Optimal treatment for patients with solid tumours in Europe through Artificial Intelligence

Initial report on the legal and ethical framework of the project

OPTIMA
Tackling Cancer through Real World Evidence and Artificial Intelligence

Deliverable number:	**D2.2**
Grant Agreement:	**101034347 (OPTIMA)**
Call identifier:	**IMI23**
Project full title:	**Optimal treatment for patients with solid tumours in Europe through Artificial Intelligence**
Project start date:	**1st October 2021**
Project duration:	**60 months**
Funded:	imi efpia

Lead contributor	13 – UNIVIE William Field-Papuga Nikolaus Forgo Katerina Polychronopoulos Saskia Kaltenbrunner
Other contributors	11 – UPPSALA UNIVERSITET (UU) 35 – F. HOFFMANN-LA ROCHE AG (ROCHE)
Due date	31 Mar 2022
Delivery date	28 April 2022
Deliverable type	R
Dissemination level	PU

Document History

Version	Date	Description
V1.0	28 April 2022	First submission IMI

Contents

1.Abstract

OPTIMA aspires to revolutionize oncology care in Europe, by giving patients suffering from lung, breast and prostate cancer access to the most up-to-date individualized treatments and innovative therapies. To achieve this it will design, develop and deliver the first GDPR-compliant, commercially sustainable European real-world oncology data and evidence generation platform that will provide the best and most personalized treatment course for patients. This will harness the power of enormous data sets, advanced analytics and AI-models. The ultimate product will be a regularly updated guideline decision-support toolset that integrates retrospective and prospective real-world data. The data used by the project will thereby validate the treatment roadmaps or guidelines. The project's use of AI will also fill gaps in knowledge and existing guidelines, and thereby recommend guideline improvements, following robust clinical validation.

The OPTIMA consortium, at the time of this Deliverable, consists of 36 members representing European Union (EU) countries, as well as certain non-EU countries (Switzerland, United Kingdom and the United States). It comprises leading academic and private institutes in diverse fields of medical research and treatment, pharmaceutical manufacturing, data protection, cyber security, data analytics and AI development, among others. Also included, in an advisory capacity, are patient representative bodies.

This Deliverable addresses key legal and ethical topics relevant to the OPTIMA project's research activities; that is, the development and training of the OPTIMA platform, and a few key issues regarding market approval and post-market clinical use of the product. As part of the legal framework, this Deliverable addresses the GDPR, MDR/IVDR and pending legislation in Europe, including the Data Governance Act and the Artificial Intelligence Act. As part of the ethical framework, this deliverable points to key ethical questions that the project raises and discusses requirements stemming primarily from the field of healthcare ethics and AI ethics.

With this background, we hope the Legal and Ethical Framework (D2.2) will support OPTIMA partners, the project as a whole, and the project coordination team to keep the project fully in line with legal and ethical requirements. Partners, as legal entities, are responsible for ensuring compliance with the relevant legislation addressed in this report.

2.Aim of this Deliverable

The aim of the Legal and Ethical Framework is to provide the Consortium with guidelines on legally compliant development of the technology and general conduct within the project.

The Legal portion of the Framework will, *inter alia*, address the following pieces of legislation relevant to OPTIMA: (1) Regulation 2016/679 (GDPR); (2) National data protection and research legislation; (3) Regulations 201/745 (MDR) and 2017/746 (IVDR); and (4) Pending legislative developments in the field including the Data Governance Act, the European Health Data Space, and the Artificial Intelligence Act.

A second iteration of this document, to be submitted in Month 20 of the Project, after conclusion of the GDPR Article 26 and 28 Agreements and the Data Management Plan (DMP) will include more detailed governance principles for the data platform and AI component.

The Ethical portion of the Framework will identify and address key ethical issues, including the use of personal data from retrospective data sources, the collection of prospective data in WP3, respect for the rights of patients and data subjects, the development of trustworthy AI. Guiding principles separately concern scientific integrity and the overall conduct of the Consortium, ethical aspects of the research in healthcare and of the use of personal data for the data platform, and development of the AI component.

With regard to the AI component, the ethical parts of the deliverable will focus on the questions of trustworthiness, prevention of unlawful discrimination and bias, and explainability. In doing so this deliverable will address, and build upon, the "Ethical Guidelines for Trustworthy AI" issued by the European Commission's High-Level Expert Group on Artificial Intelligence.

3.Methods

The methodology used in this report was mostly based on desktop research, including reviews of current and pending legislation and academic commentaries or papers regarding the same. The legal analysis undertaken by UNIVIE has been conducted primarily on EU law. In addition to desktop research, UNIVIE consulted with individual partners' legal departments and distributed a questionnaire regarding national data protection laws to individual partners. The answers UNIVIE did receive were incorporated into this report and can be reviewed as Annex 1 to this Deliverable. The Patient Public Advisory Board was consulted, in particular for input on the ethical framework and to discuss the key ethical challenges that OPTIMA will face from a patient perspective.

4.Legal and Ethical Framework

In order to fulfill OPTIMA's goals of developing the first interoperable European real-world oncology data and evidence generation platform and decision support tools, the project will draw on a large volumes of real-world patient data now available through Electronic Health Records (EHRs) across Europe. Data from claims, national registries, clinical trials or other research projects including observational studies will also be used by the platform's decision support tool. Prospective data will also be collected during the project as part of WP3. The project will analyze these records and use Artificial Intelligence (AI) algorithms to improve existing medical guidelines for cancer treatment and diagnosis.

Numerous legal and ethical issues apply to OPTIMA's use of a large number of patient medical records and the use of AI in assessing those records and improving diagnostic and treatment tools. On an EU-level, the main pieces of legislation that will apply to OPTIMA's activities include data protection laws and laws governing the development and marketing of medical devices in the European Union.

With respect to the applicable ethical issues raised by OPTIMA's activities, these include the processing of large amounts of health data, the collection of prospective data in WP3, and the development of the AI component of the project. Ethical requirements for the project stem from key documents from the field of healthcare ethics, such as the Declaration of Helsinki, and from key guidelines on the use of trustworthy AI.

The sections below will discuss the individual legal and ethical requirements applicable to the OPTIMA project and, together with the DPIA and other Work Package 2 Deliverables, will serve as a guideline for OPTIMA members during their work on the project, including the platform design.

a. Legal Framework

i. Legal Concepts under GDPR

The first piece of legislation we will address is the GDPR – which applies to any entity processing personal data, which includes patient medical records. The GDPR distinguishes between entities who make decisions about, or can influence what is done with the personal data, and why (controllers) and those who simply follow the controllers' instructions with respect to the personal data processing (processors). The GDPR assigns those two groups different responsibilities and liabilities.

After introducing the "who" and "what" – that is, entities processing data and the concept of personal data itself – we will provide a brief overview of the GDPR's relevant provisions. Specifically, the idea that any personal data processing requires one processing the data to have a legal basis, conditions under which the data can be used or reused (purpose limitation), the principles of data minimization, storage limitation and data security, and the rights the GDPR gives to data subjects to control their own data.

1. Personal data, data concerning health

The GDPR governs the processing of "personal data,"[1] which is defined as *any information relating to an identified or identifiable natural person (data subject). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*.[2]

The Court of Justice of the European Union ("CJEU") has made clear that term "identified or identifiable" is to be interpreted very broadly. In Breyer case[3] the CJEU stated that "it is not necessary that information alone allows the data subject to be identified" in order to treat it as personal data. In fact, "to determine whether a person is identifiable, account should be taken of all means likely to be used either by the controller or by any other person to identify the said person." That is, data can still be considered personal data if someone is able to, even with significant additional effort, piece together different pieces of information (including the data in question) to identify an individual.

Under the GDPR, electronic health records, medical images, clinical notes, etc. – *i.e.*, data concerning health – which partners will process to complete their work on the OPTIMA project - certainly qualify as personal data, but those data also fall under a special category of personal data that receives additional legislative protection. Specifically, Article 9 of the GDPR begins with a broad prohibition on processing special categories of data, including genetic data and data concerning health and then carves out specific instances in which such processing is permissible (*i.e.*, where the prohibition does not apply); such as where the data subject has given consent. These specific instances will be

[1] Art 3 GDPR provides that the GDPR applies to data processing activities by organizations within the EU and data processing activities relating to data subjects situated in the EU.
[2] Art 4(1) GDPR
[3] Case C-582/14 Patrick Beyer v Bundesrepublik Deutschland [2016] ECLU:EU:C:2016:779

discussed later as the "legal bases" which OPTIMA partners must satisfy/rely on in order to process data concerning health.

Data concerning health means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status[4]. As part of the risk-based approach of the GDPR, this type of data needs to be treated with greater care because collecting and using it is more likely to interfere with the data subject's fundamental rights. Therefore, research projects, which intend to process sensitive data will need to satisfy stricter conditions as well as a higher level of protection for processing data lawfully.

2. Data controllers and processors and "Article 26 and 28 Agreements"

a) Data Controllers and Joint Controllers

The concepts of data controller and data processor presuppose the existence of data processing, which is defined under Article 4(2) if the *General Data Protection Regulation* as:

> Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

The legal definitions of data controller and data processor can be found under Articles 4(7) and 4(8) of the *General Data Protection Regulation* respectively. Article 4(7) defines the term **"data controller"**:

> the natural or legal person, public authority, agency or other body which, alone or jointly with others, *determines the purposes and means of the processing of personal data*; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Under Article 26, several operators may together determine the purpose and means of the data processing. This is referred to as a **Joint Controllership**. Importantly, a joint controllership does not mean that each member has an equal level of responsibility for determining the purposes and means of data processing.[5]

There is a low threshold for finding a controllership.[6] The Guidelines provided by the European Data Protection Supervisory Authority, for instance, interpret "data controller" very broadly. Those guidelines state that "a 'general' level of complementarity and unity of purpose could already trigger a situation of joint controllership, if the purposes and (essential elements of the) means of the processing operation are jointly determined".[7] According to the European Data Protection

[4] Art 4(15) GDPR
[5] European Data Protection Supervisor, 'Guidelines 07/2020 on the concepts of controller and processor in the GDPR – Version 2.0' (7 July 2021) 20.
[6] See Lee A. Bygrave and Luca Tosoni, "Article 4(7). Controller" in Christopher Kuner et al (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press, 2020) 145, 151-2.
[7] European Data Protection Supervisor, 'EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725' (7 November 2019) 23.

