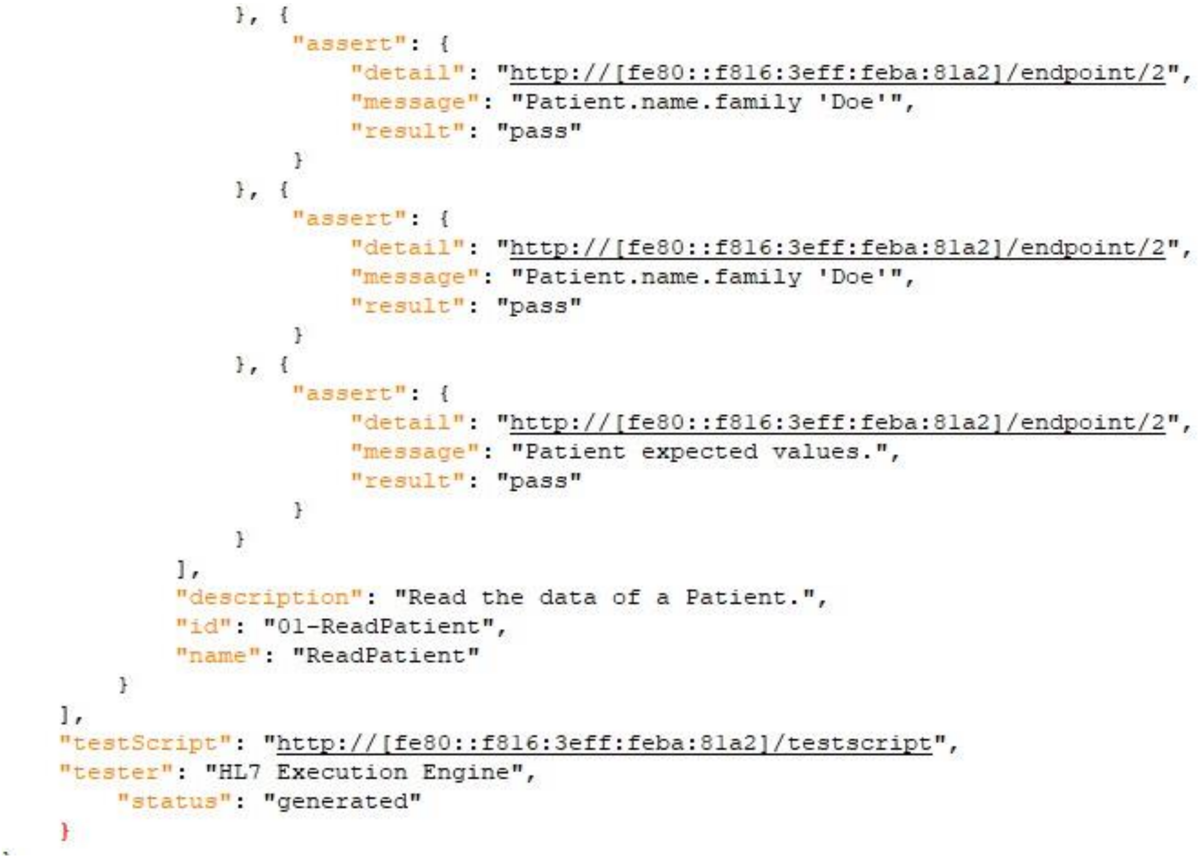
```
{
    "id": "testreport-1",
    "identifier": {
        "system": "urn:ietf:rfc:3986",
        "value": "urn:oid:1.2.3.4.5.6.12345.2023.11.6.1000"
    },
    "issued": "2023-11-06T10:30:00+01:00",
    "name": "TestReport for GATEKEEPER",
    "participant": [{
                "display": "GATEKEEPER",
                "type": "client",
                "uri": "http://[fe80::f816:3eff:feba:81a2]/"
        }, {
                "display": "Test server",
                "type": "server",
                "uri": "http://[fe80::f816:3eff:fe52:b1e5]/"
        }
    ],
    "resourceType": "TestReport",
    "result": "pass",
    "score": 100.0,
    "setup": {
        "action": [{
                "operation": {
                    "detail": "http://[fe80::f816:3eff:feba:81a2]/endpoint/1",
                    "message": "DELETE Patient",
                    "result": "pass"
                }
            }, {
                "assert": {
                    "detail": "http://[fe80::f816:3eff:feba:81a2]/endpoint/1",
                    "message": "HTTP 204",
                    "result": "pass"
                }
            }, {
                "operation": {
                    "detail": "http://[fe80::f816:3eff:feba:81a2]/endpoint/1",
                    "message": "POST Patient/fixture-patient-create",
                    "result": "pass"
                }
            }, {
                "assert": {
                    "detail": "http://[fe80::f816:3eff:feba:81a2]/endpoint/1",
                    "message": "HTTP 201",
                    "result": "pass"
                }
            }
        ]
    },
    "status": "completed",
```

Figure 40 Test report part 1



```
"teardown": {
    "action": [{
            "operation": {
                "detail": "http://[fe80::f816:3eff:feba:81a2]/endpoint/3",
                "message": "DELETE Patient/fixture-patient-create.",
                "result": "pass"
            }
        }
    ]
},
"test": [{
        "action": [{
                "operation": {
                    "detail": "http://[fe80::f816:3eff:feba:81a2]/endpoint/2",
                    "message": "GET Patient/fixture-patient-create",
                    "result": "pass"
                }
            }, {
                "assert": {
                    "detail": "http://[fe80::f816:3eff:feba:81a2]/endpoint/2",
                    "message": "HTTP 200",
                    "result": "pass"
                }
            }, {
                "assert": {
                    "detail": "http://[fe80::f816:3eff:feba:81a2]/endpoint/2",
                    "message": "Last-Modified Present",
                    "result": "pass"
                }
            }, {
                "assert": {
                    "detail": "http://[fe80::f816:3eff:feba:81a2]/endpoint/2",
                    "message": "Response is Patient",
                    "result": "pass"
                }
            }, {
                "assert": {
                    "detail": "http://[fe80::f816:3eff:feba:81a2]/endpoint/2",
                    "message": "Response validates",
                    "result": "pass"
                }
            }, {
                "assert": {
                    "detail": "http://[fe80::f816:3eff:feba:81a2]/endpoint/2",
                    "message": "Patient.name.family 'Doe'",
                    "result": "pass"
                }
            }, {
                "assert": {
                    "detail": "http://[fe80::f816:3eff:feba:81a2]/endpoint/2",
                    "message": "Patient.name.given 'John'",
                    "result": "pass"
                }
```

Figure 41 Test report part 2



```
                }, {
                    "assert": {
                        "detail": "http://[fe80::f816:3eff:feba:81a2]/endpoint/2",
                        "message": "Patient.name.family 'Doe'",
                        "result": "pass"
                    }
                }, {
                    "assert": {
                        "detail": "http://[fe80::f816:3eff:feba:81a2]/endpoint/2",
                        "message": "Patient.name.family 'Doe'",
                        "result": "pass"
                    }
                }, {
                    "assert": {
                        "detail": "http://[fe80::f816:3eff:feba:81a2]/endpoint/2",
                        "message": "Patient expected values.",
                        "result": "pass"
                    }
                }
            ],
            "description": "Read the data of a Patient.",
            "id": "01-ReadPatient",
            "name": "ReadPatient"
        }
    ],
    "testScript": "http://[fe80::f816:3eff:feba:81a2]/testscript",
    "tester": "HL7 Execution Engine",
        "status": "generated"
    }
```

Figure 42 Test report part 3

The test reports are particularly useful for the developers who are creating solutions and products based on the family of HL7 FHIR standards, because they can identify and correct errors quickly. The conformance and the interoperability are important to ensure the good integration of new software in an ecosystem based on FHIR.

6.2 Trust

Since the project's initial phases, WP4 was notably providing a microservice usable by the other components of the GATEKEEPER platform which serves as a certification authority. Indeed, this service offers a whole process to validate the data generated by the devices (Things) deployed in the different pilots against predefined standards. The validation process returns a validation score which is used to generate a certificate for each Thing. This microservice named Thing Validation and Certification utilises a Hyperledger Fabric blockchain network deployed by the different organisations of the project consortium. The access to this blockchain network is limited to the participants identified through a Public Key Infrastructure (PKI). Through the blockchain network, it is possible to retrieve the certificate given to a Thing.

The components linked to the GATEKEEPER trust and certification authority were improved in an iterative way, particularly during the second part of the project. Now, the Things Validation System, as known as Validator, is collecting the different files used for the validation. Two categories of files can be uploaded through this component: data, mainly JSON files, and legal documents. For data, two standards are considered and employed for the validation: FHIR and W3C WoT. For the legal aspect of the validation, the GDPR, the MDR (Medical Device Regulation) and other guidelines and standards are used in the process. Concerning the validation of data, the process is automated; on the other hand, the validation for the legal part is made semi-manually through a Graphical User Interface (GUI). Independently of the types of validations, this component generates a validation score and sends it to the Things Certification component.

For each Thing, a certificate based on the validation score is generated and stored in the blockchain: this is the role of the Things Certification component. The next component linked to the trust and certification authority is the Things Action Tracking which is responsible for logging all the actions made by the different categories of users on the Things. This component allows the auditing of the GATEKEEPER platform.

More information about the GATEKEEPER trust and certification authority and the related components can be found in the following deliverables:

- D4.5 Gatekeeper Trust Authority: which provides the initial definition of the trust authority and it's goals.
- D4.14 Gatekeeper Trust Authority v2 (confidential): This deliverable presents the different components involved in the GATEKEEPER trust authority and certification and their instantiations in the development and production environments of GATEKEEPER.
- D2.8 Trust Authority Report (confidential): presents the results of the usage of the GATEKEEPER Trust Authority and the recommendations to be applied to the components of the GATEKEEPER Trust Authority, notably the usage policies. This report emphasis the compliance with ethical and regulatory requirements to be ensure in the whole GATEKEEPER solution.

6.3 Interoperability and trust: key outtakes

Based on the analysis and the work undertaken in the task related to the certification and reported in this deliverable, a combination of different elements existing in the whole GATEKEEPER platform ensures the technical conformance and interoperability, mainly for the family of HL7 FHIR standards.

Indeed, HL7 is more focused on the certification of technical capabilities of individuals, namely the developers and engineers involved in the conception, the development and the implementation of a large panel of products and solutions based on HL7 FHIR standards. This means these qualified people are aware of the different aspects linked to the HL7 conformance and interoperability. They should also follow the implementation guides provided by HL7, in particular the one dedicated to the GATEKEEPER project. In fact, the compliance, the conformance and the interoperability are linked together in the HL7 FHIR standards. Indeed, the interoperability is realised through the implementation of the HL7 standards and specifications to ensure the communication between different healthcare systems.

Firstly, each component of a such healthcare system is tested independently to guarantee its compliance to HL7 FHIR standards and indirectly, underlying regulations for the legal compliance, The next step in the whole testing process is to realise the interoperability tests with two components which are declared conform to the HL7 FHIR standards. These tests are covering in fact several layers, from the communication layer to the application layer. The interoperability and the conformance are evaluated through the test scripts and reports.