Supervisor's interpretation of the Court of Justice of the European Union case law,[8] a legal entity does not need to have access to personal data to still be considered a controller. The CJEU considers that it is enough that "a natural or legal person … exerts influence over the processing of personal data, for his own purposes, and … participates, as a result, in the determination of the purposes and means of that processing".[9] The European Data Protection Supervisory Authority also considers that:

> An entity does not need to have access to personal data to be considered a controller. It is enough if it determines the purposes and means of processing, has influence on the processing by causing the processing of personal data to start (and being able to make it stop), or receives the anonymous statistics based on personal data collected and processed by another entity.[10]

The European Data Protection Supervisory Authority deems one can exert this "decisive influence" over the purpose and means of processing by reaching a common decision, or converging decisions that complement one another, having a tangible impact on determining the purpose and means of processing.[11] "Influence" may manifest in several forms, in the past the CJEU has determined that the administrator of a Facebook fan page determined jointly the purpose and means of data processing with Facebook, because of its definition of parameters of processing *i.e.* determination of "the target audience and the objectives of managing and promoting its activities".[12] Similarly, embedding a Facebook "Like" button on a third party website, similarly meant that the third party concerned determined jointly the means and purposes of processing with Facebook because it had a decisive influence in collecting and transmitting the data from the visitors of its webpage to Facebook.[13]

However, this common decision or converging decision must relate to the processing of data, it cannot relate to "other aspects of the commercial relationship between the parties".[14] Other factors that might tend to indicate that a party as a controller include where the party:[15]

- Is appointed by a legal act as a controller.
- Decides what personal data will be collected and processed.
- Determines the categories of data subjects whose data will be processed.
- Determines whether and to whom the personal data will be disclosed.
- Determines the storage duration of the personal data.
- Has complete autonomy regarding the processing of personal data
- Benefits from, or has an interest in, the data processing.[16]

[8] Ibid 10 referencing *Jehovan todistajat* (Case C-25/17) (Court of Justice of the European Union, ECLI:EU:C:2018:551, 10 July 2018) [68]-[72]; *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH* (Case C-210/16) (Court of Justice of the European Union, ECLI:EU:C:2018:388, 5 June 2018); *FashionID & Co.KG v Verbraucherzentrale NRW eV* (Case C-40/17) (Court of Justice of the European Union, ECLI:EU:C:2019:629, 29 July 2019); *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* (Case C-131/12) (Court of Justice of the European Union, ECLI:EU:C:2014:317, 13 May 2014) [28], [41].
[9] *Jehovan todistajat* [68]; see also *FashionID & Co.KG v Verbraucherzentrale NRW eV* [68].
[10] See also European Data Protection Supervisor, "EDPS Guidelines on the concepts of controller" (n 3) 10.
[11] European Data Protection Supervisor, 'Guidelines 07/2020 on the concepts of controller and processor in the GDPR – Version 1.0' (2 September 2020) 3.
[12] *Wirtschaftsakademie* [36]
[13] *FashionID* [77]-[79].
[14] European Data Protection Supervisor, 'Guidelines 07/2020 - Version 2.0' (n 1) 19.
[15] European Data Protection Supervisor, 'Guidelines 07/2020 – Version 1.0' (n 7) 46-8.
[16] Mutual benefit may occasionally be a relevant factor in deciding that two parties are joint controllers, see ibid 19.

b) Data Processor

Meanwhile, Article 4(8) defines the term **"data processor"** as "a natural or legal person, public authority, agency or other body which *processes personal data on behalf of the controller*".

The data processor must be legally separate from the controller. As such, an employee, processing personal data at the behest of an employer, is not considered a data processor. Nonetheless, a controller may processes personal data themselves, in which case there would be no data processor involved within the meaning of Article 4(8).

As such, where processing occurs only under the instruction of another party, especially where these instructions are stipulated in a contract, the party is likely a data processor. Data processors might also make autonomous decisions about "non-essential means". This refers to the practical implementation of the data controller's purposes and means of data processing. This might include deciding the particular hard- or software to be used, or the security measures to be taken.[17]

c) What are Legal Implications for Controllers and Processors?

Under Article 82(1) of the GDPR, an aggrieved data provider has a right to compensation where their rights under the GDPR have been infringed. Data controllers will incur a relatively higher degree of liability than data processors. This is because processors will only be liable for breach of GDPR obligations specifically directed at processors, or where it has acted outside of the lawful instructions of the controller established in the contract. As such, data processors may be able to escape liability by (successfully) claiming that they were merely carrying out the instructions of the controller.

Under Article 82(4) where there is more than one controller or processor that is responsible for the wrongdoing, they may each be liable for the entire damages sought by the data subject. However, under Article 82(5) the data controller or processor that has paid the entire amount of the damages to the data subject, in compensation, shall be entitled to compensation from the other processors or controllers involved in the data processing that gave rise to the damages.

Importantly, according to the rulings of the CJEU, a joint controller will only be liable for the parts of the data processing where they were involved in making a co-decision. As such, they will not be liable for the parts of the data processing over which they had no influence.[18]

d) What is the Importance of Article 26 and Article 28 Agreements?

Under the OPTIMA Grant Agreement (Task 2.4), the consortium has committed to ensuring that agreements mentioned under Articles 26 and 28 of the GDPR are in place before personal data is shared within the consortium. These agreements will establish the data protection roles within the consortium, identifying each OPTIMA beneficiary as either a data controller, joint controller, or data processor. Importantly, these agreements must reflect the reality of each beneficiary's legal position. As such, these agreements do not give OPTIMA beneficiaries the option to choose whether they would like to be a data controllers, joint controller or processor. The reality of the situation will supersede the terms of the agreement, if the agreement does not accurately reflect any beneficiaries data protection role.[19]

[17] Ibid 3, 13-4, 46-8.
[18] *Fashion ID* [99].
[19] See eg. Christopher Millard and Dimitra Kamarinou, "Article 26 Joint Controllers" in Christopher Kuner et al (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press, 2020) 582, 587.

The GDPR refers to two types of agreements that must be reached among the data controllers and data processors. Firstly, the agreements referred under Article 26 for joint controllers, these will establish how their responsibilities for compliance with the GDPR will be apportioned between them. This include responsibilities relating to the exercise of rights by data subjects. This arrangement should establish a contact point for data subjects. Under Articles 26(2), (3) the essence of the agreement must be made available to the data subject, who may, regardless of what is mentioned in the agreement, bring a claim for all damages against either of the controllers. These agreements ensure that, even in spite of complex controllership arrangements, at least one controller will be responsible for the obligations expected of controllers under the GDPR.

Secondly, the agreements referred to under Article 28 govern arrangements between data controllers and data processors. These agreements will establish certain obligations on the data processor, including that the data processor:

I. Processes data only on the documented instructions of the data controller.
II. Ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality
III. Assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights.
IV. At the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data

Article 28 obliges controllers to "use a processor who is reliable and can demonstrate the required technical knowledge, expertise and resources to provide adequate guarantees".[20] It also allows processors to sub-contract certain processing tasks to other parties, under certain conditions with the controller's permission.

The potential structure of a consortium wide Article 26/28 Agreement is currently being negotiated with the individual OPTIMA partners. UNIVIE has drafted a legal opinion recommending a specific contract structure. Data providers who simply provide data for the project and are not parties to the Consortium Agreement will not be signatories.

ii. General Requirements of Personal Data Processing

1. Principles of Personal Data Processing

So far, we have discussed what kind of data the GDPR covers (personal data, including health related data) and who the actors are that the GDPR intends to regulate (controllers, processors).

Article 5 of the GDPR articulates certain general principles of data protection. This section will address most of those important principles that controllers and processors must observe when processing personal data. Namely, we will discuss the concept of a legal basis – a prerequisite for personal data processing to be legal; the purpose of the data processing; and the concepts of data minimization, storage limitation and confidentiality, security and integrity.

[20] Christopher Millard and Dimitra Kamarinou, "Article 28 Processors" in Christopher Kuner et al (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press, 2020) 599, 605.

a. Lawfulness of Personal Data Processing

In order to lawfully process personal data, one must point to a legal basis under either Article 6 and/or Article 9 of the GDPR. If OPTIMA partners seek to process only personal data (*e.g.*, names and addresses of individuals), identification of an Article 6 basis is sufficient. If a partner seeks to process health related data, which falls under the definition of a "special category" of personal data, partners must also seek a legal basis in Article 9.[21] OPTIMA partners may be able to rely on a number of different legal bases under those two Articles:

Legal basis for processing of personal data for building and training of OPTIMA platform

Consent. Explicit consent of the data subject is a proper legal basis for processing personal data, including special categories thereof, under both Articles 6(1)(a) and 9(2)(a).[22] Note that consent to data processing is distinct from consent to participate in research and/or medical research or studies (as may be required under the Clinical Trial Regulation, for example). OPTIMA can rely on consent as a basis for prospective data – that is data collected during the project – because we can actively obtain consent as part of the data collection process

Consent may also be relied on as a legal basis for retrospective data[23] in some cases. In order for the consent to be a valid basis for already-collected data, the consent obtained must be broad enough that its scope includes research such as that conducted in OPTIMA. Article 6(4) of the GDPR provides additional conditions which must be taken into account by the controller when processing personal data for a purpose other than that for which the personal data were originally collected. The principle of purpose limitation will be discussed later.

Research exemptions under national or EU law. However, for many retrospective data sets, consent forms may either not be available, or not be broad enough to cover the secondary processing[24] we need to do in OPTIMA. Where consent is not available, we need to identify a different legal basis to process health related personal data under Article 6 and 9.[25]

Article 9(2)(j) together with Article 6(1)(e) or (f) will be the most likely option. Article 6(1)(e) permits the processing if its undertaken as part of the performance of a task in the public interest, while Article 6(1)(f) permits the processing if necessary for legitimate interests pursued by the controller, so long

[21] *See, e.g.*, ICO, "Special category data' (*Information Commissioner's Office)* <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data>

[22] Unless Member State law states that explicit consent still cannot lift Article 9(1)'s general prohibition. "This is the case in some EU countries for genetic tests or other specific medical examinations." Hansen *et al.*, European Commission, DG Health and Food Safety, *Assessment of the EU Member States' rules on health data in the light of GDPR*, at p. 58 (citing van Veen, 2018) < https://ec.europa.eu/health/system/files/2021-02/ms_rules_health-data_en_0.pdf>

[23]Data that was collected prior to the commencement, and outside the scope, of OPTIMA and which will be re-used for the project, such as data contained in Electronic Health Records or in national disease registries

[24] "Secondary use" or "secondary processing" is the use of retrospective data by a third party (not the original data collector) or by the same party for a different purpose.

[25] Note Article 9 contains additional exceptions, which are not likely to apply in OPTIMA. However, at least Article 9(2)(b) is worth mentioning in the event that some partners' national laws permit its use. Article 9(2)(b) allows one to process health related personal data for carrying out one's duties under social security law as set out in Member State or Union law. This may apply to processing for research by public sector bodies if the administration of healthcare services in a partner's country is set out within wider social security law there. Article 9(2)(i) will also be discussed later in the context of device approval. However, it may also serve as a legal basis for the general research processing in OPTIMA in the special case that a specific member state has officially declared cancer research as a matter of public interest in the area of public health, pursuant to national law.

as those interests are not overridden by the interests or fundamental rights and freedoms of the data subject. Article 9(2)(j) concerns data processing for scientific or historical research by both public and private sector organizations. It permits processing where it is "*necessary for…scientific…research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law….*" Reading closely, the exception is available only if such processing for research purposes is provided for in Member State or EU law.[26]

When the GDPR was drafted, it was envisioned that member states would make use of this implicit invitation[27] to implement national laws allowing secondary use of health related data for research purposes, if such laws were not already in place. The GDPR also permits[28] Member States to pass laws allowing researchers to ignore certain rights the GDPR grants data subjects[29] in limited contexts. We asked partners whether their respective countries had made use of this permissive clause (see additional subsection, below).

The responses we received varied widely. According to the responses, only the Netherlands, UK and Luxembourg had laws clearly permitting secondary use for medical research purposes without the presence of consent. We have also concluded that Estonia, Germany, Spain, and Italy (and possibly France and Belgium) also have national laws, which offer a legal basis for using health related data for research without consent.[30] The Commission's 2021 DG Health and Food Safety Report entitled *Assessment of the EU Member States' rules on health data in the light of GDPR* at pages 62 – 63, 66-67, 71 provides some additional background on the national legislation of Estonia, Germany, Spain and Italy.

This apparently varied patchwork of national laws is consistent with the findings of the Commission's report:

> It is clear from responses provided by the correspondents that the Member States have not implemented such legislation in a homogenous way, resulting in a complex and fragmented landscape for researchers to navigate. Consequently, differences between Member States in the way the GDPR is implemented and interpreted in the area of scientific research has made data exchange between Member State and EU bodies for research purposes difficult and in some cases highly technical.[31]
>
> [T]here are divergences in the application of the GDPR in the context of health research…It is evident there is a variance of safeguards [under Article 89(1)] and lawful basis leading to confusion and technical difficulty when conducting inter-jurisdictional research.[32]

[26] *See, e.g.*, Staunton, C., Slokenberga, S. & Mascalzoni, D. The GDPR and the research exemption: considerations on the necessary safeguards for research biobanks. *Eur J Hum Genet* 27, 1159–1167 (2019). https://doi.org/10.1038/s41431-019-0386-5

[27] Article 9(4) also permits Member States to introduce further conditions…with regard to the processing of genetic data, biometric data or data concerning health.

[28] *See* GDPR, Article 89(2).

[29] Under GDPR Articles 15, 16, 18, and 21.

[30] Hansen *et al.*, European Commission, DG Health and Food Safety, *Assessment of the EU Member States' rules on health data in the light of GDPR,* at pp. 62 – 63, 66-67, 71 < https://ec.europa.eu/health/system/files/2021-02/ms_rules_health-data_en_0.pdf> at

[31] *Id.* at p. 58.

[32] *Id.* at p. 73.

In addition to the presence of an EU or national law permitting the secondary use, reliance on Article 9(2)(j) as a legal basis requires additional technical safeguards to be in place in order to protect data subjects' rights. The GDPR's Article 89(1) lists those requirements. Specifically, that section requires that "technical and organisational measures [be] in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that [the research] purposes can be fulfilled in that manner…"

Legal basis of processing of personal data during the mandatory device approval and post-market approval processes

For personal data processing in the course of OPTIMA's application for approval of the device under the MDR Article 6(1)(c) ("processing is necessary for compliance with a legal obligation to which the controller is subject) together with Article 9(2)(i) can provide another potential legal basis. The latter subsection permits the processing of data concerning health where it is "necessary for reasons of public interest in the area of public health, such as…ensuring high standards of quality and safety of health care and of medicinal products or medicinal devices, on the basis of Union or Member State law…" It is important to note that the processing here must be *mandatory*, that is, it must be required by the MDR or IVDR, as applicable.

It is not likely that data processing for post market approval surveillance will occur within the scope of the OPTIMA project, Nonetheless, we found it worth mentioning that with respect to post market approval surveillance activities, although they may be

> based on an EU directive (2010/84/EU), that directive does not state that personal data may be processed for this purpose. In the absence of member state legislation allowing authorities or even pharmaceutical companies to process personal data for pharmacovigilance, these data need to be either anonymised or their processing based on consent.[33]
>
> Member States can take, and have taken, different routes concerning post market surveillance (PMS) and serious incidents with medical devices. As also for PMS for medical devices, soon to be fully regulated under Regulation 2017/745, there is no guidance on the EU level how such data can be collected at the national level…Regulation 2017/745 states in section 10 of article 87 that Member States shall take appropriate measures to encourage and enable health care professionals to report serious incidents with the devices…Some Member States, such as the Nordic countries and Greece have instituted systems for pharmacovigilance or PMS of devices, often via registries…[34]

i. National Data Protection Legislation and/or National Research Legislation

As discussed in above subsection, in addition to EU-wide legislation governing data protection, several individual EU member states have their own rules governing the processing of personal data, including data concerning health. Some of these laws, which we will call "implementing laws", were issued in response to the GDPR (or its predecessor's) "opening clauses" – that is, clauses where the

[33] ." Hansen *et al.*, European Commission, DG Health and Food Safety, *Assessment of the EU Member States' rules on health data in the light of GDPR*, at p. 48
[34] *Id.* at pp. 48-49.

GDPR states it will permit member states discretion in passing additional legislation to address a specific issue.

Much of the processing that will occur during the OPTIMA project falls under the category of "secondary use". That is, the data were not originally collected with the purpose of being used for the OPTIMA project. Instead, the data were collected either during a routine clinical visit, or as part of a clinical trial, or perhaps are part of a disease registry. Under the GDPR Articles 5(1)(b), 9(h), (i), (j), and Article 89, the legal bas(es) we may rely on for such further processing will usually depend on the existence of specific national implementing laws, permitting such further processing in certain contexts, such as for research. Where such national legislation does not exist, we will likely have to rely on consent as the legal basis for the further processing.

The GDPR (Article 89(2)) also permits Member States to allow researchers to derogate from certain data subject rights granted by the GDPR (*e.g.*, GDPR Articles 15, 16, 18, and 21). We also asked partners whether their country's national law took advantage of this permission and included such derogations.

We sent OPTIMA partners a questionnaire in order to assist us in determining what such national data protection laws might exist in partner member states. Below is a table reflecting responses we received:

Country	**Code or Law**	**Content**	**Potential Consequences for OPTIMA**	**Responding Partners**
Netherlands	Clause 24 of the UAVG	Permits processing of special categories of personal data if the research serves a public interest, requesting explicit consent involves a disproportionate effort *and* data subjects' rights will not be disproportionately harmed	OPTIMA partners in the Netherlands can access and provide data without relying on consent as a legal basis. Some flexibility with respect to data subject rights. Even personal data collected during treatment do not necessarily require consent for processing if certain conditions are met.	Maastricht University (UM), Erasumus Universitair Medisch Centrum Rotterdam (ERM), Stichting European Association of Urology Foundation (EAU)
	Clause 28 of the UAVG	Permits the processing of genetic data without consent if "an important medical interest prevails" (e.g., informing relatives about hereditary diseases) or if the processing is necessary for scientific research that serves the public interest		
	Clause 44 of the UAVG	Articles 15, 16, and 18 of the GDPR may be disregarded if the processing is out for scientific research and if the personal data are used exclusively for scientific purposes		
	Dutch Civil Code 7:457	Creates an exception to the obligation to keep patient data secret in the course of a medical treatment (as required in 7:457 of the Dutch civil code) if the information is being used for scientific research without consent if *either* the privacy of the patient is not disproportionately harmed *or* the data is provided in such a way that it can reasonably be prevented from being traced back to the individual natural person. The research must also serve the public interest, the data must be critical to the investigation and the patient must have not explicitly objected.		

France	No exceptions provided; referred to Art. 9(2)(i).	General information provided: In response to the question: "what are the national implementations of the opening clause in Art. 89(2) GDPR?" it was stated that the French DPO can grant a waiver when one cannot obtain a data subject's consent. It was also mentioned that Law no. 2018-493, dated 20 June 2018 amended France's Data Protection Act to bring national law in line with the European legal framework but no details provided. Each clinical study must be approved by a committee for the protection of subjects per the law on bioethics 02 August 2021; Article L1123-1 through L1123-14. For genetic data the French Public Health Code states specific consent is needed.	Not clear whether any exceptions under Art. 9(2)(j); approval of committee may be required; if processing genetic data consent necessary	Insitut Cancerologie de l'Ouest (ICO)
Luxembourg	Luxembourg Data Protection Act of 1 August 2018, Art. 65	Special categories of personal data can be processed for research purposes "if certain conditions are met: (1) appointment of a DPO; (2) performance of a DPIA; (3) anonymization or pseudonymisation, "or other operational measures guaranteeing the data collected…cannot be used to adopt decisions or take actions concerning data subjects"; (4) use of a 3d party for anonymization or pseudonymization; (5) encryption of personal data in transit and at rest; (6) use of technology reinforcing protection of private lives of data subjects; (7) use of access restrictions to personal data w/in controller; (8) use of log file; (9) promoting awareness of staff involved; (10) regular evaluation of T&O measures; (11) prior DMP; (12) adoption of sector specific codes. Controller relying on Art. 9(2)(j) must document and justify any exclusion of one or several of above mentioned measures for each project conducted for scientific research purposes.	OPTIMA partners in Luxembourg may access and provide data without relying on consent as a legal basis but must comply with a lengthy list of internal requirements aimed at protecting data subject rights. Some flexibility with respect to data subject rights.	Information Technology for Translational Medicine (ITTM)
	Luxembourg DP Act (no section mentioned)	Permits derogations from GDPR's Art. 15 (right of access); 16 (right to rectification); 18 (right to restriction); and 21 (right to object) where the exercise of such rights is likely to render impossible or seriously impair the achievement of the scientific research purpose but Art. 65 of the Luxembourg DP Act's requirements must be met.		
Germany	BSDG, §§3, 22, 27, 28	No content details provided	No content details provided	Smart Reporting GmbH (Smart Reporting)
Sweden	Swedish Ethics Review Act, Lag (2003:460), §§3, 6, 9	Ethical approval is required by Swedish Ethical Review Authority, which applies to any research containing processing of special categories of personal data. Often the committee will require consent for approval.	Not entirely clear whether the Högskolelagen (1992:1434), §2 permits OPTIMA partners located in Sweden to rely on Art. 9(2)(j) without the need for consent. This may be irrelevant as stated by UU as the Swedish Ethical Review Board tends to	Uppsala University (UU)
	Högskolelagen (1992:1434), §2	Officially declares University research as a task carried out in the public interest		

			require consent for approval.	
UK	UK GDPR Article 9(2)(j), UK Data Protection Act 2018 ("DPA 2018"), Schedule 1, Condition 4 and Section 19 of DPA 2018	Special categories of personal data may be processed for research where one can (1) demonstrate that the processing is necessary for research purposes (it must be a reasonable and proportionate way of achieving the research purpose and you may not have more data than you need); (2) comply with the safeguards of Article 89(1) GDPR and Section 19 of 2018 DPA; and (3) demonstrate the processing is in the public interest	OPTIMA partners in the UK can access and provide data without relying on consent as a legal basis.	The University of Oxford (UOXF)
Spain	None provided	No content details provided. Referred to Spanish website: https://www.aepd.es/en/guias-y-herramientas/guias and https://www.aepd.es/documento/nota-equivocos-biometria-en.pdf Websites referenced give no information on Spain's national GDPR implementing laws However, it was stated that "[r]esearch legislation establishes no []special treatment for research data."	No content details provided	GMV Soluciones Globales Internet SAU (GMV-SGI)

ii. Gathering of consent required for collection of prospective data in WP3

Collection of prospective data within the framework of WP3 requires that it will be based on a valid consent for (i) participation in medical research and for (ii) processing personal data under the GDPR. With regard to the latter, a number of legal requirements defined in the GDPR must be met for such consent to be considered lawful.

First, as the collected data will include health data, the consent must qualify under both art. 6(1)(a) and art. 9(2)(a) GDPR simultaneously, i.e. it must be explicit. In practical terms, the patient must clearly state that they agree to their data, including their health data, be processed within OPTIMA. The scope of processing, its purposes and entities involved must be clearly defined and communicated to the patient, along with additional information defined in art. 13 GDPR. The consent form must be in a language understandable to the patient – with regard to both the choice of language (English, Dutch, French, etc.) as well as the complexity of the information communicated.

Second, for each piece of data collected via a consent form, it must be as easy for the patient to withdraw the consent, as it was to give it. This means, that any bureaucratic hurdles aimed at discouraging patients from withdrawing consents are illegal under the GDPR and expose entities involved to liability.