These testing principles were applied in the development of the GATEKEEPER components deployed in the GATEKEEPER Trust Authority. Indeed, the data generated by the different components are tested and validated against the selected standards, namely HL7 standards and W3C IoT.

In this context, a complex technical certification of FHIR is not so relevant, considering the organisational burden of a certification and the fact that a such technical certification is somehow reinventing the wheel already put in place in the GATEKEEPER Trust Authority. This being said, the notion of certification (particularly technical compliance certification) was implemented in the work done in the GATEKEEPER Trust Authority, using a blockchain to ensure the immutability of a certification given to a particular device or Thing.

The deliverables associated with this task (including Section 6.1 of this deliverable) also demonstrated what a sufficient number of tools are available through HL7 and GATEKEEPER to test the conformance and the interoperability without the limitations encountered by a rather complex and formalistic process of a technical/organizational interoperability certification. Furthermore, the implementation of the GATEKEEPER Trust Authority managing not only the technical aspects of the interoperability, but also the legal compliance, was deemed to be more useful and relevant to the GATEKEEPER project's immediate needs than an interoperability certification.

The GATEKEEPER Trust Authority has demonstrated its usefulness compared to the needs and expectations formulated at the beginning of the project, mainly by the tests and validations undertaken by the GTA components for the data generated by the Things (see Deliverables 4.5, 4.14 and 2.8).

In conclusion, initial testing performed by WP4 shows the viability of the GATEKEEPER Trust Authority as a technical conformance and interoperability testing solution which meets stakeholder inputs regarding interoperability-oriented CRS. This being considered, WP8 activities WP8 on this area were limited to avoid activity duplication and focused instead on the generation of contributions to regulatory compliance certification and CRS to address the trust-generation requirements identified by WP4 and the recommendation on the subject found in D2.8, namely:

*“**RECOMMENDATION 1**: It is advised to complement the development of the technical basis for the secondary use of health data (done by CERTH) with the creation of a solid ethical and legal basis, if data sharing is the agreed goal of all concerned parties. Such ethical and legal basis is indispensable for an actual and meaningful use of the GTA.*

Regulations in Europe increasingly require health and care institutions to enable the secondary use of health data. In parallel, however, ethical concerns arise and ethics protocols in GK, but also more in general, do therefore often not align with this move in data sharing regulations as different countries and ethics committees have different interpretations of the GDPR and for example how to deal with ‘anonymization’. In addition to any further technological development of the GTA, we therefore advise to invest time and effort in addressing this complex issue of the secondary use of health data.” (Source: Gatekeeper D2.7, p27).

The contents of this recommendation were particularly considered by WP8 T8.3 and led to the development of relevant CRS as reported in the following sections (particularly 7.1.1 and 7.2.1).

7 Regulatory Compliance Report

7.1 Personal data protection CRS development

As specified in section 5.2, work done with regards to personal data protection commenced through the integration of the project's results and research into the overall framework of the Europrivacy certification and contributed to its approval as the firs EU Data Protection Seal. Additionally, a specific CRS, the unilateral contractually binding registered commitment tool was researched.

7.1.1 Europrivacy Certification Extensions

As mentioned in section 4.1.2 and depicted in the following image, the Europrivacy GDPR certification scheme is comprised of several groups of criteria and controls:

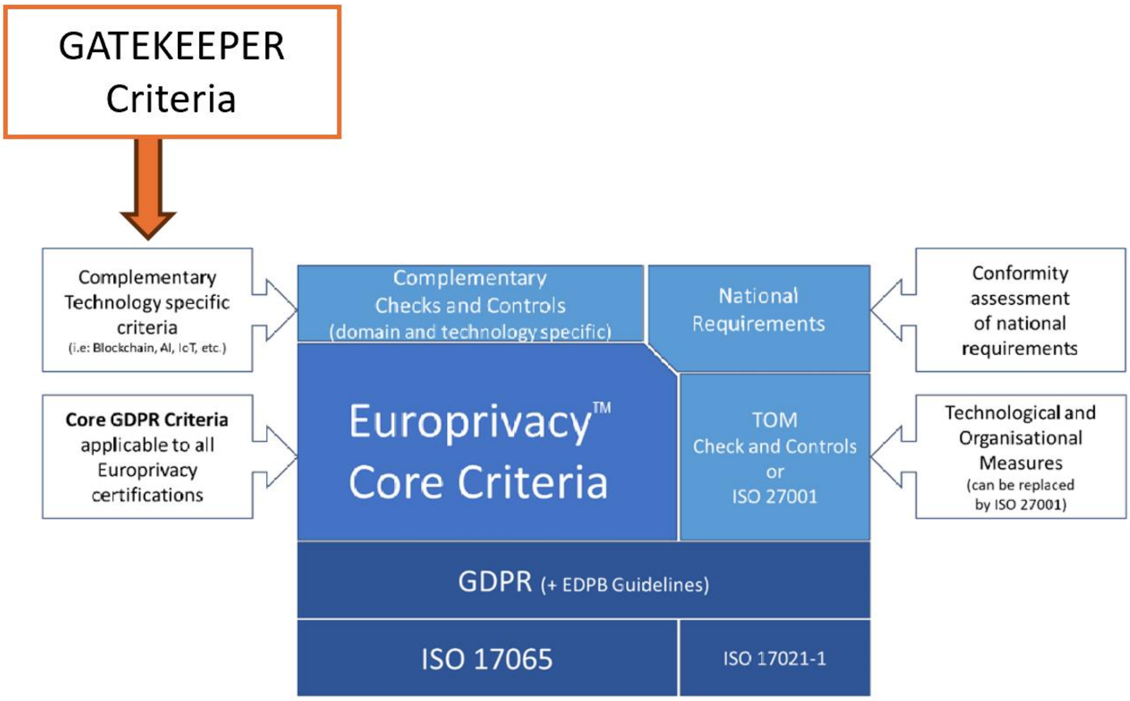

GATEKEEPER Criteria
Complementary Technology specific criteria (i.e: Blockchain, AI, IoT, etc.)
Core GDPR Criteria applicable to all Europrivacy certifications
Complementary Checks and Controls (domain and technology specific)
National Requirements
Europrivacy™ Core Criteria
TOM Check and Controls or ISO 27001
Conformity assessment of national requirements
Technological and Organisational Measures (can be replaced by ISO 27001)
GDPR (+ EDPB Guidelines)
ISO 17065
ISO 17021-1

Figure 43: Mapping of Europrivacy Requirements and GATEKEEPER contributions

These include:

- Core GDPR Criteria: These are the essential criteria applicable to all Europrivacy certifications, ensuring the foundation of the certification is aligned with GDPR principles. These criteria are fundamentally based on the GDPR dispositions and consider also the relevant guidelines defined by the European Data Protection Board. These are operationalized by the certification scheme, which is based fundamentally on ISO 17065: An international standard for bodies certifying products, processes, and services (but, in some cases can also be extended to consider ISO 17021-1: A standard that outlines requirements for bodies providing audit and certification of management systems.)
- National Requirements: Recognizing that individual countries may have additional or varying data protection requirements that need to be met.

- TOM Check and Controls or ISO 27001: TOM refers to Technical and Organizational Measures, ensuring that both the technology and the organization's policies adhere to security standards. ISO 27001 is a widely recognized standard for information security management systems.
- Complementary Technology-specific Criteria: This involves additional requirements that pertain to specific technologies like blockchain, artificial intelligence (AI), Internet of Things (IoT), etc.

As part of the activities carried out by the GATEKEEPER project, and in preparation for the definition of the potential Health Data Sharing Certification mentioned in section 7.2.3, the project generated a set of complementary criteria for e-health which were submitted to the European Centre for Certification and Privacy for consideration. Upon their validation and adoption as part of the Scheme's Contextual Checks and Controls, they were submitted for evaluation by the Luxembourgish Data Protection authority and the European Data Protection Board. In October 2022, the scheme (including the aforementioned criteria) was officially adopted by the EDPB as the first European Data Protection Seal under the GDPR.

Following this development, all consortium partners were granted access to the Europrivacy Academy (academy.europrivacy.org) by ECCP. The training resources found therein focus on the implementation of the Europrivacy scheme, (incorporating of course the use of contextual criteria developed within the project).

The Europrivacy criteria for health data enables the scheme to cover most personal data processing activities that might take place within the GATEKEEPER framework, with a particular focus on processing special categories of data (with the exception of genetic data as requested by EDPB).

In addition to this work, a series of dedicated extensions for additional checks and controls that could be necessary in the context of GATEKEEPER was prepared and submitted to ECCP for consideration (alongside the health data sharing certification and self-assessment solution detailed in Section 7.2). These include:

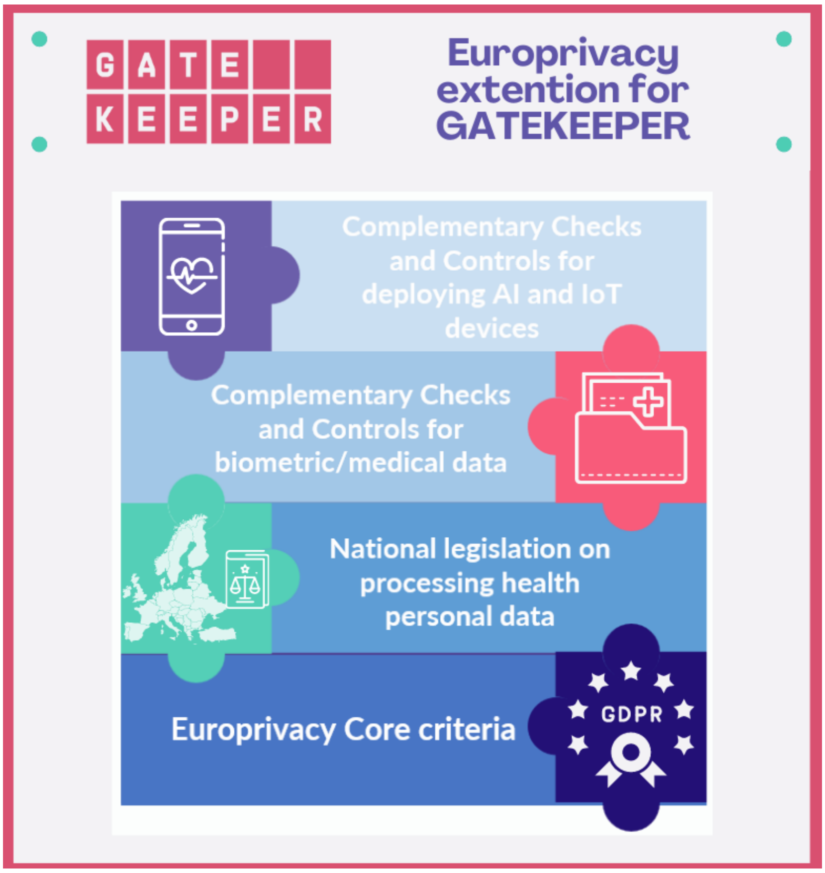
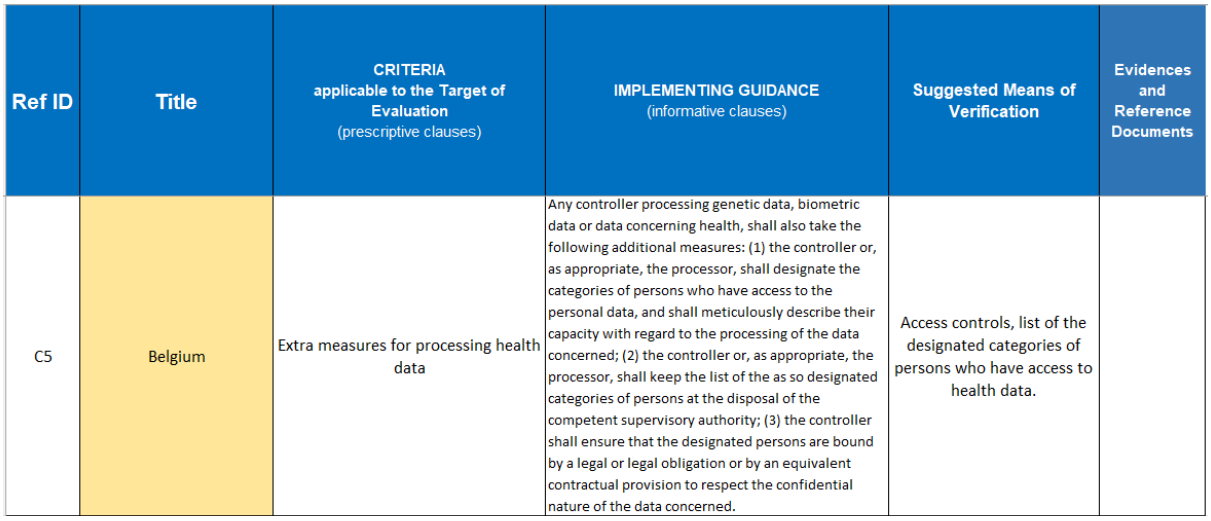