Third, consent for processing personal data within OPTIMA (and/or similar further research) must be distinct from other consents/consents for other purposes. Even if connected to the consent for participation in medical research ("ethical consent", see above), the two must be distinguishable from each other.

Fourth, consent must be freely given, free from duress or any other form of conditionality.

For the purposes of accountability, the controller must retain proof that patients have given appropriate consents (usually signed consent forms).

iii. Status of retrospective data and its compliance with EU legal framework

As discussed in the *Lawfulness* section, above, OPTIMA partners will primarily be able to rely on one of two legal bases in processing retrospective data that is in engaging in secondary processing. The first is consent, the second is GDPR Article 9(2)(j)'s exception for scientific research per EU or national law.

If OPTIMA partners choose to rely on consent, they should ensure the scope of the original consent that is provided by data subjects is broad enough to cover the processing the partner will be doing as part of OPTIMA. If partners choose to rely of Article 9(2)(j), partners should take care to comply with Article 89(1) of the GDPR and to identify the national (or EU) law on which they rely and comply with any additional provisions contained in those laws. UNIVIE is available to assist if guidance is required regarding whether the original consent gathered is sufficiently broad for use in OPTIMA.

b. Purpose Limitation

We have already discussed the differences between primary and secondary use of data. To review, primary use of data occurs when a researcher uses personal data that was directly collected for the purpose of that research. Secondary use occurs when a researcher re-uses data that was originally collected for another purpose (*e.g.,* during the course of clinical care, for a different study, or as part of a national disease registry).

The second principle of data processing under GDPR's Article 5 is the "purpose limitation." This principle require that personal data be "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes".

Article 6(4) also requires that for secondary use, the purpose of the data processing be compatible with the initial or original purpose for which the data was collected. That subsection requires controllers, "in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected" to take into account 5 factors, including the "link between the purposes for which the personal data have been collected", the context in which that data was collected, whether the data includes any special categories under Article 9, and the "possible consequences of intended further processing for data subjects".

If the further processing is for research, Article 5(1)(b) of the GDPR (and Recital 50) permits a presumption as to the purpose of the secondary use: the further processing will be presumed to be compatible with the initial purpose for which the data was collected so long as there are measures in place to ensure respect for the principle of data minimisation (discussed below).[35]

[35] *See* GDPR Articles 5(1)(b) and 89(1).

c. Data Minimisation

The third principle of data processing under GDPR's Article 5 is that of 'data minimisation', that is, personal data shall be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')".[36]

This principle aims to ensure controllers and processors do not collect and process more personal data than is necessary for to achieve the purpose of their processing. A corollary to this, of course, is that the personal data collected and processed must actually be relevant to the purpose of the processing; this means that where pseudonymisation can be implemented because identifying details of an individual are not relevant to the research purpose, such measures should be taken.

OPTIMA partners have already been made aware of, and addressed the Data Minimisation Principle in the DPIA, submitted as Deliverable 2.1. For instance, the federated learning model minimizes the amount of direct contact between OPTIMA members and raw personal data. This is because, from the analytical queries sent from the OPTIMA centralized platform to the data providers, the data providers will return anonymous statistical data. Furthermore, when mapping data to the OMOP structure, the members of the Work Package 6 team are provided pseudonymised data by the data providers, and will avoid handling personal data, which is not useful data to OPTIMA. Regarding non-OMOP unstructured data, such as genomic and image data, Owkin, an OPTIMA partner in Work Package 7, aims to enable the training of AI algorithms in a federated way. This means that, as with OMOP data, OPTIMA consortium members can receive anonymous statistical data in response to their queries made regarding non-OMOP data in the federated network.

As far as the centralized database is concerned, pseudonymisation is also a critical feature. Any data that is transferred to the centralized database must be pseudonymised by the data provider beforehand. Work Package 6 will provide its own risk assessment regarding the possibility of re-identification from the pseudonymised data sets that are shared to the OPTIMA consortium.

d. Storage Limitation

Article 5(1)(e) of the GDPR sets forth the storage limitation principle. That subsection provides that personal data should be "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for…purposes in the public interest, scientific…research purposes…in accordance with Article 89(1)…"

As described in the DPIA (D2.1), while a definitive storage limitation has not been decided on yet, OPTIMA currently plans to comply with this principle by limiting the storage duration of prospective data collected during the OPTIMA project to the end of the OPTIMA project.[37] Deviations from this principle should, generally, be reflected in the consent that is obtained from the data subjects, where consent was the legal basis for processing the data. Where storage period is expired, it will be the responsibility of the clinical partners to erase the data.

[36] GDPR Article (5)(1)(c).
[37] Individual clinical partners may have different arrangements regarding storage duration after the end of the OPTIMA project. For instance, the Erasmus Universitair Medisch Centrum Rotterdam, when gathering informed consent from its data subjects, asks that data collected is stored for a period of 15 years. They may also ask, as part of informed consent for an extended period of 50 years of storage.

The intended storage duration of data in the centralized network is not currently confirmed and will depend on, among other things, the building and training of the AI component of the OPTIMA platform. However, it is intended that this will be clarified in the update to the DPIA, to be provided in month 50 of the project.

e. Confidentiality, Integrity and Data Security

Article 5(1)(f) sets forth the last principle of data protection – that of data security. The subsection states that personal data shall be, "processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised and unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."

Article 32 provides some additional guidance regarding what types of measures a controller can implement to ensure security of processing:

> 1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:
>
> a) the pseudonymisation and encryption of personal data;
>
> b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
>
> c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
>
> d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

To the extent OPTIMA's centralized node at the Helmholtz Centre makes use of cloud computing, partners should be particularly conscious of potential risks regarding lack of control over personal data, and insufficient transparency of the architecture and uncertainty concerning the transfer of personal data to cloud providers established outside of the EEA. The Article 29 Data Protection Working Party's *Opinion 5/2011 on Cloud Computing* (WP 196 2012) provides additional information regarding these potential risks and recommendations to ensure GDPR compliance.

f. Brief Summary/Checklist

In summary, a checklist of data protection requirements to be used by partners when processing any personal data in OPTIMA:

- At all stages of data processing adhere to the principles of personal data contained in Article 5 GDPR
  - Lawfulness of processing (Article 5(1)(a) GDPR).
  - Purpose limitation (Article 5(1)(b) GDPR)
  - Data minimisation (Article 5(1)(c) GDPR)
  - Accuracy of processing (Article 5(1)(d) GDPR)
  - Storage limitation (Article 5(1)(e) GDPR)

- Confidentiality, integrity and security (Article 5(1)(f) GDPR)

- OPTIMA partners must have a legal basis for processing personal data (data concerning health), which is likely to be based on Article 9(2)(a) GDPR (consent) or Article 9(2)(j) GDPR (research exemption) + a national implementing law

2. Data Subject Rights

In addition to conferring obligations on controllers and processors, the GDPR grants data subjects certain affirmative rights in Articles 12-23. These will be relevant for OPTIMA especially in the context of the currently-under-negotiation Article 26 and 28 Agreements insofar as controllers and processors must ensure that data subjects have viable and straightforward ways to exercise these rights. This means Article 26 and 28 agreements should include information regarding who will ensure data subjects are made aware of their rights and who data subjects may contact in order to exercise those rights. Briefly those articles confer the following rights on data subjects:

- **Article 12**: Requires the controller to provide the data subject with clear and concise information regarding the rights afforded them by GDPR Articles 13 through 22 and 34. This Article also requires the controller to "facilitate the exercise of data subject rights" including the provision of information requested by the data subject.

- **Article 13**: Provides a list of information the controller or processor must provide a data subject, when collecting personal data directly from the data subject. A non-exhaustive list of that information includes: the purposes of the processing and the legal basis for it, the recipients or categories of recipients of the personal data, whether the controller intends to transfer the data to a third country, the period of data storage, the existence of the right to request access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability, the right to withdraw consent at any time, and the existence of automated decision making (such as with an AI program). In the case of a secondary processing, the controller is to inform the data subject of the further processing and of the other/new purpose for the secondary processing.

- **Article 14**: If the data was not obtained directly from the data subject, Article 14 provides a list of information which the controller must provide the data subject. This list is very similar to that of Article 13 and also provides that there are certain conditions in which this information need not be provided, such as if the data subject already has the information or if its provision "proves impossible or would involve a disproportionate effort, in particular for processing for…purposes in the public interest, scientific or historical research purposes…"

- **Article 15**: Permits data subjects to access all personal data and the ways in which it is being processed, including information about their rights under GDPR Chapter 3 and a copy of the personal data undergoing processing.

- **Article 16**: Allows data subjects to rectify inaccurate personal data.

- **Article 17**: Allows data subjects to demand a controller or processor erase their personal data in a variety of contexts.

- **Article 18**: Allows data subjects to request a restriction on processing of their personal data in certain cases.

- **Article 19**: Requires a controller to "communicate any rectification or erasure of personal data or restriction of processing… to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves a disproportionate effort."

- **Article 20**: Right of the data subject to receive a copy of his or her personal data in a "structured, commonly used and machine-readable format"

- **Article 21**: Allows a data subject to object to the processing of his or her personal data at any time including where the data is processed for scientific research purposes, "unless the processing is necessary for the performance of a task carried out for reasons of public interest."

- **Article 22**: Provides the data subject with "the right not to be subject to a decision based solely on automated processing…which produces legal effects concerning him or her or similarly significantly affects him or her." For OPTIMA the implication is that when implementing/using the AI aspect of the planned platform there always needs to be a human in the loop (unless the data subject has given explicit consent to the automated processing).

- **Article 34**: Requires the controller to communicate a data breach to the data subject if it is "likely to result in a high risk to the rights and freedoms of natural persons".

For our purposes. The Article 26 and 28 Agreements should identify which partners will be responsible for providing data subjects with the information required by Articles 12 through 14 and who those data subjects will contact in the event they wish to exercise their rights under Chapter 3. Partners should also consider how they apportion responsibility for compliance with possible data subject requests under this Chapter.

3. Transfers of Personal Data to Third Countries

The GDPR only permits transfers to third countries or to international organisations under certain conditions set forth in Chapter 5 of the Regulation.[38] For OPTIMA this means we must find a justification within that Chapter to transfers to and from the UK, Switzerland and the U.S.

For the UK and Switzerland this justification can be found in Article 45 of the GDPR, which permits transfers made on the basis of an adequacy decision without any additional authorization. Given the decisions by the European Commission, and the UK government, regarding the adequacy of data protection in both jurisdictions,[39] no new arrangements or added safeguards need be made at this time, regarding the transfer of data to and from the UK. Nonetheless, these adequacy decisions are not permanent, and the situation may not necessarily stay the same throughout the course of the OPTIMA project. Should this adequacy situation change during the OPTIMA project, Work Package 2 will reflect on the relevant legal implications this has on OPTIMA, in the second iteration of the Legal and Ethical Framework, in Month 20 of OPTIMA as Deliverable 2.4. More immediate assistance will be provided to the OPTIMA consortium members through the Legal and Ethical

[38] *See* GDPR Art. 44.

[39] *See* United Kingdom Department for Digital, Culture, Media & Sport, 'International data transfers: building trust, delivering growth and firing up innovation' (26 August 2021) <https://www.gov.uk/government/publications/uk-approach-to-international-data-transfers/international-data-transfers-building-trust-delivering-growth-and-firing-up-innovation>; see also Information Commissioner's Office, 'International transfers after the UK exit from the EU Implementation Period' (accessed 7 December 2021) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers-after-uk-exit/> .

Helpdesk, Task 2.3.

The Commission has also issued an adequacy decision with respect to Switzerland.[40] As with the UK, given this decision no new arrangements or added safeguards need be made at this time regarding the transfer of data to and from Switzerland.

Any potential controllers based in the UK or Switzerland, will be bound by those respective legal systems, which have been deemed as adequate to EU standards. Furthermore, they will be bound by the OPTIMA consortium and grant agreements, as well as controller agreements and, potentially, data sharing agreements and data processing accords. Overall, these will oblige said controllers to follow EU standards in data protection.

There is no adequacy decision with respect to the United States after the European Court of Justice's *Schrems II* ruling on 16 July 2020, which invalidated the European Commission's adequacy decision allowing firms to self-certify under the EU-U.S. Privacy Shield.[41] Instead, personal data transfers to and from the U.S. will likely need to be based on Standard Contractual Clauses under GDPR Article 46(2)(c)[42], or less likely Article 49(1)(a) or (d). We will only address the first possibility, below. Should this not be a feasible basis for third party transfers to and from the U.S., WP2 together with the relevant U.S. partners will identify an appropriate basis for the transfer under Article 47 or 49.

Article 46 sets forth the conditions for transfers by way of appropriate safeguards in the absence of an adequacy decision:

> 1. In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country … **only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available**.
>
> 2. The appropriate safeguards referred to in paragraph 1 may be provided for, **without requiring any specific authorisation from a supervisory authority**, by: (c) **standard data protection clauses adopted by the Commission** in accordance with the examination procedure referred to in Article 93(2); (d) **standard data protection clauses adopted by a supervisory authority and approved by the Commission** pursuant to the examination procedure referred to in Article 93(2);

There are thus two possibilities are offered to apply the additional appropriate safeguards: (1) through the use of Standard Contractual Clauses ("SCCs") adopted by the Commission or (2) through the use of SCCs adopted by a supervisory authority and approved by the Commission.

In the *Schrems II* judgement the Court highlighted that it is the responsibility of the data exporter and the data importer to assess whether the level of protection required by EU law is respected in the third country concerned in order to determine if the guarantees provided by the SCCs or the Binding Corporate Rules can be complied with in practice:

[40] Commision Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland < https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000D0518&from=EN >

[41] *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* (Case C-311/18) (Court of Justice of the European Union, ECLI:EU:C:2020:559, 16 July 2020).

[42] Binding Corporate Rules, under Article 47 are another option but those need to be approved by a "competent supervisory authority"

> That validity depends…on whether, in accordance with the requirement of Article 46(1) and Article 46(2)(c) of the GDPR, interpreted in the light of Articles 7, 8 and 47 of the Charter, such a standard clauses decision incorporates effective mechanisms that make it possible, in practice, to ensure compliance with the level of protection required by EU law and that transfers of personal data pursuant to the clauses of such a decision are suspended or prohibited in the event of the breach of such clauses or it being impossible to honour them.[43]

The European Commission updated its approved SCCs for third country transfers in June 2021.[44] In the context of OPTIMA use of these clauses will be the preferred way forward as their use does not require any specific authorization from the supervisory authority. The only drawback of the use of such clauses is that the set of SCCs must be adopted in their entirety and cannot be modified in any way.

4. Remedies, Liability and Penalties

The GDPR's enforcement provisions are in Chapter 8, Articles 77 through 84.

Articles 79, 82, 83 and 84 are relevant for OPTIMA's purposes.

Article 79 provides with the right to bring an action against a controller or a processor – that is "'the right to an effective judicial remedy against a controller or processor" but does not specify penalties.

Article 82 provides the right to compensation and liability – that is, the right to payment/compensation should the infringement of the data subject's rights have caused any material or non-material damage. Article 82 distinguishes between controllers and processors. Whereas a controller can become liable for the full extent of damages a data subject suffers, a controller will only be liable to the extent "it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller."[45]

Article 83 GDPR sets forth the 'General conditions for imposing administrative fines'. This Article applies to the provision of fines by supervisory authorities aimed at controllers and processors. However, this is not the only corrective action supervisory authorities can order. Article 58(2) provides supervisory authorities with additional options, such as issuing warnings or reprimands, ordering compliance with the data subject's requests, or issuing a temporary or definitive ban on processing.[46] If supervisory authorities do choose to impose a fine, it must be "effective, proportionate and dissuasive".[47] It must also take into consideration 11 factors aimed at indicating how culpable the controller or processor was in its infringement.[48] Fees have the potential to be significant – ranging

[43] CJEU Case C-311/18, 16 July 2020 ("Schrems II"), para 137.
[44] Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (c/2021/3972) <https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en>
[45] GDPR Art. 82(2).
[46] Additional options available to supervisory authorities can be found at GDPR, Article 58(2).
[47] Article 83(1) GDPR
[48] The complete list is:

> *(a)* ***the nature, gravity and duration of the infringement*** *taking into account … the number of data subjects affected and the level of damage suffered by them;*
> *(b) the* ***intentional or negligent character*** *of the infringement;*
> *(c) any* ***action taken by the controller or processor to mitigate the damage*** *suffered by data subjects;*
> *(d) the* ***degree of responsibility of the controller or processor*** *taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;*
> *(e)* ***any relevant previous infringements*** *by the controller or processor;*

up to 10 million Euro, or 2% of a company's worldwide annual turnover for infringements of Articles 8, 11, 25 to 39 and 42 and 43. Infringements of Articles 5, 6, 7, 9, 12 to 22, and 44 to 49 can result in administrative fines of up to 20 million Euro or 4% of a company's annual turnover.

Lastly, Article 84(1) GDPR on 'Penalties' requires Member States to also provide for administrative fines for infringements which were not mentioned in Article 83.

iii. Regulation 2017/745 (MDR) and Regulation 2017/746 (IVDR)

In the EU, a medical device is defined as "any instrument, apparatus, appliance, software, implant, reagent, material or other article intended by the manufacturer to be used, alone or in combination, for diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease and which does not achieve its principal intended action by pharmacological, immunological or metabolic means, in or on the human body" (medical device regulation [MDR] article 2).

Medical devices for *in vitro* diagnostic regulation (IVDR) are defined as "any device, a reagent, reagent product, calibrator, control material, kit, instrument, apparatus, piece of equipment, software or system, whether used alone or in combination that are intended to be used in vitro for the examination of specimens, including blood and tissue donations, derived from the human body with the purpose to bring information about a physiological condition, congenital physical and mental disabilities or for monitoring of patient treatment" (IVDR article 2).

Medical device software (MDSW in EU) can be regulated under the MDR or the IVDR, depending on the intended use of the SW and the source of the clinical data. The European Commission's MDCG 2019-11 guidance on software qualification and classification includes a decision tree for determining when MDSW is regulated by MDR or IVDR. The MDCG guidance also outlines which types of software are subject to MDR/IVDR. Unlike the US FDA, the EU does not have an official definition of clinical decision support (CDS) software. The intended use of the software, specifically its functions and features, will determine if and how it will be regulated. For example, in "Manual on Borderline and Classification in the Community Regulatory Framework for Medical Devices," example 9.4 provides an example of a software product that interprets guidelines and is not considered a medical device.

The software functions developed in OPTIMA that fall under MDR/IVDR are those that meet the definition of a medical device or IVD as described above. General computing functions or other software used in OPTIMA that do not meet the definition of a medical device/IVD or have been excluded from qualification as a device by MDCG 2019-11 are not subject to MDR/IVDR requirements. Section 7 of MDCG 2019-11 provides additional details regarding regulatory considerations for software products that consist of multiple modules, some of which have medical

---

(f) ***the degree of cooperation with the supervisory authority****, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;*
(g) ***the categories of personal data affected by the infringement****;*
(h) ***the manner in which the infringement became known to the supervisory authority****, in particular* ***whether, and if so to what extent, the controller or processor notified the infringement****;*
(i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;
(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and
(k) ***any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement****.*

device functionality and others of which do not have medical device functionality. Medical devices follow a risk classification based on potential consequences for the patient if the device does not perform as intended. For stand-alone MDSW that is under the scope of MDR, it is subject to classification Rule 11, which consists of 3 parts termed a-c below.

[Rule 11a] Software intended to provide information which is used to take decisions with diagnosis or therapeutic purposes is classified as class IIa, except if such decisions have an impact that may cause: — death or an irreversible deterioration of a person's state of health, in which case it is in class III; or — a serious deterioration of a person's state of health or a surgical intervention, in which case it is classified as class IIb.

[Rule 11b] Software intended to monitor physiological processes is classified as class IIa, except if it is intended for monitoring of vital physiological parameters, where the nature of variations of those parameters is such that it could result in immediate danger to the patient, in which case it is classified as class IIb.

[Rule 11c] All other software is classified as class I.

For stand-alone MDSW that is under the scope of IVDR, a different set of classification rules apply as specified under Annex VIII of the IVD Regulation (EU) 2017/746.

In addition to assessment of the appropriate qualification and classification of the MDSW, there are a multitude of additional requirements on the legal manufacturer (LM) of the product. The LM should operate under a quality management system (QMS) according to ISO 13485:2016. Technical documentation and life cycle management should be developed according to applicable standards - for software including IEC 62304 class B or C. For a device of MDR class IIa, there is a requirement for QMS audit and conformity assessment by an external Notified Body-Documentation supporting the clinical efficacy of the device must be provided for regulatory approval. It can be estimated that these processes can be performed in 24 months, depending on the extent of documentation supporting efficacy that needs to be provided.

Based on current (March 2022) understanding of the potential OPTIMA CDS software, the OPTIMA CDS will most likely be subject to MDR and, at a minimum, classified as IIa. The risk classification will be assessed by whomever will be the legal manufacturer of the software and based on the intended use of the product.

1. Impacts of AI/ML on Medical Device Software

Regarding use of artificial intelligence/machine-learning within MDSW (AI/ML-based MDSW), the qualification and classification of the AI/ML-based MDSW is, in general, not affected simply because the SW uses AI. A variety of marketed devices use AI/ML for training purposes and then "lock" the algorithm, meaning the algorithm does not change on its own over time. For example, IVD manufacturers have used these approaches for some time for digital pathology products. This regulatory approach to AI/ML-based MDSW is used in the EU as well as the US and other jurisdictions.

There are distinctions between AI/ML-based MDSW that leverage locked algorithms versus AI/ML-based MDSW that leverage algorithms that are adaptive, or continuously learning. Regulators continue to assess how to best regulate adaptive algorithms, and we are not aware of any such medical devices currently being marketed. Some regulatory approaches being considered by Health Authorities include use of predetermined change control plans, which includes the types of anticipated postmarket modifications, and the associated process necessary to implement those

changes in a controlled manner, which are approved during the initial conformity assessment of the SW. Although the MDR does not specifically call out "predetermined change control plans," it does require that Notified Bodies have documented procedures in place with the manufacturer relating to the assessment of changes. This implies that a manufacturer can already establish a predetermined change control plan concept with a Notified Body under the existing regulatory construct, which is described in a paper by industry group COCIR..

If the OPTIMA CDS software utilizes artificial intelligence/machine-learning (AI/ML) to train the algorithm and then "locks" the algorithm, meaning the algorithm does not continue to iterate or learn on its own, the use of AI/ML does not affect the classification of the MDSW under MDR/IVDR.