GATEKEEPER
Europrivacy extention for GATEKEEPER
Complementary Checks and Controls for deploying AI and IoT devices
Complementary Checks and Controls for biometric/medical data
National legislation on processing health personal data
Europrivacy Core criteria
GDPR

Figure 44: Europrivacy extension for GATEKEEPER -overview

The proposed extensions include also the nationally specified requirements for processing health data, which was originally identified by WP1 to ensure GATEKEEPER pilot compliance with the applicable legislation each time. A sample of the above extension is shown in the following figure:



Ref ID	Title	CRITERIA applicable to the Target of Evaluation (prescriptive clauses)	IMPLEMENTING GUIDANCE (informative clauses)	Suggested Means of Verification	Evidences and Reference Documents
C5	Belgium	Extra measures for processing health data	Any controller processing genetic data, biometric data or data concerning health, shall also take the following additional measures: (1) the controller or, as appropriate, the processor, shall designate the categories of persons who have access to the personal data, and shall meticulously describe their capacity with regard to the processing of the data concerned; (2) the controller or, as appropriate, the processor, shall keep the list of the as so designated categories of persons at the disposal of the competent supervisory authority; (3) the controller shall ensure that the designated persons are bound by a legal or legal obligation or by an equivalent contractual provision to respect the confidential nature of the data concerned.	Access controls, list of the designated categories of persons who have access to health data.	

Figure 45: Sample of Europrivacy extension on national legislation on processing health data

7.1.2 Unilateral Contractually Binding Registered Commitment Tool

According to the GDPR, written Agreements are frequently required, either to define the relationship between a data controller and a data processor or to share data with other parties. Such requirements may be easily tackled in business environments, however in research projects, especially large-scale research projects such as GATEKEEPER, traditional agreement instruments are not flexible enough to capture the complex relationships that may arise thereof. To address these needs, a different approach was developed in the context of GATEKEEPER, namely the Unilateral Contractually Binding Registered Commitment Tool.

The Unilateral Contractually Binding Registered Commitment Tool takes the form of a formal contract that satisfies formal and regulatory requirements despite its non-traditional unilateral nature, including a clear description of the beneficiaries, the obligations, as well as a mechanism to enter the contract and to exit the contract, including a clear starting date.

As such, it contains clear and explicit dispositions to produce legally binding obligations for the signatory party without the need to enter and negotiate complex bilateral or multilateral contracts. On the contrary, it enables the signatory party to formally express its will to voluntarily and unconditionally comply with also the obligations contained in the commitment. It enables the accession of multiple stakeholders in the same "agreement", permitting scalability, without requiring additional agreements for each of the new entries.

Based on international law jurisprudence (ICJ, Australia v. France, 1977, Nuclear Tests), it has also been based on an analysis of International, European and national legislation and jurisprudence. This approach is the result of multiple discussions on data agreements within GATEKEEPER and it has already been presented to both the EDPB and various national data protection authorities. Thanks to the positive feedback received, the tool has been marked for exploitation by UDGA who will further refine the approach and coordinate with national data protection authorities for its formal validation in the upcoming months.

7.2 Health data sharing

As noted in section 5.2, work on the facilitation of health data sharing was identified as a priority for the project. This led to the following developments:

7.2.1 Medical data sharing self-assessment solution

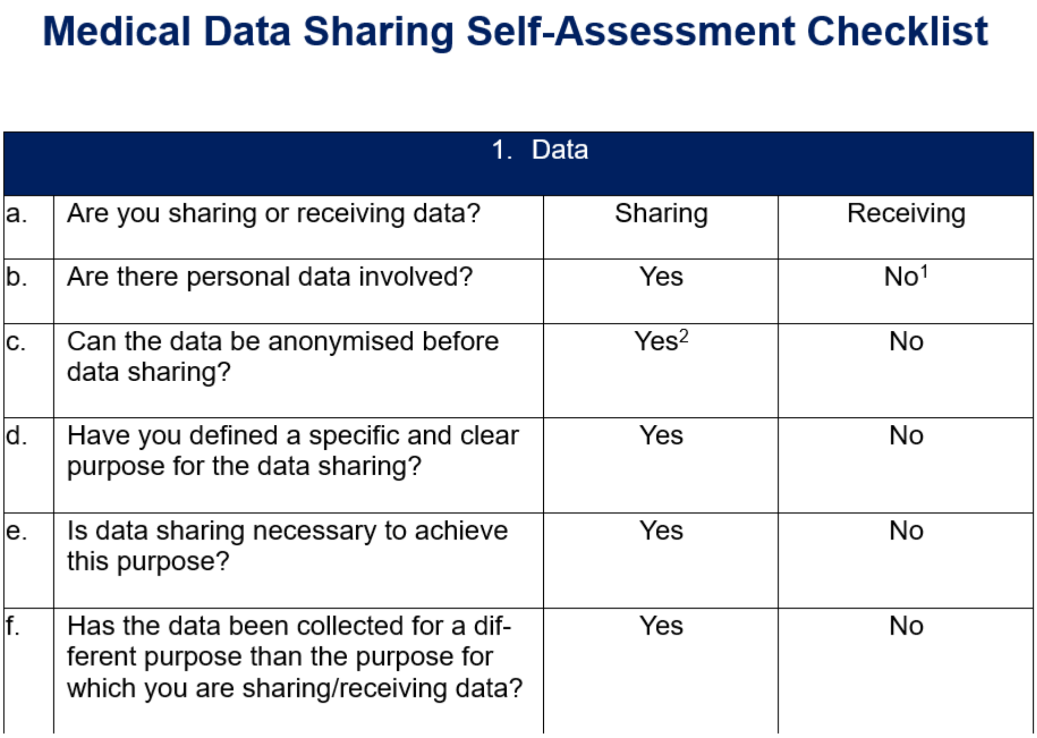
In the context of the GATEKEEPER project, a self-assessment methodology was designed, aimed to assist data holders lawfully share health and medical data, whether this involves personal data or not. The goal behind this is to enable data holders and data receivers to ensure that all organisations that wish to share data to comply with the mandatory requirements set out by applicable legislations. This would be particularly relevant for GATEKEEPER partners wishing to share data through the project's platform, or in order for said data to be reused in a manner that fosters research and innovation.

It is worth highlighting that said self-assessment solution has been designed to assist organisations in reviewing the lawfulness of their data sharing activities, but is not intended to provide presumption of compliance.

Taking the above into consideration and to ensure that a comprehensive list is in place, first an analysis of the relevant legislation, including the GDPR, the EHDS and the Data Governance Act, was performed. Said analysis was further complemented by analysis of ad hoc guidelines and recommendations issued by competent authorities [such as the European Data Protection Board's Guidelines 05/2020 on consent under Regulation 2016/679 (2020)], which were used to complement and better translate the requirements into a step-by-step analysis of compliance.

The self-assessment has been designed to be as simple and intuitive as possible without compromising quality. To assist the parties using this solution to self-assess their compliance with health data sharing requirements, the procedure considers that on many occasions the parties might not have legal expertise. As such, an easy-to-follow step-by-step approach has been adopted, starting from the lawfulness of the original data collection onwards. In order to further facilitate comprehension of the various requirements included, additional relevant material per requirement has been listed.

The original design of the self-assessment solution adopted the form of a question-based checklist (see figure below) and served as an initial draft of the proposed Health Data Certification (See the following section). Following the finalization of GATEKEEPER, the self-assessment methodology draft was presented to the EDPB and other research initiatives in November 2023 for research continuity and validation. UDGA is currently working on its potential integration with relevant tools (AI chatbots, etc.) as part of its exploitation strategy for the methodology.



Medical Data Sharing Self-Assessment Checklist

1. Data			
a.	Are you sharing or receiving data?	Sharing	Receiving
b.	Are there personal data involved?	Yes	No[1]
c.	Can the data be anonymised before data sharing?	Yes[2]	No
d.	Have you defined a specific and clear purpose for the data sharing?	Yes	No
e.	Is data sharing necessary to achieve this purpose?	Yes	No
f.	Has the data been collected for a different purpose than the purpose for which you are sharing/receiving data?	Yes	No

Figure 46: Example of the Medical Data Sharing Self-Assessment Checklist.

7.2.2 Proposed health data certification

As mentioned in previous sections on the topic, the proposed health data sharing certification will cover the requirements set out under the Data Governance Act, Data Act, European Health Data Space Regulation, NIS2 Directive and the DSA. However, as the scope of this certification will focus solely on health data sharing activities (health-related data processing activities), only those requirements derived from the abovementioned regulations and are applicable to this specific scope will be included in the certification. The table below provides a list of the articles considered by the current draft of the health data sharing certification criteria:

Table 12: List of Articles of relevance to Health Data Sharing Certification

Legislation	Articles
GDPR	5, 6 ,7, 9, 12-21, 25, 32, 35, 44-50, 89
DSA	31,36
NIS2	18,21,26
DGA	4,5,6,9-12,16-19
DA	5-8,11,14-19,21
EHDSR	17,31,32,34,35,40

As mentioned in section 7.7.1, the proposed certification scheme is aligned with the Europrivacy model, as this enables an EDPB approved approach to evaluating conformity of health data processing activities (and particularly for those related to sharing personal health data with third parties). Thus, in order to increase trust between data holders and data receivers, both the Europrivacy certification and the health data sharing certification would be ideally deployed, to ensure a holistic compliance with the entire regulatory framework. The figure below visualises which requirements are included under which proposed certification.