2. Impacts of proposed AI Act

Under the proposed EU AI Act (AIA), products that use AI can be placed into one of four risk categories: unacceptable risk; high risk; limited risk; and minimal risk. The "risk" under the proposed AIA is entirely separate from the device risk assigned by MDR/IVDR. The majority of AI/ML-based MDSW - those that require conformity assessment under MDR/IVDR - will fall under the "high risk" category under the proposed AIA. Lower risk MDSW that uses AI/ML could fall under the limited risk category. The proposed regulation could impart additional documentation or possibly additional requirements above what MDR/IVDR already requires for MDSW.

Industry has voiced its concern about the duplicative nature of this regulation and the need for devices to either be out-of-scope or for the overlap with the MDR/IVDR to be minimized.

iv. Pending Legislation

1. Data Governance Act

The Data Governance Act ("DGA") is a legislative proposal of the European Commission, officially presented on November 25, 2020. It is part of EC's general digital market strategy and is intended to complement other legislation, such as the GDPR, the Digital Market Act[49] and the Digital Services Act.[50] The Council of the European Union is currently undergoing its first reading of the draft law.

The DGA's aim is to increase the cross-border re-use of personal data held by public bodies (including state-owned or funded hospitals) for scientific and other purposes of general interest and to increase trust in data sharing and data intermediaries. It aims to do this by "creating a harmonised framework for data exchanges."[51] The DGA consists of three primary sections:

(1) It "creates a compulsory notification regime applying to a range of data sharing services."[52]

[49] Proposal for a Regulation on contestable and fair markets in the digital sector ("Digital Market Act"), COM/2020/842 final, 15.12.2020

[50] Proposal for a Regulation on a Single Market for Digital Services ("Digital Services Act"), and amending Directive 2000/31/EC, COM/2020 825 final.

[51] Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act), 2020/0340 (COD) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767>, hereinafter the "DGA Proposal"

[52] Julie Baloup, *et al.*, "CiTiP Working Paper Series: White Paper on the Data Governance Act," KU Leuven Center for IT & IP Law – imec, 23 June 2021 6, 57.

(2) It "introduces a voluntary registration regime applying to data altruism services. In this way, the DGA proposal should ensure trust in data sharing and data intermediaries, to the benefit of both these intermediaries and their users…"[53] And

(3) "[V]iewed as a complement to the Open Data Directive which mandates public sector bodies to share the data that they hold, the DGA proposal creates a legal regime for the re-use of public sector data which are subject to the rights of third parties."[54] Importantly, the regulation does *not* offer a new legal basis for the re-use of personal data for purposes of general public interest. The proposed legislation is not intended to have any impact on intellectual property rights or trade secret law.

If passed, the proposed legislation could have a number of consequences for OPTIMA or similar projects. Consortium members who are publicly funded hospitals[55] are likely to be most affected by the law as they will be subject to the legal regime for the re-use of specific data held by them. That specific data being personal and non-personal data protected on grounds of commercial or statistical confidentiality, intellectual property or personal data protection.[56] The proposed DGA requires the following with respect to such data:

- Encourages, but does not require, public hospitals to make such public sector data available
- Prohibits public hospitals from entering into contracts which grant exclusive rights to the re-use of public sector data held by the hospital [Art. 3(3)][57]
- Requires that public hospitals "make publicly available the conditions" for allowing re-use of their data [Art. 5(1)] and that those conditions be "non-discriminatory, proportionate and objectively justified". [Art. 5(2)]
- Public hospitals are permitted to put restrictions on the re-use of their data, such as an obligation to:
    - use only pseudonymized or anonymized data. [Art. 5(3)]
    - access the data only within a secure processing environment provided by the public sector. [Art. 5(4)]
    - access the data only within the physical premises of the secure processing environment, if remote access might "jeopardis[e] the rights and interests of third parties." [*Id.*]
- Requires public hospitals "be able to verify any results of processing of data undertaken by the re-user" [Art. 5(5)]
- Instructs public hospitals to support re-users in seeking consent or permission for re-use "where it is feasible without disproportionate cost". [Art. 5(6)].
- Requires the public hospital, in the case that the re-user intends to transfer non-personal data to a third country, to inform the "data holder" about the transfer to a third country. [Art. 5(13)]. The proposed DGA also contains language suggesting that the Commission may issue

[53] *Id.*
[54] *Id. See also* Proposal on DGA, Recital (3) at 11, 42 ("A horizontal regime for the re-use of certain categories of protected data held by public sector bodies, the provision of data sharing services and of services based on data altruism in the Union should be established.")
[55] *See* DGA Proposal Art.2 (11) & (12): "'bodies governed by public law' means bodies that have the following charcateristics:…they are established for the specific purpose of meeting needs in the general interest, and do not have an industrial or commercial character;..they are financed, for the most part, by the State, regional or local authorities, or by other bodies governed by public law; or are subject to management supervision by those authorities or bodies….
[56] DGA Proposal, Art. 3.
[57] Unless it is "necessary for the provision of a service or a product in the general interest" and then only for a period of three years. [Art. 3(2) & (5)].

additional acts "laying down special conditions" for transfers of "highly sensitive" data to third countries in the future. [Art. 5(11)].

- Permits public hospitals to charge fees for the re-use of the data, so long as those fees can be paid online, are non-discriminatory, proportionate and objectively justified and do not restrict competition. [Art. 6]. It also instructs that they should "take measures to incentivise the re-use of…data…for non-commercial purposes and by small and medium-sized enterprises…"[Art. 6(4)].
- Public hospitals will receive requests for the re-use of specific public sector data from single information points that the proposed DGA requires Member States to establish. [Art. 8 (1) & (2)]. These single information points will be responsible for merging information on the conditions and fees and for receiving requests for the re-use and transmitting the request to the relevant public sector body.

The proposed DGA may have additional effects on OPTIMA depending on whether or not any Consortium member or the ultimate market proponent of OPTIMA's end product is classified under the law as "data sharing service." The proposed DGA defines a "data sharing service" and any entity who offers

> "intermediation services between data holders which are legal persons and potential data users…those services may include bilateral or multilateral exchanges of data or the creation of platforms or databases enabling the exchange or joint exploitation of data, as well as the establishment of a specific infrastructure for the interconnection of data holders and data users."

[Art. 9(1)]. Unfortunately, this description is very vague, as many commentators have already observed.[58] We currently believe OPTIMA's envisioned end product does not qualify under this definition although, in a strict sense it could be considered to enable "the exchange or joint exploitation of data" or qualify as a "specific infrastructure for the interconnection of data holders and data users." Our opinion is based on the exemptions from the definition of "data service provider" articulated in Recital 22 of the proposed DGA. Specifically, we obtain data from data holders and "aggregate, enrich or transform" it before making aggregated statistics available or before providing any advice to clinicians based on the incoming data; our goal is not primarily to "facilitate the aggregation and exchange of substantial amounts of relevant data" but rather to create a diagnostic and research tool to help patients.[59]

---

[58] *See, e.g.,* Centrum für Euopäische Politik (cepPolicy Brief No. 2021-6) on the EU-Regulation Data Governance Act. <https://www.cep.eu/en/eu-topics/details/cep/data-governance-act-ceppolicybrief-com2020-767.html> ("the vague provisions on providers of data sharing services are highly unclear as to their scope….the provisions…contradict each other, e.g., on who may be the data holder and potential data users. Furthermore, it is not clear which of the services shall encompass which type of data, e.g., personal vs. non-personal…."); Julie Baloup, *et al.*, "CiTiP Working Paper Series: White Paper on the Data Governance Act," KU Leuven Center for IT & IP Law – imec, 23 June 2021 at 3, 57. ("The DGA proposal needs to set out the exact scope of the data sharing service providers, by laying down specific criteria that providers will need to meet. At the moment, both the included entities and those exempted are vaguely defined.").

[59] *See* Recital (22):

> Data intermediaries offering services that connect the different actors have the potential to contribute to the efficient pooling of data as well as to the facilitation of bilateral data sharing...This Regulation should only cover providers of data sharing services that have as a main objective the establishment of a business, a legal and potentially also technical relation between data holders, including data subjects, on the one hand, and potential users on the other hand, and assist both parties in a transaction of data assets between the two…*excluding* data sharing services that are meant to be used by a closed group of data holders and users." (emphasis added.) "[S]ervice providers that obtain data from data holders,

The proposed DGA also contains provisions relating to what it calls, "data altruism" – which requires an entity operate on a not-for-profit basis to qualify. [Art. 16]. If any of our members qualify under this definition, they eventually may be able to streamline the consent process through a standardized consent form, which the Commission will soon adopt. [Art. 22].[60]

Finally, the proposed DGA requires public sector bodies or any re-user of data to take measures to prevent third party transfers if such transfers "would create a conflict with Union law or the law of the relevant Member State". [Art. 30 (1) and (5)].

The Commission also plans to publish another legislative proposal called the Data Act this year addressing substantive rights on data access including business-to-business and business-to-government access.[61]

2. European Health Data Space

The European Health Data Space is Commission imitative to permit easier and more interoperable cross border access to health data among Member States. It will "promote the better exchange and access to different types of health data (electronic health records, genomics data, data from patient registries, etc.) not only to support healthcare delivery…but also for health research…"[62] The Commission's goal is to ensure the system is "built on transparent foundations that fully protect citizens' data and reinforce [its] portability."[63] The envisioned data space will be built on the following three pillars: (1) "a strong system of data governance and rules for data exchange"; (2) "data quality"; and (3) "strong infrastructure and interoperability."[64]

The Commission and Member States are currently undergoing preparatory work for the space and there is no formal proposed legislation that is a direct product of this initiative. For example, a study was commission to map how the GDPR is implemented in different Member States; to provide an "overview of the legal and technical modalities applicable to health data sharing for primary and secondary uses"; and to provide "an overview of the existing governance structures for secondary use of health data in" Member States.[65]

Given the lack of a draft legislation in this space, it is difficult to predict how the European Health Data Space may affect OPTIMA other than to say that the increased technical and semantic

---

aggregate, enrich or transform the data and licence the use of the resulting data to data users, without establishing a direct relationship between data holders and data users, for example…providers of data products resulting from value added to the data by the service provider" are excluded from the definition. Moreover, "[e]ntities which restrict their activities to facilitating use of data made available on the basis of data altruism and that operate on a not-for-profit basis should not be covered by Chapter III of this Regulation, as this activity serves objectives of general interest by increasing the volume of data available for such purposes."

[60] *See also* Recitals (35) and (36)

Support for scientific research is considered a "purpose of general interest" and data subjects providing data to data altruistic organizations would "consent to specific purposes of data processing, but could also consent to data processing in certain areas of research or parts of research projects as it is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection."

[61] < https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13045-Data-Act-&-amended-rules-on-the-legal-protection-of-databases_en>

[62] <https://ec.europa.eu/health/ehealth-digital-health-and-care/european-health-data-space_en>

[63] *Id.*

[64] *Id* .