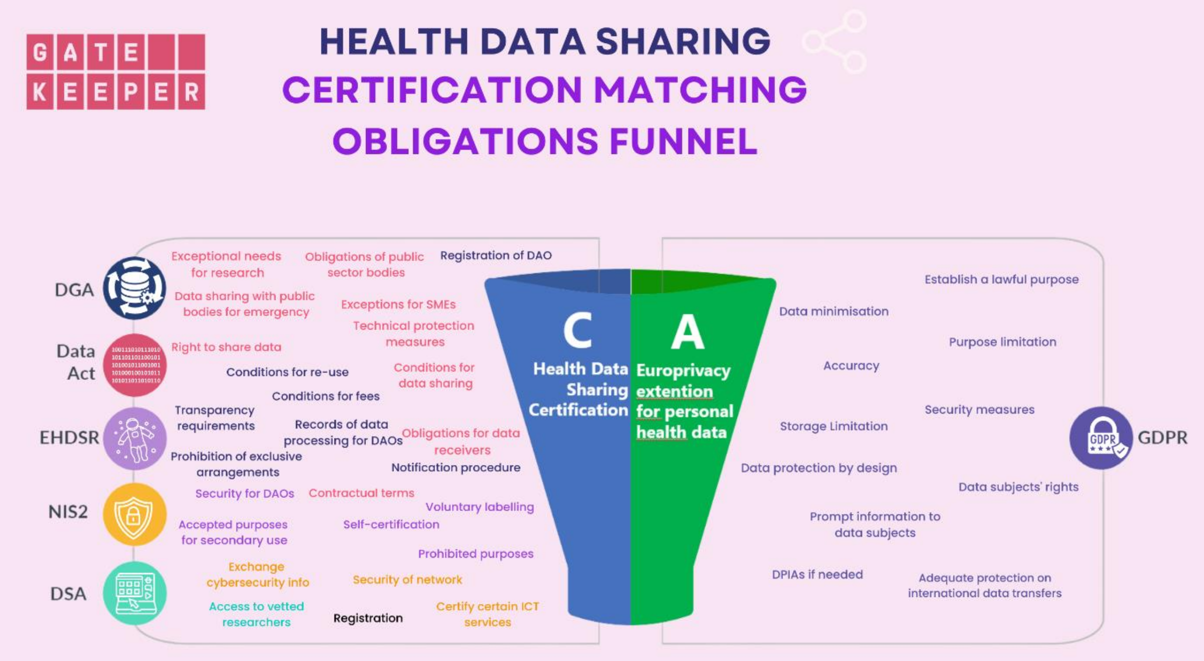

GATE KEEPER
HEALTH DATA SHARING
CERTIFICATION MATCHING
OBLIGATIONS FUNNEL
DGA
Data Act
EHDSR
NIS2
DSA
Exceptional needs for research
Obligations of public sector bodies
Registration of DAO
Data sharing with public bodies for emergency
Exceptions for SMEs
Technical protection measures
Right to share data
Conditions for re-use
Conditions for data sharing
Conditions for fees
Transparency requirements
Records of data processing for DAOs
Obligations for data receivers
Prohibition of exclusive arrangements
Notification procedure
Security for DAOs
Contractual terms
Voluntary labelling
Accepted purposes for secondary use
Self-certification
Prohibited purposes
Exchange cybersecurity info
Security of network
Access to vetted researchers
Registration
Certify certain ICT services
C
Health Data Sharing Certification
A
Europrivacy extention for personal health data
Establish a lawful purpose
Data minimisation
Purpose limitation
Accuracy
Security measures
Storage Limitation
Data protection by design
Data subjects' rights
Prompt information to data subjects
DPIAs if needed
Adequate protection on international data transfers
GDPR

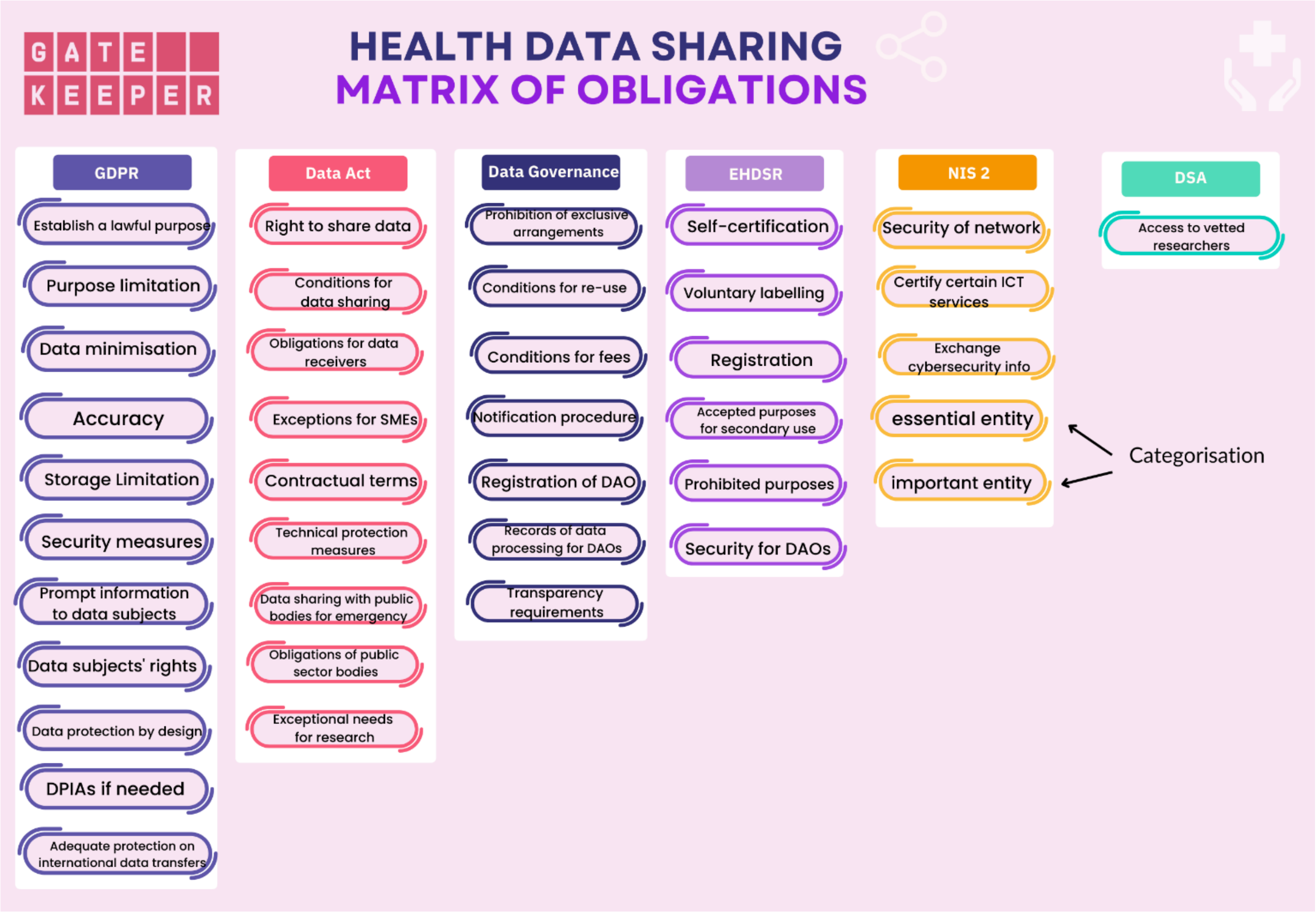
Figure 47: Health Data Sharing Certification – Matching of obligations with available/proposed certifications

The envisioned health data sharing certification aims to build trust between parties wishing to share health data. As already stated above, this model certification developed is not mandatory under any current or foreseeable legislation. This is why a more gradual approach is proposed with assurance levels that must be referred in the statement of conformity. The first "basic" level will be a self-certification scheme (building upon the self-assessment tool mentioned in the previous section) where the party will declare compliance with the mandatory requirements by announcing the name of the document, policy, measure in place that can demonstrate this compliance per obligation.

For the second "substantial" assurance level, the party-data holder will decide whether or not it will share its data with the data receiver, and determine if they have enough access to assess whether the applicant-data receiver complies with the main requirements and has sufficient documentation that proves so.

Lastly, for the final assurance level, "high" in addition to the process followed for the "substantial" assurance level, the data holder will have the chance to practically test whether compliance with all requirements is achieved (before processing real personal health data of natural persons). The above assurance levels follow the logic proposed for the Cybersecurity certification scheme under art. 52 of the Cybersecurity Act, to be consistent with the new upcoming certification schemes in the EU. Especially the "substantial" and "high" assurance levels can be part of the due diligence process before a data sharing agreement between the parties is drafted.

Following the Europrivacy approach and criteria for organisations and implementation guidance, a detailed file with the main requirements for health data sharing was drafted as summarised in the figure below:



GATEKEEPER

HEALTH DATA SHARING
MATRIX OF OBLIGATIONS

GDPR
Establish a lawful purpose
Purpose limitation
Data minimisation
Accuracy
Storage Limitation
Security measures
Prompt information to data subjects
Data subjects' rights
Data protection by design
DPIAs if needed
Adequate protection on international data transfers

Data Act
Right to share data
Conditions for data sharing
Obligations for data receivers
Exceptions for SMEs
Contractual terms
Technical protection measures
Data sharing with public bodies for emergency
Obligations of public sector bodies
Exceptional needs for research

Data Governance
Prohibition of exclusive arrangements
Conditions for re-use
Conditions for fees
Notification procedure
Registration of DAO
Records of data processing for DAOs
Transparency requirements

EHDSR
Self-certification
Voluntary labelling
Registration
Accepted purposes for secondary use
Prohibited purposes
Security for DAOs

NIS 2
Security of network
Certify certain ICT services
Exchange cybersecurity info
essential entity
important entity