[65] *Id.*

interoperability that will likely result from the initiative may make it easier to implement OPTIMA's tool and may permit our project to access a wider variety of health data than we would otherwise anticipate. The results of the study "allow for a detailed assessment of possible elements at Member States/EU level that might affect the movement of health data across borders [and] identifies practices that could facilitate this exchange of data, as well as possible policy options for strategies in this area."[66]

The Commission hopes to adopt the first legislative proposal in the first half of 2022.[67]

3. Artificial Intelligence Act (AIA)

On April 21, 2021, the Commission published its Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on Artificial Intelligence (Artificial Intelligence Act) (hereinafter, "AIA") and amending certain union legislative acts.[68] The proposed regulation aims to "develop[] an ecosystem of trust by proposing a legal framework for [human-centric], trustworthy AI…to give people and other users the confidence to embrace AI-based solutions, while encouraging businesses to develop them. "[69]

The proposed regulation takes a risk-based approach; classifying different AI devices based on the likelihood they may pose a significant risk to the health and safety of natural persons. Many medical devices and in vitro diagnostic medical devices will qualify as "high-risk" under the proposed regulation – assuming they must undergo a third-party conformity assessment.[70] That is, OPTIMA's anticipated device will qualify as a high-risk AI device under the proposed AIA.

Under the proposed AIA, high risk AI is subject to a number of requirements including:

- **A risk management system (AIA, Article 9)**
  Requires AI providers[71] , importers[72] to establish and maintain a continuous, iterative risk management system through the AI system's lifetime. The risk management system must include an analysis of the foreseeable risks associated with the AI system; an estimation and evaluation of risks that may emerge; an evaluation of other risks based on post market analysis (Article 61); and risk management measures. Risk mitigation measures should include elimination or reduction of risk through adequate design and development and a testing

[66] DG Health and Food Safety, Assessment of the EU Member States rules on health data in light of GDPR, Luxembourg: Publications Office of the European Union, 2021, at 9, 262 <https://ec.europa.eu/health/system/files/2021-02/ms_rules_health-data_en_0.pdf>
[67] 19th eHealth Network meeting (Teleconference), 3 June 2021, Brussels, Belgium. <https://ec.europa.eu/health/latest-updates/cover-notes-and-presentations-19th-meeting-ehealth-network-3-june-2021-2021-07-15_en>
[68] <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206>
[69] *Id.* at 1.
[70] *See* AIA Article 6 (defining a high risk system as one in which:
"the AI system is intended to be used as a safety component of a product, or is itself a product, covered by the Union harmonisation legislation listed in Annex II [which includes the MDR and IVDR at Annex II, Section A, 11. & 12.]" and in which "the product whose safety component is the AI system, or the AI system itself as a product, is required to undergo a third-party conformity assessment with a view to the placing on the market…"
).
[71] That is, anyone who "develops an AI system or that has an AI system developed with a view to placing it on the market or putting it into service under its own name or trademark, whether for payment or free of charge" (AIA, Article 3(2)).
[72] *See* AIA Article 26.

procedure to be performed during the development process in order to identify the most appropriate risk management measures. Residual risks must be communicated to users.

- **Data governance and management requirements (Article 10)**
  Requires AI systems to be trained and validated on data sets that meet specific quality criteria. For example, "[t]raining, validation and testing data sets shall be relevant, representative, free of errors and complete".[73]

- **Technical documentation (Article 11)**
  Providers and importers must provide technical documentation that demonstrates the AI system complies with the AIA and sets forth "all the necessary information to assess the compliance of the AI system with those requirements".[74] The Commission has provided a list, as part of Annex IV to the proposed legislation, which sets out specific details such a technical documentation must include. However, the technical documentation/application under the MDR will suffice to meet this requirement.[75]

- **Recording system/Automatic logging system (Article 12 and 20)**
  The AI system must have the ability to automatically record events while the system is operating enabling the "monitoring of the operation of the high-risk AI system with respect to the occurrence of situations that may result in the AI system presenting a risk" to the health and safety (or fundamental rights) of persons "or lead to a substantial modification, and facilitate [] post-market monitoring."[76]

- **Transparency requirements and information to users (Article 13)**
  Requires AI systems to be developed so that their "operation is sufficiently transparent to enable users to interpret the system's output and use it appropriately."[77] Transparency measures should include a set of instructions for use (which include, among other things details regarding its performance, the level of accuracy, robustness and cybersecurity for which the device has been tested, warnings regarding risks of normal and foreseeable misuse, and specifications regarding input data); pre-determined possible changes to the device and its performance; human oversight measures; and expected lifetime of the device.

- **Human oversight (Article 14)**
  Requires AI systems to be designed and developed that they can be effectively overseen by a natural person with an aim toward "preventing or minimising the risks to health, safety or fundamental rights".[78] Specific capabilities of the system, as appropriate, should include enabling the users of the system to: (1) understand the capacities and limitations of the system and monitor its operation; (2) remain aware of the possible tendency to over-rely on output produced by an AI system particularly for recommendations for decisions to be taken by natural persons; (3) correctly interpret the output; (4) to be able to decide not to use the AI system or otherwise disregard, override or reverse the output of the system; (5) be able to intervene on the operation of the AI system or interrupt the system through a stop button or similar procedure.

[73] AIA, Article 10(3).
[74] AIA, Article 11.
[75] AIA, Article 11(2).
[76] AIA, Article 12
[77] AIA, Article 13.
[78] AIA, Article 14.

- **Accuracy, robustness, and cybersecurity (Article 15)**
  Requires AI systems to exhibit an "appropriate level of accuracy, robustness and cybersecurity".[79] The levels of accuracy and relevant accuracy metrics must be provided in the accompanying instructions of use. Robustness indicates the device's ability to be "resilient as regards errors, faults or inconsistencies that may occur within the system" and can be achieved through technical redundancy solutions. Resilience indicates that the system should be able to withstand attempts by unauthorised third parties to alter the use or performance of the system by exploiting its vulnerabilities.

- **Quality management systems (Articles 16 and 17; similar to MDR)**
  Requires AI providers to put a quality management system in place, documented in the form of written policies, procedures and instructions, including a long list of items specified by the Article.[80] For example, "a strategy for…compliance with conformity assessment procedures and procedures for management of modifications to the high-risk AI system;"[81] "techniques, procedures and systematic actions to be used for the design, design control and design verification of the high-risk AI system;"[82] and "systems and procedures for data management, including data collection, data analysis, data labelling, data storage, data filtration, data mining, data aggregation, data retention and any other operation regarding the data that is performed before and for the purposes of the placing on the market or putting into service of the high-risk AI system."[83]

- **Conformity assessment procedure and declaration of conformity/registration (Articles 40, 41, 43 & 44, 48 & 51)**
  Requires AI devices to undergo a conformity assessment procedure. However, medical devices, under item 3. of this article, are able to rely on the conformity assessment procedure under the MDR to satisfy this requirement, so long as the requirements of Chapter 2 of the AIA are part of that conformity assessment procedure; as well as the AIA's Annex VII, Points 4.3 through 4.6.
  Anytime there is a substantial modification, the high-risk AI system must undergo a new conformity assessment procedure. *However*, certain changes that an AI system undergoes as a result of learning after being placed on the market, will *not* necessarily be considered a substantial modification so long as the changes "have been predetermined by the provider at the moment of the initial conformity assessment and are part of the information contained in the technical documentation…"[84]

  The provider must draw up a declaration of conformity, stating that system's compliance with Chapter 2 of the AIA for each system.[85] For medical devices this declaration will also include the declaration of conformity with the MDR. The provider must also register the system in an EU public database.[86]

- **Post marketing monitoring obligations (Article 61)**
  Requires AI providers to establish and document a post-market monitoring system for the device. The post-market monitoring system under the MDR qualifies to meet this requirement

[79] AIA, Article 15.
[80] AIA, Article 17.
[81] *Id.*
[82] *Id.*
[83] *Id.*
[84] AIA, Article 43(4).
[85] AIA, Article 48.
[86] AIA, Articles 51, 60.

so long as paragraphs 1-3 of Article 61 are also integrated into the system (*i.e.*, that it is proportionate to the potential risks posed by the system; that it actively and systematically collects, documents and analyses relevant data provided by users or collected through other sources on the performance of the system and allows the provider to evaluate the continuous compliance of the system with the requirements in Chapter 2; and that it be set out as part of the technical documentation for the device and include items that are to be enumerated by the Commission at a later date).

Although it is unlikely to affect OPTIMA, the AIA regulation anticipates the building of "regulatory sandboxes" made to test "innovative AI systems".[87] Vague language in those articles indicate that supervisory authorities may allow for some flexibility with respect to the (non-)existence of an independent legal basis under the GDPR for data used to test AI devices making use of the sandbox.

Finally, penalties under the proposed AIA are severe. Specifically, if a device is deemed to be non-compliant with data and data governance requirements, fines of up to 30 million Euro or 6% of the total worldwide annual turnover for the preceding financial year, whichever is higher, could apply. In the event of non-compliance with other AIA requirements, fines of up to 20 million Euro, or 4% of the annual turnover could apply.[88]

b. Ethical Framework

Ethical obligations and considerations in the OPTIMA project stem from European Commission Guidelines, Article 34 of the Grant Agreement, and widely recognised ethical principles, some of them ingrained in law. A serious breach of ethical principles may lead to the suspension of the grant or suspension of the implementation of the action, as per Article 48.1 and Article 49.2.1 of the Grant Agreement. Following a solid ethical framework will also be key for the success of OPTIMA as it will contribute to the take-up of the project, as it will contribute to creating and maintaining trust of patients, clinicians, researches, policy-makers and other actors. The development of new technologies inherently enshrines a system of values and can therefore not be neutral in regards to ethics. Instead, ethical research and implementation must be actively promoted, and ethical risks and considerations must be acknowledged at an early stage.

Ethics in OPTIMA will be guided by WP2 and WP10. A continuous evaluation of the ethical framework and the monitoring of ethical issues and requirements will be reflected in D2.2, D2.4, D2.6, D10.1 and D10.2. In particular, D2.4 (Second Iteration of the Legal and Ethical Framework) and D2.6 (Helpdesk report) due in M20 and M60 can reflect the ethical challenges that have emerged in OPTIMA over time. The Legal and Ethical Helpdesk established in WP2 and the Ethical Advisory Board established in WP1 can support partners in remaining compliant with all ethical requirements.

OPTIMA aims for the highest standards of ethical research and responsible scientific practice, also hoping to promote these standards and to therefore contribute to a culture of ethically responsible research. This section outlines the key ethical considerations taken into account by OPTIMA and points to some of the documents relevant to ethics in OPTIMA. Key considerations are related to research ethics and integrity, healthcare ethics, ethical aspects of privacy and personal data, and Artificial Intelligence ethics.

[87] AIA, Article 53, 54.
[88] AIA, Article 71.

i. Research ethics and overall conduct of the consortium

The OPTIMA project is designed and undertaken in a way to maximise positive and minimise negative impacts. The benefits for research and for society as a whole must be balanced with individuals' rights. OPTIMA partners are committed to promoting responsible research practices based on the highest standards of scientific integrity. This includes meeting the highest possible standards of quality, accuracy and transparency in the processes and results of the project. Unacceptable practices are, for example:

- the manipulation of data
- the manipulation of data representations or consents
- the suppression of relevant findings
- the misappropriation of ideas or intellectual property
- the misrepresentation of material interests or conflicts of interest.[89]

OPTIMA is committed to sharing its results within and outside the scientific research community, in line with the FAIR principles, while always balancing this against the rights of individuals and other considerations, such as IP rights.