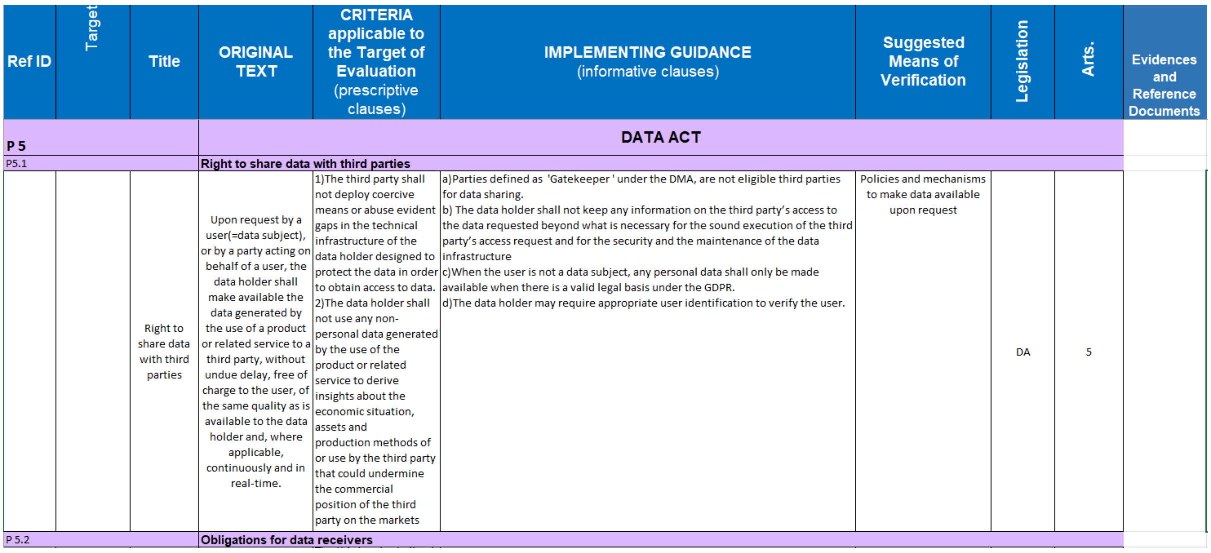
DSA
Access to vetted researchers

Categorisation

Figure 48: Health Data Sharing Certification – Matrix of Obligations

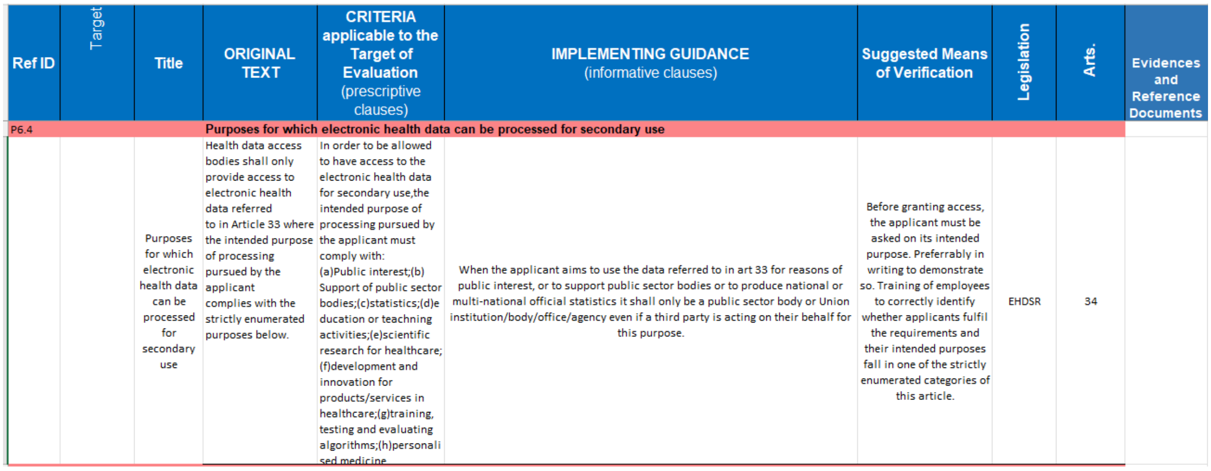
To facilitate the implementation and assessment of compliance with the above obligations, each criterion is accompanied by implementing guidance and suggested means of verification in order to further facilitate their implementation.

A sample of the certification criteria is shown in the figures below:



Ref ID	Target	Title	ORIGINAL TEXT	CRITERIA applicable to the Target of Evaluation (prescriptive clauses)	IMPLEMENTING GUIDANCE (informative clauses)	Suggested Means of Verification	Legislation	Arts.	Evidences and Reference Documents
P 5			DATA ACT						
P5.1			Right to share data with third parties						
		Right to share data with third parties	Upon request by a user(=data subject), or by a party acting on behalf of a user, the data holder shall make available the data generated by the use of a product or related service to a third party, without undue delay, free of charge to the user, of the same quality as is available to the data holder and, where applicable, continuously and in real-time.	1)The third party shall not deploy coercive means or abuse evident gaps in the technical infrastructure of the data holder designed to protect the data in order to obtain access to data. 2)The data holder shall not use any non-personal data generated by the use of the product or related service to derive insights about the economic situation, assets and production methods of or use by the third party that could undermine the commercial position of the third party on the markets	a)Parties defined as 'Gatekeeper ' under the DMA, are not eligible third parties for data sharing. b) The data holder shall not keep any information on the third party's access to the data requested beyond what is necessary for the sound execution of the third party's access request and for the security and the maintenance of the data infrastructure c)When the user is not a data subject, any personal data shall only be made available when there is a valid legal basis under the GDPR. d)The data holder may require appropriate user identification to verify the user.	Policies and mechanisms to make data available upon request	DA	5	
P 5.2			Obligations for data receivers						

Figure 49: Sample I of the first draft of qualification requirements for the certification on health data sharing



Ref ID	Target	Title	ORIGINAL TEXT	CRITERIA applicable to the Target of Evaluation (prescriptive clauses)	IMPLEMENTING GUIDANCE (informative clauses)	Suggested Means of Verification	Legislation	Arts.	Evidences and Reference Documents
P6.4			Purposes for which electronic health data can be processed for secondary use						
		Purposes for which electronic health data can be processed for secondary use	Health data access bodies shall only provide access to electronic health data referred to in Article 33 where the intended purpose of processing pursued by the applicant complies with the strictly enumerated purposes below.	In order to be allowed to have access to the electronic health data for secondary use,the intended purpose of processing pursued by the applicant must comply with: (a)Public interest;(b) Support of public sector bodies;(c)statistics;(d)education or teaching activities;(e)scientific research for healthcare;(f)development and innovation for products/services in healthcare;(g)training, testing and evaluating algorithms;(h)personalised medicine	When the applicant aims to use the data referred to in art 33 for reasons of public interest, or to support public sector bodies or to produce national or multi-national official statistics it shall only be a public sector body or Union institution/body/office/agency even if a third party is acting on their behalf for this purpose.	Before granting access, the applicant must be asked on its intended purpose. Preferrably in writing to demonstrate so. Training of employees to correctly identify whether applicants fulfil the requirements and their intended purposes fall in one of the strictly enumerated categories of this article.	EHDSR	34	

Figure 50: Sample II of the first draft of qualification requirements for the certification on health data sharing

The certification model and draft criteria have been submitted in November 2023 to the European Centre for Certification and Privacy, the Europrivacy scheme owner for consideration and potential adoption following technical validation by supervisory authorities.

7.3 AI certification/extension

The last years of the GATEKEEPER project saw a fast evolution in the regulatory landscape for AI. As mentioned in Chapter 5, GATEKEEPER T8.3 identified relevant gaps where certification could be of use to demonstrate compliance, for this reason draft criteria were defined as part of the task. To do so, a similar methodology was followed as the one used in developing criteria for e-health certification, adapted to address the unique challenges and opportunities presented by AI technologies. This involved a thorough analysis of existing standards and requirements, consultations with stakeholders, and alignment with emerging EU regulations.

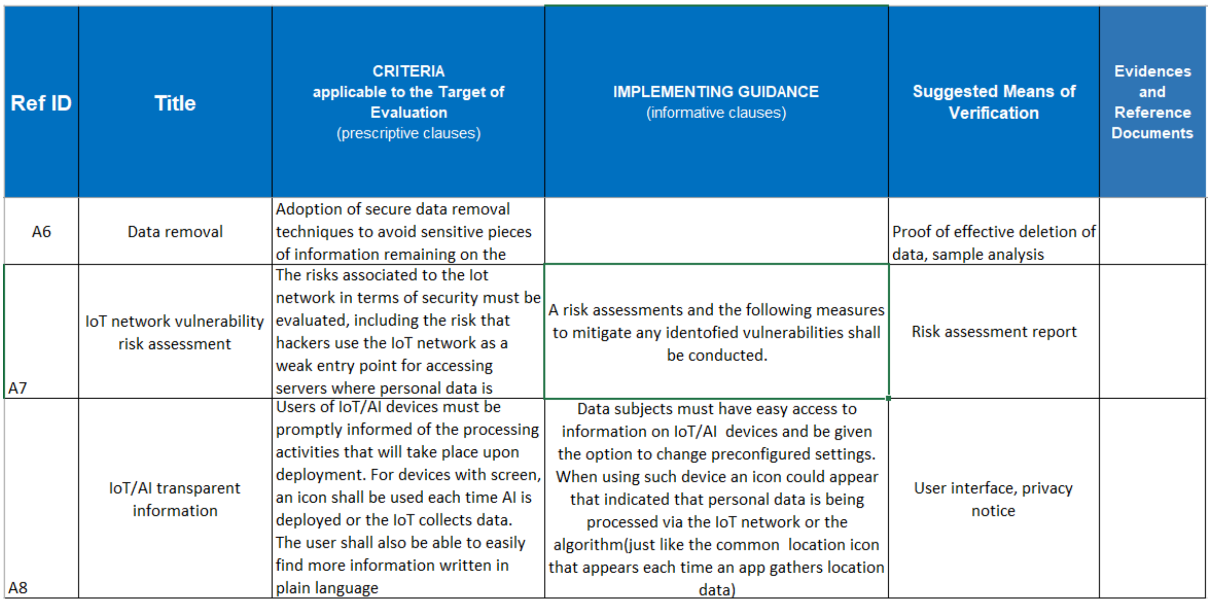
A significant challenge encountered in this process was the delay in the finalization of the EU AI Act. The pace at which the final text of the EU AI Act was approved introduced uncertainties and complexities in defining precise and future-proof criteria for AI certification. This delay impacted the ability to identify clear and definitive technical requirements and relevant standards for their alignment with the legal framework.

Despite these challenges, work on developing AI certification criteria within the GATEKEEPER project is ongoing. The project team is committed to continuing this effort, even beyond the lifespan of the GATEKEEPER project. Key action areas include:

- Alignment with Finalized AI Act: Continuous monitoring and analysis of the final AI Act text to ensure that the developed criteria are fully compliant and relevant.
- Stakeholder Engagement: Engaging with a broad range of stakeholders, including AI developers, regulatory bodies, and end-users, to ensure that the criteria are practical, implementable, and address the needs of all parties.
- Market Readiness: Preparing for the anticipated increase in demand for AI certification once the AI Act is enforced, positioning the GATEKEEPER project's outputs as a valuable resource in this emerging space.
- Collaboration with Standardization Bodies: Seeking collaboration opportunities with major standardization bodies to enhance the impact and acceptance of the developed criteria.

The following table provides an example of the draft criteria prepared in the context of the project and submitted for consideration by ECCP.

Table 13: Sample of the extension of complementary checks and controls that deploy IoT/AI devices.