Finally, the consortium will consider the legal and ethical bases for any action within the project, taking into account that legal and ethical frameworks may vary between states and over time. Additionally, it should be considered that, while legal and ethical frameworks often converge, not all ethical requirements are codified in law and should therefore be considered in combination with, but distinctly from the legal framework.

ii. Healthcare ethics

In the context of the project (with prospective data collected in WP3) and in the future deployment of OPTIMA, direct interactions with and research involving human subjects is envisaged. This involves a number of ethical risks which have to be acknowledged at an early stage, mitigated, and monitored. In particular, there may be clinical risks (a worsening of physical health as a result of the research study), psychological risks (a worsening of psychological health as a result of the research study), social risks (for example the risk of isolation as a result of participation in the study), and the risk of discrimination (discrimination during the study, during recruitment to participate in the study, as a result of the study…).[90] Working with personal data, in particular sensitive data, includes additional risks which will be addressed in the next section (4.b.iii).

Regarding the direct interactions with human subjects and the future deployment of OPTIMA in a healthcare setting, four key principles dominate the field of healthcare ethics: beneficence, non-maleficence, respect for autonomy and justice.[91] These principles should not only guide direct interactions with research subjects in OPTIMA, but also guide the overarching aim of the project and the design of the AI component and the guideline decision support tool. The principle of beneficence states that healthcare providers should act with the intent to do good for their patients. This includes finding the best treatment option, but it can lead to difficult questions of what good means to each patient. This principle can be promoted by better understanding patients' wants, needs and

[89] City University of London, Principles of Research Ethics <https://www.city.ac.uk/research/support/integrity-and-ethics/ethics/principles>
[90] World Health Organisation, <https://www.who.int/patientsafety/research/ethical_issues/en/>
[91] Beauchamp and Childress, Principles of Biomedical Ethics, 1979

experiences. Non-maleficence is the rule to do no harm and should guide treatment options and interactions with patients and amongst healthcare professionals. Respect for autonomy, on the other hand, relates to the control over decision-making and over the own body that patients themselves exercise. Health care professionals should ensure that patients are informed and educated, and retain the ability to decide on a course of action for themselves. This reflects, for instance, in informed consent processes. Finally, the principle of justice states that medical decisions should be fair and equitable. Justice is often separated into two categories: procedural justice (having fair procedures and following due process), and distributive justice (concerning the fair allocation of resources).

Ethical requirements are to some extent engrained in law. Overarching principles guiding ethics in a healthcare context often stem from the European Convention of Human Rights and the EU Charter of Fundamental Rights, including its first article referring to human dignity, relevant to the use of the human body in biomedicine, and the treatment of research participants and patients as subjects and not as objects.[92] Responding to the need for more guidance on ethics in a healthcare setting, the World Medical Association issued the Declaration of Helsinki (DoH), a non-binding document which became legally binding in the EU through EU Regulation 536/2014. It states a commitment to key principles such as respect for the individual, self-determination, and the precedence of the research subjects' welfare over the interests of science. Additionally, it states that the risk of research projects should be assessed and researchers must show that the risks to research subjects are not unreasonable or disproportionate.[93] The first version of the Declaration was adopted in 1964, but has been amended seven times since. Additionally, the Declaration of Taipei on Ethical Considerations Regarding Health Databases and Biobanks complements the DoH since 2016, reflecting the increased need for a solid ethical framework to work with patients and research subjects (and their data) on a large scale. The Declaration of Taipei also declares that while it is still primarily aimed at clinicians, it is not only clinicians who work with health data and who should therefore adopt these principles.

All partners in the OPTIMA consortium are committed to meeting the highest standards for ethical conduct in a healthcare setting. This includes contacting the Legal and Ethical Helpdesk for guidance where necessary, and, for high level ethical questions, involving the Patient Public Advisory Board (PPAB) and the Ethical Advisory Board (EAB).

iii. Development of the platform and ethical data use

Conducting research using personal data involves certain ethical risks, in particular related to privacy of the data subjects (loss of confidentiality, potential for reidentification, etc.) and risks such as potential discrimination, data misuse or psychological distress resulting from a loss of privacy. Health data constitutes a special category of data, as per Art 9 of the GDPR, due to the increased risk to data subjects in case of misuse or loss of privacy or confidentiality.

It is important to consider in the context of OPTIMA that sensitive personal data stems not only from direct interactions in the context of the project (the prospective data collected). Personal data, in particular health data, and all the risks associated with it in OPTIMA will primarily stem from retrospective data integrated into the platform. While the DoH already enunciates the right to privacy and confidentiality, the Declaration of Taipei really shows the increased emphasis on privacy and the need to balance the rights of individuals with the potential benefits of using health data as a powerful

[92] Frischhut and Werner-Felmayer, A European perspective on medical ethics, <https://www.sciencedirect.com/science/article/pii/S135730392030164X>
[93] Declaration of Helsinki, World Medical Association, 2013, Article 16. https://www.wma.net/policies-post/wma-declaration-of-helsinki-ethical-principles-for-medical-research-involving-human-subjects/

tool to increase knowledge.[94]

OPTIMA strives to achieve this balance and is committed to respecting and promoting all ethical requirements. Additionally, continuous research will be conducted to update this deliverable to reflect developments in the project, and emerging ethical requirements. In the interests of promoting the principles of self-determination and respect for autonomy, the PPAB and the EAB will be consulted at critical points, for instance when it comes to developing informed consent processes for the activities in WP3. Key principles for the ethical use of personal data in OPTIMA therefore include:

1. **Lawfulness**: For all use of personal data there must be a legal basis as discussed in 4.a.

2. **Data subject protection**: Data subjects' rights, dignity, privacy and security have to be ensured and balanced against the positive outcomes of data use.

3. **Agency and informed consent**: The autonomy of the data subjects has to be respected and agency of data subjects should be promoted. Informed consent processes for WP3 should be developed with this aim in mind and the use of retrospective data should, where possible be based on informed consent. Where this is not the case, a different legal basis has to be stated and it should be discussed if and how the benefits outweigh a certain loss of agency.

4. **Patient involvement**: Through the PPAB it should be ensured that the patient perspective on data use in OPTIMA is strongly considered.

5. **Transparency and trustworthiness**: For the OPTIMA platform to achieve its aim, it must maintain the trust of researchers, patients, and clinicians. This should be encouraged through strong involvement of those stakeholders, and through transparency in the use of data, including and in particular where the federated structure is not used and data is transferred to the Helmholtz centre.

6. **Trade-offs**: Where there are inevitable trade-offs between ethical principles, these should be approached methodically and in line with current literature. They should be handled transparently.

iv. Artificial Intelligence ethics and the development of the OPTIMA AI component

The OPTIMA consortium is committed to following the European Commission's approach to Artificial Intelligence development. This includes in particular the "Ethics guidelines for trustworthy AI" developed by the European Commission's High-Level Expert Group on AI.[95] These Guidelines state that for AI to be trustworthy it should be "lawful, ethical and robust". This is based on the principles of

- Respect for human autonomy
- Prevention of harm

[94] Declaration of Taipei on ethical considerations regarding health databases and biobanks, World Medical Association, 2016, https://www.wma.net/policies-post/wma-declaration-of-taipei-on-ethical-considerations-regarding-health-databases-and-biobanks/

[95] European Commission, Ethics Guidelines for Trustworthy AI, <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>

- Fairness
- Explicability

The Guidelines also provide a non-exhaustive set of seven key requirements:

1. Human agency and oversight

Human beings should be empowered by their use of AI, as prescribed by the principle of respect for human autonomy. Users should be able to make informed decisions and "where possible, be enabled to reasonable self-assess or challenge the system".[96] The principle of human agency and autonomy must be central to OPTIMA's AI component. A key aspect of this is ensuring that participants in WP3 and future users of OPTIMA are not subjected to decisions based solely on automated decision-making. Proper oversight mechanisms need to be ensured, such as the "human-in-the-loop", "human-on-the-loop" or "human-in-command" approaches.

2. Technical robustness and safety

AI systems need to be resilient, secure, accurate, reliable and reproducible. This includes protection against attacks potentially targeting the data, the model, or the underlying infrastructure, for a system to be considered secure. Systems can be corrupted and data, as well as system behaviour can be changed. In a healthcare setting, there is the risk of making erroneous decisions based on AI systems, meaning that a lack of robustness and safety can lead to significant physical and psychological harm. Potential abuse of the system should be taken into account and measures should be introduced to mitigate this risk, including a fallback plan for the event of an attack or problem. Additionally, for a system to be considered accurate and reliable it must be able to make correct judgements in a range of situations, and to indicate how likely an error is in situations where there may be inaccuracies.

3. Privacy and data governance

Full respect for the fundamental right of privacy needs to be ensured and adequate data governance mechanisms must be put in place. The AI component of the project must guarantee privacy and data protection for the information provided by users, and the information generated about users. Data collected must not be used unlawfully. There must be adequate data governance mechanisms, including the data access protocols and the requirements to ensure privacy in data processing.

4. Transparency

AI systems, the data and AI business models should be transparent (linked to the principle of explicability). This can be achieved through traceability mechanisms, which can point to the reasons for an error in an AI system. Humans need to be aware when they are interacting with an AI system, and the decisions made by AI systems must be explainable to the stakeholders concerned. The complexity of AI systems can lead to a "black-box-problem", where errors are difficulty to identify and responsibility is difficult to allocate, therefore there must be a focus on transparency. Explainability requires that the decisions made by an AI system can be understood by humans. Even where trade-offs may have to be made between accuracy and explainability, it is key that humans should be able to understand the information generated by AI.

[96] European Commission, Ethics Guidelines for Trustworthy AI, p16.

5. Diversity, non-discrimination and fairness

Unfair bias must be avoided. While AI has the potential to avoid human bias, it can also perpetuate or amplify prejudice and discrimination. Bias can stem for example from human error in the training of AI systems, or from non-representative datasets used (inadvertent historic bias). During data collection, this should be considered and discriminatory bias should be removed or counteracted where possible. Afterwards, oversight mechanisms should be put in place to address the risk of unfair bias. Preventing unlawful discrimination and AI bias will be pursued in close cooperation between WP2 and WP7 when defining the design of the AI component of OPTIMA. Stakeholder participation (inclusion of those stakeholders affected by the AY systems) can also help counteract unfair bias, and OPTIMA will achieve this through close collaboration with the PPAB.

6. Societal and environmental well-being

AI systems should be designed to be sustainable, take into account the environment, and benefit future generations, in line with the principles of fairness and prevention of harm. In regards to environmental well-being, the AI systems supply chain, development and deployment should be examined to assess resource usage and energy consumption, and opt for the most sustainable and least harmful options where possible.

7. Accountability

Responding to the principle of fairness, mechanisms for accountability and responsibility of AI systems and their outcomes should be put in place. This includes auditability, which enables the assessment of algorithms, data and design processes. Not all information about the system must be openly available, particularly as there may be concerns about intellectual property, however, evaluation by internal and external auditors must to some extent be possible. For accountability purposes, it is important to report negative impacts of the AI system. Redress mechanisms should be foreseen in case of adverse impacts.

8. Future developments

Particularly in the field of AI, the legal and regulatory framework is developing quickly, as for example with the upcoming AI Act. OPTIMA is committed, on the one hand, to monitoring these changes and continuously updating the ethical framework to meet high ethical standards. On the other hand, OPTIMA aims to contribute to the development of new policy and new projects through WP8. To inform all partners of upcoming legislation and discuss how to contribute to future developments, OPTIMA organised an initial internal discussion workshop on the AI Act in March 2022. A continuation of these efforts will be organised by close collaboration between WP2 and WP8.