Ref ID	Title	CRITERIA applicable to the Target of Evaluation (prescriptive clauses)	IMPLEMENTING GUIDANCE (informative clauses)	Suggested Means of Verification	Evidences and Reference Documents
A6	Data removal	Adoption of secure data removal techniques to avoid sensitive pieces of information remaining on the		Proof of effective deletion of data, sample analysis	
A7	IoT network vulnerability risk assessment	The risks associated to the Iot network in terms of security must be evaluated, including the risk that hackers use the IoT network as a weak entry point for accessing servers where personal data is	A risk assessments and the following measures to mitigate any identofied vulnerabilities shall be conducted.	Risk assessment report	
A8	IoT/AI transparent information	Users of IoT/AI devices must be promptly informed of the processing activities that will take place upon deployment. For devices with screen, an icon shall be used each time AI is deployed or the IoT collects data. The user shall also be able to easily find more information written in plain language	Data subjects must have easy access to information on IoT/AI devices and be given the option to change preconfigured settings. When using such device an icon could appear that indicated that personal data is being processed via the IoT network or the algorithm(just like the common location icon that appears each time an app gathers location data)	User interface, privacy notice	

8 Conclusions and future plans

Deliverable 8.3 presents the key results of GATEKEEPER Task 8.3. Through a combination of stakeholder workshops, surveys, and expert consultations, the task achieved an in-depth understanding of the needs and requirements for certification and CRS development in various domains. The examination of current certification solutions, gap analysis, and a proposed certification scheme strategy underscore our commitment of developing a viable, sustainable solution. This goal was achieved through by leveraging existing initiatives, such as the Europrivacy Certification Scheme, and integrating technical tools and solutions to develop well-rounded and efficient approaches to certification.

The demand and requirement analysis, alongside a comprehensive research on standards and legal frameworks, identified relevant areas of opportunity for potential certification/CRS development. The following bullets will synthetize the main outcomes for each:

- Trust and Interoperability: While the valuable perspectives of stakeholders emphasised the necessity of interoperability solutions ensuring reliable data exchanges and adherence to common standards, particularly in the context of HL7 FHIR formats. Work on this topic was particularly addressed through WP4 and the GATEKEEPER Trust Authority, which enables technical and legal certification and trust generation.
- Artificial intelligence: While the late approval of the text of the EU AIA prevented additional progress in the approval of the developed criteria, the draft with GATEEPER project's criteria was submitted for consideration by ECCP.
- Personal Data Protection: Following a comprehensive examination of relevant legal standards, the Europrivacy Certification Scheme, was highlighted for its' GDPR-focus and interoperability with ISO standards. GATEKEEPER contributions were instrumental to the scheme's approval as the first Data Protection Seal endorsed by the EDPB. Furthermore, a unilateral contractually binding registered commitment tool was developed to help simplify complex personal data processing and sharing agreements.
- Health Data Sharing: Following the identification of relevant gaps, a self-assessment methodology for medical data sharing was generated and presented to EDPB and ECCP, this in turn enabled the specification of a potential multi-regulatory compliance certification to be used in tandem with an Europrivacy Certification, which could be adopted in the future. Draft criteria were submitted to ECCP for consideration and further refinement beyond the GATEKEEPER project's life-cycle.

Since its inception, the GATEKEEPER project has sought to balance technological innovation with legal and ethical compliance while paving the way for future advancements in health data management. Given the lengthy nature of the definition, validation, adoption, accreditation, and exploitation process for certification-related solutions. Continuous stakeholder engagement, the monitoring of legal developments, alignment with relevant (technical and organizational) standards, and their development bodies is crucial for ensuring the success of future certification-related activities.

9 References

1. Article 29 Working Party (2016) Guidelines on consent under Regulation 2016/679 (wp259, rev. 01) https://ec.europa.eu/newsroom/article29/items/623051/en

2. Article 29 Working Party (2017) Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, (WP248 rev.01) https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

3. Article 29 Working Party (2018) Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251, rev.01) https://ec.europa.eu/newsroom/article29/items/612053/en

4. BSI, 'BS 10012 Personal information management' https://www.bsigroup.com/en-GB/BS-10012-Personal-information-management/

5. COCIR (2021), 'Artificial Intelligence in EU Medical Device Legislation' https://www.cocir.org/fileadmin/Publications_2021/COCIR_Analysis_on_AI_in_medical_Device_Legislation_-_May_2021.pdf

6. Council of the European Communities, Directive 93/42 EEC of 14 June 1993 Concerning Medical Devices [1993] OJ L 169/1 ('MDD').

7. Council of the European Union(2021a), Proposal of the European Parliament and of the Council on European data governance (Data Governance Act)-Mandate for negotiations with the European Parliament

8. Council of the European Union (2021b), Promoting data sharing: presidency reaches deal with Parliament on Data Governance Act https://www.consilium.europa.eu/en/press/press-releases/2021/11/30/promoting-data-sharing-presidency-reaches-deal-with-parliament-on-data-governance-act/

9. Council of the European Union (2021c), 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-Presidency compromise text, 2021/0106(COD)

10. Council of Europe (2021), 'The CAHAI held its 6th and final plenary meeting' https://www.coe.int/en/web/artificial-intelligence/-/outcome-of-cahai-s-6th-plenary-meeting

11. David Schönberger, 'Artificial Intelligence in Healthcare: a Critical Analysis of the Legal and Ethical Implications' (2019) 27(2) Int J Law Inf Techno 171.

12. Dimitra Kamarinou, Christopher Millard et al, 'Protection of Personal Data in Clouds and Rights of Individuals, in *Cloud Computing Law*, 2nd edn, OUP 2021.

13. EDPB, (2018a) 'Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679' https://edpb.europa.eu/our-work-tools/documents/public-consultations/2018/guidelines-12018-certification-and-identifying_en

14. EDPB (2018b) 'Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679)' (version 3, June 2019) https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201804_v3.0_accreditationcertificationbodies_annex1_en.pdf

15. EDPB (2019) 'Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities'. Available at: https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-52019-interplay-between-eprivacy_en (Accessed: 12 January 2022).

16. EDPB (2020) Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf

17. EDPB-EDPS (2021) - Joint Opinion 03/2021 on the Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act) (v.1.1) https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-032021-proposal_en

18. Eric Lachaud (2020), 'ISO/IEC 27701 Standard: Threats and Opportunities for GDPR Certification' 6 Eur Data Prot L Rev, 194.

19. European Commission, 'European data strategy – Making the EU a role model for a society empowered by data' https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en

20. European Commission (2017), 'Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM/2017/010 final - 2017/03 ('ePR')

21. European Commission (2020a) Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act)

22. European Commission (2020b) -Shaping Europe's digital future: Commission presents strategies for data and Artificial Intelligence https://ec.europa.eu/commission/presscorner/detail/en/ip_20_273

23. European Commission (2020c) 'Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148'. Available at:

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:823:FIN (Accessed: 12 October 2021).

24. European Commission (2020d), 'Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC', available at https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-european-parliament-and-council-single-market-digital-services-digital-services (Accessed: 17 January 2022)
25. European Commission (2020e), 'REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on contestable and fair markets in the digital sector (Digital Markets Act)' available at https://ec.europa.eu/info/sites/default/files/proposal-regulation-single-market-digital-services-digital-services-act_en.pdf .
26. European Commission (2020f). 'COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS- Commission Work Programme 2021' COM(2020)690 final https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0690
27. European Commission (2021a) Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence and amending certain Union legislative acts (AIA)
28. European Commission (2021b) IMPLEMENTING DECISION (EU) 2021/1182 of 16 July 2021 on the harmonised standards for medical devices drafted in support of Regulation (EU) 2017/745 of the European Parliament and of the Council OJ L 256/100 https://eur-lex.europa.eu/eli/dec_impl/2021/1182/oj
29. European Commission (2021c), 'Inception Impact Assessment' Ares(2021)3527151-28/05/2021 available at https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13045-Data-Act-including-the-review-of-the-Directive-96-9-EC-on-the-legal-protection-of-databases-_en
30. European Commission (2022), 'Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on harmonised rules on fair access to and use of data (Data Act)' COM (2022) 68 final https://digital-strategy.ec.europa.eu/en/library/data-act-proposal-regulation-harmonised-rules-fair-access-and-use-data
31. European Commission (2022b), 'COMMISSION STAFF WORKING DOCUMENT on Common European Data Spaces' SWD(2022) 45 final https://digital-strategy.ec.europa.eu/en/library/staff-working-document-data-spaces
32. European Commission (2022c), 'ANNEX to the Commission Notice - The 2022 annual Union work programme for European standardisation' COM(2022)546final https://ec.europa.eu/docsroom/documents/48601
33. European Commission (2022d), 'Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space' (2022)197final

https://ec.europa.eu/health/publications/proposal-regulation-european-health-data-space_en

34. European Parliament, (2002) 'Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) OJ L 201/37 ('ePD')

35. European Parliament (2016) General Data Protection Regulation ('GDPR')

36. European Parliament and European Council, (2016b) 'Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union'. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC (Accessed: 12 October 2021).

37. European Parliament (2017) REGULATION (EU) 2017/745 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC ('MDR')

38. European Parliament (2019) Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), OJ L 151/15.

39. ICO, 'Data sharing covered by the code' https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/data-sharing-a-code-of-practice/data-sharing-covered-by-the-code/

40. Medical Device Coordination Group (2019) 'Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR' ('MDCG 2019').

41. Member States and the European Commission (2022) 'EUROPEAN ETHICAL PRINCIPLES FOR DIGITAL HEALTH' https://presidence-francaise.consilium.europa.eu/media/mw3b3zjq/european-ethical-principles-for-digital-health-introduction_vdef_revue-002.pdf

42.

43. Nativi, S. and De Nigris, S.(2021), 'AI Standardisation Landscape: state of play and link to the EC proposal for an AI regulatory framework', Publications Office of the European Union, Luxembourg, ISBN 978-92-76-40325-8, doi:10.2760/376602, JRC125952.

44. Oxford Commission on AI & Good Governance, (2021) 'Harmonising Artificial Intelligence: The role of standards in the EU AI Regulation,

https://oxil.uk/publications/2021-12-02-oxford-internet-institute-oxil-harmonising-ai/Harmonising-AI-OXIL.pdf

45. UNESCO (2021), 'Report of the social and human sciences Commission (SHS), 41 C/73, 22 November 2021 https://unesdoc.unesco.org/ark:/48223/pf0000379920.page=14

Appendix A Gatekeeper Certification Survey

Dear partners, in order to pave the way to a successful certification strategy in the framework of the GATEKEEPER project, we need your inputs. We would like to get each partner on board in our certification activities and to understand the specific certification needs and requirements of your domain. The results of this survey will be used to identify the demand side for certification, conduct a gap analysis, and based on the findings to develop a Gatekeeper-tailored certification strategy.

Partner's name:

Person of contact name:

Person of contact email:

1. **To which category of the GATEKEEPER ecosystem does your organisation belong?**

□ Healthcare provider to patients

□ Solutions and service provider to medical domain

□ Representative of patients and/or medical professionals

□ Research Institution and/or Academy

□ Ecosystem enlargement, Standardization and Impact

2. **Why certification would be useful for Gatekeeper?**

3. **What are the research results of GATEKEEER that could benefit from a certification for their exploitation and adoption?**

4. **What fears or concerns could a certification address to facilitate the adoption and use of GATEKEEPER solutions and services? What should be the priority scope of certification?**

5. **What existing certification scheme do you know that could be relevant for Gatekeeper results for:**

   a. **Privacy and regulatory compliance?**

   b. **Interoperability?**

6. **What should be the key requirements and principles to be considered for the development of GATEKEEPER certification solutions?**

Optional for solution providers and health services:

7. **What are the main regulations you have to comply with?**

8. **What certification do you have?**

9. **Other suggestions and remarks**

Appendix B AI-related standards: summary introduction

Each standard is briefly introduced in the following pages:

A. ISO standards

Reference ID
ISO/IEC 25024:2015
Title
Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Measurement of data quality
Main objectives/content
ISO/IEC 25024:2015 defines data quality measures for quantitatively measuring the data quality in terms of characteristics defined in ISO/IEC 25012. It contains a basic set of data quality measures for each characteristic, a set of target entities to which the quality measures are applied during the data life cycle and guidance for organisations defining their own measures for data quality. This standard does not define ranges of values of these quality measures to rate levels or grades but allows each system depending on its nature and user needs to define it. The scope does not include data mining techniques, knowledge representation nor statistical significance for random sample.
Useful link
https://www.iso.org/standard/35749.html

Reference ID
ISO/IEC AWI 5259 (1-4)
Title
Artificial intelligence — Data quality for analytics and machine learning (ML)
Main objectives/content
This standard aims to provide the landscape for understanding and associating of data quality for analytics for ML. It will include an overview, terminology, and examples (part 1), data quality measures (part 2), data quality management requirements and guidelines (part 3) as well as a data quality process framework (part 4).
Useful link
https://www.iso.org/standard/81088.html?browse=tc

Reference ID

ISO/IEC DIS 24668
Title
Information technology — Artificial intelligence — Process management framework for big data analytics
Main objectives/content
This standard provides a framework for developing processes to effectively leverage big data analytics across the organisation irrespective of the industries/sectors. This standard specifies process management for big data analytics with its various process categories taken into account along with their interconnectivities. These process categories are organisation stakeholder processes, competency development processes, data management processes, analytics development processes and technology integration processes. This standard describes processes to acquire, describe, store and process data at an organisation level which provides big data analytics services.
Useful link
https://www.iso.org/standard/78368.html

Reference ID
ISO/IEC DTS 4213.2
Title
Information technology — Artificial Intelligence — Assessment of machine learning classification performance
Main objectives/content
This standard aims to specify methodologies for measuring classification performance of machine learning models, systems and algorithms
Useful link
https://www.iso.org/standard/79799.html

Reference ID
ISO/IEC CD 24029-2
Title
Artificial intelligence (AI) — Assessment of the robustness of neural networks — Part 2: Methodology for the use of formal methods
Main objectives/content
-

Useful link
https://www.iso.org/standard/79804.html

Reference ID
ISO/IEC DIS 23894
Title
Information technology — Artificial intelligence — Risk management
Main objectives/content
This standard provides guidelines on managing risk during the development and application of artificial intelligence (AI) systems. Processes for the effective implementation and integration of AI risk management are included. The application of these guidelines can be customised to any organisation and its context.
Useful link
https://www.iso.org/standard/77304.html

Reference ID
ISO/IEC AWI TR 5469
Title
Artificial intelligence — Functional safety and AI systems
Main objectives/content
This International Standard describes properties, relevant risk factors, usable methods and processes for the application of AI in safety-relevant functions, to control AI systems.
Useful link
https://www.iso.org/standard/81283.html?browse=tc

Reference ID
ISO/IEC TR 24372:2021
Title
Information technology — Artificial intelligence (AI) — Overview of computational approaches for AI systems

Main objectives/content
This document provides an overview of the state of the art of computational approaches for AI systems, by describing: a) main computational characteristics of AI systems; b) main algorithms and approaches used in AI systems, referencing use cases contained in ISO/IEC TR 24030.
Useful link
https://www.iso.org/standard/78508.html

Reference ID
ISO/IEC DTR 24368
Title
Information technology — Artificial intelligence — Overview of ethical and societal concerns
Main objectives/content
-
Useful link
https://www.iso.org/standard/78507.html?browse=tc

Reference ID
ISO/IEC CD 5338
Title
Information technology — Artificial intelligence — AI system life cycle processes
Main objectives/content
The standard aims to provide processes that support the control and improvement of AI system life cycle processes used within an organisation or a project.
Useful link
https://www.iso.org/standard/81118.html

Reference ID
ISO/IEC AWI TS 6254
Title

Information technology — Artificial intelligence — Objectives and approaches for explainability of ML models and AI systems
Main objectives/content
This document describes approaches and methods that can be used to achieve explainability with regards to ML models and AI systems' behaviours, outputs, and results. Stakeholders include but are not limited to, industry, and end-users. It provides guidance concerning the applicability of the described approaches and methods to the identified objectives throughout the AI system's life cycle, as defined in ISO/IEC 22989.
Useful link
https://www.iso.org/standard/82148.html

Reference ID
ISO/IEC 20547-4:2020
Title
Information technology — Big data reference architecture — Part 4: Security and privacy
Main objectives/content
This document specifies the security and privacy aspects applicable to the big data reference architecture (BDRA) including the big data roles, activities and functional components, and also provides guidance on security and privacy operations for big data.
Useful link
https://www.iso.org/standard/71278.html

Reference ID
ISO/IEC TR 24028:2020
Title
Information technology — Artificial intelligence — Overview of trustworthiness in artificial intelligence
Main objectives/content
This document surveys topics related to trustworthiness in AI systems, including the following: — approaches to establish trust in AI systems through transparency, explainability, controllability, etc. — engineering pitfalls and typical associated threats and risks to AI systems, along with possible mitigation techniques and methods; and

— approaches to assess and achieve availability, resiliency, reliability, accuracy, safety, security and privacy of AI systems. The specification of levels of trustworthiness for AI systems is out of the scope of this document
Useful link
https://www.iso.org/standard/77608.html

Reference ID
ISO/IEC TR 24027:2021
Title
Information technology — Artificial intelligence (AI) — Bias in AI systems and AI aided decision making
Main objectives/content
This document addresses bias in relation to AI systems, especially with regards to AI-aided decision-making. It provides measurement techniques and methods for assessing bias, with the aim to address and treat bias-related vulnerabilities. All AI system lifecycle phases are in scope, including but not limited to data collection, training, continual learning, design, testing, evaluation and use.
Useful link
https://www.iso.org/standard/77607.html

Reference ID
ISO/IEC TR 24029-1:2021
Title
Artificial Intelligence (AI) — Assessment of the robustness of neural networks — Part 1: Overview
Main objectives/content
This document provides background about existing methods to assess the robustness of neural networks.
Useful link
https://www.iso.org/standard/77609.html

Reference ID
ISO/IEC CD 25059

Title
Software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Quality model for AI systems
Main objectives/content
This standard aims to introduce a quality model for AI systems. It is a specific extension to the SQuaRE series. The model characteristics provide a consistent terminology for specifying, measuring and evaluating AI system quality.
Useful link
https://www.iso.org/standard/80655.html

Reference ID
ISO/IEC FDIS 38507
Title
Information technology — Governance of IT — Governance implications of the use of artificial intelligence by organisations
Main objectives/content
To provide guidance for governing bodies of organisations that are using tools or systems that incorporate artificial intelligence. This document is a high level, principles-based advisory standard. In addition to providing broad guidance on the role of a governing body, it encourages organisations to use appropriate standards to underpin their governance of information technology – including the use of artificial intelligence (AI).
Useful link
https://www.iso.org/standard/56641.html

Reference ID
ISO/IEC CD 42001
Title
Information Technology — Artificial intelligence — Management system
Main objectives/content
To provide the requirements and provides guidance for establishing, implementing, maintaining and continually improving an artificial intelligence management system within the context of an organisation.
Useful link

https://www.iso.org/standard/81230.html

Reference ID
ISO/IEC AWI TS 5471
Title
Artificial intelligence — Quality evaluation guidelines for AI systems
Main objectives/content
To provide guidelines for assessing the quality of AI systems using a specific AI system quality model, providing a structured framework to ensure the effectiveness, reliability, and overall quality of AI systems across diverse organizational contexts.
Useful link
https://www.iso.org/standard/82570.html

B. IEEE Standards

Reference ID
IEEE P7002
Title
IEEE Draft Standard for Data Privacy Process
Main objectives/content
The requirements for a systems/software engineering process for privacy-oriented considerations regarding products, services, and systems utilising employee, customer, or other external user's personal data are defined by this standard. Organisations and projects that are developing and deploying products, systems, processes, and applications that involve personal information are candidate users of the P7002 standard. Specific procedures, diagrams, and checklists are provided for users of the P7002 standard to perform conformity assessments on their specific privacy practices. Privacy impact assessments (PIAs) are described as a tool for both identifying where privacy controls and measures are needed and for confirming they are in place.
Useful link
https://standards.ieee.org/ieee/7002/6898/

Reference ID
IEEE P7003
Title

Algorithmic Bias Considerations
Main objectives/content
IEEE Standards Project for Algorithmic Bias Considerations provides developers of algorithms for autonomous or intelligent systems with protocols to avoid negative bias in their code. Bias could include the use of subjective or incorrect interpretations of data like mistaking correlation with causation. The project offers specific steps to take for eliminating issues of negative bias in the creation of algorithms
Useful link
https://ethicsinaction.ieee.org/p7000/

Reference ID
IEEE P7009
Title
Standard for Fail-Safe Design of Autonomous and Semi-Autonomous Systems
Main objectives/content
IEEE Standards Project for Standard for Fail-Safe Design of Autonomous and Semi-Autonomous Systems establishes a practical, technical baseline of specific methodologies and tools for the development, implementation, and use of effective fail-safe mechanisms in autonomous and semi-autonomous systems. The standard includes (but is not limited to): clear procedures for measuring, testing, and certifying a system's ability to fail safely on a scale from weak to strong, and instructions for improvement in the case of unsatisfactory performance. The standard serves as the basis for developers, as well as users and regulators, to design fail-safe mechanisms in a robust, transparent, and accountable manner.
Useful link
https://standards.ieee.org/ieee/7009/7096/

Reference ID
IEEE P7006
Title
PERSONAL DATA AI AGENT WORKING GROUP
Main objectives/content
This standard addresses concerns raised about machines making decisions without human input. It describes the technical elements required to create and grant access to a personalised AI that will comprise inputs, learning, ethics, rules and values controlled by individuals. Designed as a tool to allow any individual to essentially create their own

personal “terms and conditions” for their data, the AI Agent will provide a technological tool for individuals to manage and control their identity in the digital and virtual world.
Useful link
https://sagroups.ieee.org/7006/

Reference ID
IEEE P7001
Title
Transparency of Autonomous Systems
Main objectives/content
IEEE Standards Project for Transparency of Autonomous Systems provides a Standard for developing autonomous technologies that can assess their own actions and help users understand why a technology makes certain decisions in different situations. The project also offers ways to provide transparency and accountability for a system to help guide and improve it, such as incorporating an event data recorder in a self-driving car or accessing data from a device’s sensors
Useful link
https://ethicsinaction.ieee.org/p7000/

Reference ID
IEEE 7000™-2021
Title
Model Process for Addressing Ethical Concerns During System Design
Main objectives/content
IEEE Standards Project for Model Process for Addressing Ethical Concerns During System Design outlines an approach for identifying and analysing potential ethical issues in a system or software program from the onset of the effort. The values-based system design methods addresses ethical considerations at each stage of development to help avoid negative unintended consequences while increasing innovation.
Useful link
https://ethicsinaction.ieee.org/p7000/

Reference ID
IEEE P7002

Title
IEEE Draft Standard for Data Privacy Process
Main objectives/content
The requirements for a systems/software engineering process for privacy-oriented considerations regarding products, services, and systems utilising employee, customer, or other external user's personal data are defined by this standard. Organisations and projects that are developing and deploying products, systems, processes, and applications that involve personal information are candidate users of the P7002 standard. Specific procedures, diagrams, and checklists are provided for users of the P7002 standard to perform conformity assessments on their specific privacy practices. Privacy impact assessments (PIAs) are described as a tool for both identifying where privacy controls and measures are needed and for confirming they are in place.
Useful link
https://standards.ieee.org/ieee/7002/6898/

Reference ID
IEEE P7012
Title
Standard for Machine Readable Personal Privacy Terms
Main objectives/content
IEEE Standards Project for Machine Readable Personal Privacy Terms. The purpose of the standard is to provide individuals with means to proffer their own terms respecting personal privacy, in ways that can be read, acknowledged, and agreed to by machines operated by others in the networked world. In a more formal sense, the purpose of the standard is to enable individuals to operate as first parties in agreements with others—mostly companies—operating as second parties. Note that the purpose of this standard is not to address privacy policies, since these are one-sided and need no agreement. (Terms require agreement; privacy policies do not.)
Useful link
https://ethicsinaction.ieee.org/p7000/

Reference ID
IEEE P7014
Title
Standard for Ethical considerations in Emulated Empathy in Autonomous and Intelligent Systems

Main objectives/content
IEEE Standards Project for the Standard for Ethical considerations in Emulated Empathy in Autonomous and Intelligent Systems. This standard defines a model for ethical considerations and practices in the design, creation and use of empathic technology, incorporating systems that have the capacity to identify, quantify, respond to, or simulate effective states, such as emotions and cognitive states. This includes coverage of 'effective computing', 'emotion Artificial Intelligence' and related fields
Useful link
https://ethicsinaction.ieee.org/p7000/

Reference ID
IEEE P2801
Title
IEEE Draft Recommended Practice for the Quality Management of Datasets for Medical Artificial Intelligence
Main objectives/content
The recommended practice promotes quality management activities for datasets used for artificial intelligence medical device (AIMD). The document highlights quality objective for dataset responsible organisations. The document describes control of records during the life cycle of datasets, including but not limited to data collection, annotation, transfer, utilisation, storage, maintenance, update, retirement and other activities. The document emphasises special consideration for the dataset quality management system, including but not limited to responsibility management, resource management, dataset realisation and quality control.
Useful link
https://standards.ieee.org/ieee/2801/7459/

Reference ID
IEEE P2807
Title
Framework of Knowledge Graphs
Main objectives/content
This standard defines technical requirements, performance metrics, evaluation criteria and test cases for knowledge graphs. The framework describes the input requirement of KG, construction process of KG, i.e., extraction, storage, data fusion and understanding, performance metrics, applications of KG, verticals, KG related artificial intelligence (AI) technologies and other required digital infrastructure.

Useful link
https://standards.ieee.org/ieee/2807/7525/

Reference ID
IEEE P2863™
Title
Recommended Practice for Organisational Governance of Artificial Intelligence
Main objectives/content
This recommended practice specifies governance criteria such as safety, transparency, accountability, responsibility and minimising bias, and process steps for effective implementation, performance auditing, training and compliance in the development or use of artificial intelligence within organisations.
Useful link
https://sagroups.ieee.org/2863/

Reference ID
IEEE P2802
Title
Standard for the Performance and Safety Evaluation of Artificial Intelligence Based Medical Device: Terminology
Main objectives/content
The standard establishes terminology used in artificial intelligence medical device, including definitions of fundamental concepts and methodology that describe the safety, effectiveness, risks and quality management of artificial intelligence medical device. The standard provides definitions using the following forms, such as but not limited to literal description, equations, tables, figures and legends. The standard also establishes a vocabulary for the development of future standards for artificial intelligence medical device.
Useful link
https://standards.ieee.org/ieee/2802/7460/

Reference ID
IEEE P2621
Title

MEDICAL DEVICES CYBERSECURITY
Main objectives/content
Medical devices used for monitoring and managing diabetes provide life-saving benefits to patients and effective implementation options to healthcare professionals. With ever-increasing connectivity and data exchange between devices there is an increased risk to the safety and privacy. This standard will aid medical device manufacturers and users to manage their cybersecurity risk.
Useful link
https://standards.ieee.org/products-services/icap/programs/p2621-series-of-standards/

C. ETSI Standards

Reference ID
DES/eHEALTH-008
Title
eHEALTH Data recording requirements for eHealth
Main objectives/content
The aim of this work is to identify the requirements for recording eHealth events, i.e. those from ICT based eHealth devices and from health practitioners. On the understanding, illustrated in the use case document and in the White Paper, that health records are subject to security and privacy constraints, but at the same time need to be available to many different stakeholders across time and space without pre-cognition of who those stakeholders are. The purpose of this technical specification is to very carefully specify at stage 1 and stage 2 level the normative framework for ensuring events/transactions related to a patient are recorded accurately by identifiable entities (devices or health professionals) and made available with minimum delay to any other health professional (i.e. to ensure that actions taken by one health professional is visible to any other health professional irrespective of location without delay). The normative framework is intended to be adopted by all groups contributing to eHealth including CYBER, smartM2M, smartBAN.
Useful link
https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=56908

Reference ID
DGR/CIM-007-SEC
Title

Context Information Management (CIM); Security and Privacy
Main objectives/content
The purpose of this Work Item is to provide a state of the art assessment of security and privacy issues associated with ISG CIM specifications, in particular related to the API, Data Publishing Platforms and Data Model Work Items. Recommendations shall be accompanied by pro/con information with the intent to reference as much as possible existing widely supported concepts. There are several issues that need to be addressed, including but not limited to provenance of data, assuring privacy and security between stakeholders, assuring trust, understanding how to ensure the aggregation of data does not increase the attack space or compromise privacy. The work item will investigate items such as but not limited to; what should be connected via the information model and are there any particular lifecycle constraints that may be placed on data? The scope of this work is strictly limited to the CIM scope of work, e.g. device security is excluded. Where appropriate, it references existing work, specifications and standards. Safety and reliability issues for systems relying on CIM-based APIs and architectures are out of scope but may be addressed at a later date.
Useful link
https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=53370

Reference ID
DGR/SAI-001
Title
Securing Artificial Intelligence (SAI); AI Threat Ontology
Main objectives/content
The purpose of this work item is to define what would be considered an AI threat and how it might differ from threats to traditional systems. The starting point that offers the rationale for this work is that currently, there is no common understanding of what constitutes an attack on AI and how it might be created, hosted and propagated. The AI Threat Ontology deliverable will seek to align terminology across the different stakeholders and multiple industries. This document will define what is meant by these terms in the context of cyber and physical security and with an accompanying narrative that should be readily accessible by both experts and less informed audiences across the multiple industries. Note that this threat ontology will address AI as a system, an adversarial attacker, and as a system defender.
Useful link
https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=58856

Reference ID

DGR/SAI-002
Title
Securing Artificial Intelligence (SAI); Data Supply Chain Security
Main objectives/content
Data is a critical component in the development of AI systems. This includes raw data as well as information and feedback from other systems and humans in the loop, all of which can be used to change the function of the system by training and retraining the AI. However, access to suitable data is often limited, causing a need to resort to less suitable sources of data. Compromising the integrity of training data has been demonstrated to be a viable attack vector against an AI system. This means that securing the supply chain of the data is an important step in securing the AI. This report will summarise the methods currently used to source data for training AI along with the regulations, standards and protocols that can control the handling and sharing of that data. It will then provide gap analysis on this information to scope possible requirements for standards for ensuring traceability and integrity in the data, associated attributes, information and feedback, as well as the confidentiality of these.
Useful link
https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=58857

Reference ID
DGR/SAI-003
Title
Securing Artificial Intelligence (SAI); Security Testing of AI
Main objectives/content
The purpose of this work item is to identify methods and techniques that are appropriate for security testing of AI-based components. Security testing of AI has some commonalities with security testing of traditional systems but provides new challenges and requires different approaches, due to (a) significant differences between subsymbolic AI and traditional systems that have strong implications on their security and on how to test their security properties, (b) non-determinism since AI-based systems may evolve over time (self-learning systems) and security properties may degrade, (c) test oracle problem, assigning a test verdict is different and more difficult for AI-based systems since not all expected results are known a priori, and (d) data-driven algorithms: in contrast to traditional systems, (training) data forms the behaviour of sub symbolic AI. The scope of this work item is to cover the following topics: • security testing approaches for AI

• security test oracles for AI • definition of test adequacy criteria for security testing of AI.
Useful link
https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=58860

Reference ID
ETSI GR SAI 005 V1.1.1
Title
Securing Artificial Intelligence (SAI); Mitigation Strategy Report
Main objectives/content
The goal is to have a technical survey for mitigating against threats introduced by adopting AI into systems. The technical survey shed light on available methods of securing AI-based systems by mitigating against known or potential security threats. It also addresses security capabilities, challenges, and limitations when adopting mitigation for AI-based systems in certain potential use cases.
Useful link
https://www.etsi.org/deliver/etsi_gr/SAI/001_099/005/01.01.01_60/gr_SAI005v010101p.pdf

Reference ID
ETSI TS 103 327 V1.1.1
Title
Smart Body Area Networks (SmartBAN); **Service and application standardised enablers and interfaces,** **APIs and infrastructure for interoperability management**
Main objectives/content
TC SmartBAN considers interfaces which would allow semantic interoperability of eHealth sensors with external systems (including by default AI).
Useful link
https://www.etsi.org/deliver/etsi_ts/103300_103399/103327/01.01.01_60/ts_103327v010101p.pdf

Reference ID
TR 103 749
Title
INT Artificial Intelligence (AI) in Test Systems and Testing AI models; Testing of AI with definition of quality metrics
Main objectives/content
The present document will report on Testing AI Models, components, systems, Metrics for Measurements and Assessments in Testing and Certification
Useful link
https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=59456

Other relevant standards

Standard	Title
ISO /IEC AWI 5339	Information Technology — Artificial Intelligence — Guidelines for AI applications
ISO/IEC FDIS 23053	Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML)