Improving cancer diagnosis and prediction with AI and big data

A Multimodal AI-based Toolbox and an Interoperable Health Imaging Repository for the Empowerment of Imaging Analysis related to the Diagnosis, Prediction and Follow-up of Cancer

Deliverable 7.3

Data Donation Legal Framework

WP 7 – Legal and Ethics Management

04-04-2023

Revision: 1.0

Status: Final

Grant Agreement n 952179

European Commission

DOCUMENT CONTROL	
Project reference	Grant Agreement number: 952179
Document name	Data Donation Legal Framework
Work Package	WP7
Work Package Title	Legal and Ethics Management
Dissemination level	PU
Revision	1.0
Status	Final
Reviewers	Gianna Tsakou (MAG); Olalla Aramburu, Berta Borras (MDT)
Beneficiary(ies)	Timelex (TLX)

Dissemination level:
PU = Public, for wide dissemination (public deliverables shall be of a professional standard in a form suitable for print or electronic publication) or CO = Confidential, limited to project participants and European Commission.

AUTHORS		
	Name	**Organisation**
Document leader	Magdalena Kogut-Czarkowska	TLX
Participants	Gianna Tsakou, Paris Laras	MAG
	Shereen Nabhani-Gebara, Lithin Zacharias	KU
	Sara Martínez Alabart	FTSS
	Berta Borras, Olalla Aramburu	MDT
	Chara Stefanou	Adaptit
	Pol Camps	WR
	Alberto Gutiérrez Torre	BSC
	Caroline Barelle	ED
	Zisis Sakellariou, Paschalis Bizopoulos	CERTH
	Giovanni Mazzeo	CERICT
	Stavros Sykiotis	ICCS

REVISION HISTORY				
Revision	**Date**	**Author**	**Organisation**	**Description**
0.1	02/02/2023	M. Kogut-Czarkowska	TLX	Table of contents
0.2	07/02/2023	M. Kogut-Czarkowska	TLX	Update of ToC to include lessons learned/further work

REVISION HISTORY				
Revision	**Date**	**Author**	**Organisation**	**Description**
				chapter
0.3	10/03/2023	M. Kogut-Czarkowska	TLX	Initial draft for further input by other contributors
0.4	22/03/2023	M. Kogut-Czarkowska	TLX	Version following input by other participants
0.5	24/03/2023	M. Kogut-Czarkowska	TLX	Consolidated version for peer-review
0.6	31/03/2023	M. Kogut-Czarkowska	TLX	Final edits before submission
1.0	04/04/2023	M. Kogut-Czarkowska	TLX	Final version ready for submission

Disclaimer and statement of originality

The content of this deliverable represents the views of the authors only and is their sole responsibility; it cannot be considered to reflect the views of the European Commission and/or the Consumers, Health, Agriculture and Food Executive Agency or any other body of the European Union. The European Commission and the Agency do not accept any responsibility for use of its contents.

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

Table of Contents

Terms and Abbreviations

Terms and Abbreviations

Term	**Description**
Central infrastructure	The cloud infrastructure of INCISIVE, hosted by Azure, comprised by 4 Virtual Machines, located in Central France that contains the centralized services required to make the INCISIVE platform work.
Central Node	Central data storage space that will host Data from the Data Providers, technically acting in the same way as the Federated nodes. The Central Node can be used as one node of the several INCISIVE Federated Nodes and/or as a centralised data repository where AI training can take place.
Data or Repository data	Medical data and images made available in the Hybrid repository, including Retrospective training data and Prospective data, once made available for sharing.
Data Provider	An entity which contributes Data to the Hybrid repository. Data Providers include INCISIVE Data Providers (during the project) and external parties (External Data Providers).
Federated data sharing	The Data Providers share the Repository data by keeping them within their infrastructures (local or cloud). After being pre-processed locally, they are indexed in the Hybrid repository, through a data sharing mechanism.
Federated learning	Means that AI model is trained in a distributed way using the required Federated nodes, i.e., the nodes that have the Data that matched with the user query.

	Each Federated or Central node contains a particular set of Data that may be required for training, and it will not leave the node to ensure privacy. The model is trained in each Federated node, including Central node, and then it is sent to the Central infrastructure to be merged to gather 'central knowledge'. This training-merging process can be repeated more than once for the same model as the more times this is done, the more robust is the solution.
Federated node	Dedicated infrastructure (cloud or local) in which the Data Provider stores the Repository data which they contribute to the Hybrid repository.
Federated space	A virtual space formed by the composition of all Federated nodes, including the Central node, enabling the performance of centralized operations, such as the training of the AI models, access to Data utilized in the INCISIVE Platform, and visualizations of the results etc.
Hybrid data sharing	Data sharing which takes place using both Federated data sharing and a Central node.
Hybrid repository or INCISIVE repository	Pan-European repository of medical images and data, where each Data Provider maintains (stores) their data locally at chosen location, which includes either a Federated node set up at own premises or premises selected by the Data Provider, or Central node, or both. The term encompasses both Federated and Hybrid data sharing.
INCISIVE Platform or Platform	Platform (technical infrastructure integrating several components) provided by the Project which includes the Hybrid repository, AI development workspaces for AI training and the Inference services.
Inference services	The process of using the AI models over new input data to obtain the targeted results, e.g., predictions or tumour segmentations.
Initial Data Providers (also as INCISIVE Data Providers)	The following consortium partners: AUTH, HCS, UoA, UNITOV, DISBA, GOC, VIS, OIV, IDIBAPS.
Project	The INCISIVE project, Grant Agreement n 952179.
Prospective data	Additional collection of data from current or future patients who are receiving diagnoses and/or treatment from the Initial Data Providers, including from pilot studies.
Retrospective training data	A subset of shared personal data consisting of

	digitalized patient medical data extracted by each Initial Data Provider from their records and provided to Temporary infrastructure.
Technical Partners	The following consortium partners: MAG, ICCS, CERTH, CeRICT, BSC, ED, TIS, SQD, UH, KU, AUTH, UNS, VIS, DISBA, FTSS, ADAPTIT. The following partners: AUTH and VIS act as both INCISIVE Data Providers and Technical Partners (dual role). FTSS is acting both as Technical Partner for Hybrid repository and processor in the context of providing Temporary infrastructure.
Temporary infrastructure	Temporary infrastructure in which Retrospective training data is hosted by FTSS.
Abbreviation	**Description**
EC	European Commission
WP	Work Package
GDPR	General Data Protection Regulation (regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. The wordings 'personal data', 'data subject', 'processing', in this document have the meanings set out in the GDPR.
OIV	Oncology Institute of Vojvodina, established in Put dr Goldmana 4, 21204 Sremska Kamenica, Serbia, linked to UNS (a project partner) as a research base of the Medical Faculty of UNS
MAG, ICCS, CERTH, CeRICT, BSC, ED, TIS, SQD, AUTH, UNS, VIS, DISBA, FTSS, HCS, PASYKAF, UNITOV, UOA, UH, IDIBAPS, GOC, KU, CUT, TLX, WR, MDT, ADAPTIT	INCISIVE partners' abbreviations as defined in the Grant Agreement number 952179 – INCISIVE

1 Introduction

1.1 Purpose and scope

The goal of D7.3 is to provide guidelines and terms for data donors to participate in INCISIVE data providers ecosystem. It is a result of task T7.4 which involves the analysis of applicable rules, ethical principles, and standards regarding the data donation in the healthcare sector. The task will take into consideration the particularities concerning the procession of health and biometric data. The outputs of this task will be a legal framework in the form of legal guidelines and terms, enabling external parties to safely donate their data in the INCISIVE pan-European repository of health images, while maintaining full control of their data.

1.2 Document structure

The document starts with explanatory comments regarding the use of the term of 'data sharing' in the deliverable (instead of 'data donation', as originally provided in the DoA) and setting the landscape of the opportunities and challenges of medical data sharing (Chapter 2). Next, it summarizes the results of the analysis of applicable legal rules and provides guidelines for their implementation (Chapter 3). The document further covers ethical principles (Chapter 4) and standards (Chapter 5) regarding the data donation in the healthcare sector. Further, the document explains the establishment of principles for building the INCISIVE data sharing framework (Chapter 6). This work is then translated into a proposal of concrete legal terms of data sharing with the INCISIVE Repository and data use on the INCISIVE Platform (Chapter 8). Last, but not least, the document includes summary of the challenges, lessons learned and next steps in the finalization of the framework and its incorporation into sustainable repository (Chapter 7).

1.3 Relation with other deliverables

The work performed to complete this deliverable is related with the following:

- D5.2 - INCISIVE pan-European repository of health images (second version) – which provides for description of the data sharing schema and different functionalities of the INCISIVE Hybrid Repository
- D7.1 Initial Data Management Plan
- D7.2 Ethics letters and ethics deliverables
- D8.5 Preliminary Operational, Deployment and Sustainability Plan for the 'European repository of health images'

2 Meaning and importance of data donation

2.1 'Data donation' and 'data sharing' – use of terms

'Data donation' is not a term defined by the law. Moreover, it may be argued that - from a legal perspective - the data cannot be simply donated. This is because from a civil law perspective[1] the main characteristics of a donation – apart from the lack of compensation – are transfer of ownership and its irrevocability (subject to certain exceptions). In the context of personal data included in medical images and related health information:

- **Personal data are not a material asset** which can be 'owned' in a similar way to owning a house or some personal belongings. It is highly debatable[2], whether individuals are 'owners' of their medical data, as if so, to what extent can they dispose of it. To complicate things further, there exist intellectual property rights to data bases, which may come into play regarding collection of data one had created with their considerable efforts (these rights protect the efforts to select and arrange the data[3]). These rights are not the same as 'ownership' of a tangible asset.[4]
- **Irrevocability** is another main characteristic of a donation in a classical civil law understanding. In this traditional understanding, a donor forfeits its rights to the donated asset and may only revoke their decision under very specific circumstances (for example, gross ingratitude). In INCISIVE (as explained below), the data provider should still be allowed to exercise control over the 'donated' data and withdraw it from the INCISIVE Repository. This is not aligned with the concept of 'donation' in a traditional legal sense.

Given the above, to avoid misleading the readers and potential institutions which would like to contribute the data within the INCISIVE framework, unless otherwise required by the context, document uses the term 'data sharing' and 'data provider' rather than 'data donorship' and 'data donor'.

2.2 Benefits and obstacles to sharing data

While considering the data sharing framework, it is relevant to bear in mind the potential benefits of data sharing. These include:

---

[1] Prainsack, B. (2019). Data Donation: How to Resist the iLeviathan. In: Krutzinna, J., Floridi, L. (eds) The Ethics of Medical Data Donation. Philosophical Studies Series, vol 137. Springer, Cham. https://doi.org/10.1007/978-3-030-04363-6_2.

[2] Ibidem.

[3] See further comments in Chapter 3.

[4] Kop, Mauritz, Machine Learning & EU Data Sharing Practices (March 3, 2020). Stanford - Vienna Transatlantic Technology Law Forum, Transatlantic Antitrust and IPR Developments, Stanford University, Issue No. 1/2020, Available at SSRN: https://ssrn.com/abstract=3409712.

- Transparency of the scientific work and its conclusions,
- Maximising the utility and impact of the data collected,
- Making collaboration between different researchers easier,
- Research acceleration,
- Reproducibility of results,
- Data citation & credit,
- Long-term data preservation,
- Meeting requirements of funding and publications[5,6].

Still, there are several barriers to data sharing, which can be grouped as follows:

- Technical: such as inadequate data collection; lack of standardization and of common protocols; varying data quality; incompatibility between databases; language barriers,
- Motivational: such as lack of incentives to share data,
- Economic: such as lack of financial & skilled human resources, limited training capacity, difficulties in retaining staff,
- Political: such as restrictive data access policies; bureaucratic hurdles, lack of guidelines; and lack of trust,
- Legal and ethical: such as ambiguous and complex legal framework[7].

INCISIVE acknowledges the mapped barriers and proposes as comprehensive data sharing solution, considering both legal and technical perspective, which could be used to tackle the stated obstacles and take advantage of the benefits of sharing data with other researchers and the broader community.

[5] Based on ODAP The Open Data Assistance Program at Harvard (https://projects.iq.harvard.edu/odap/benefits-sharing-data).
[6] Based on "The Benefits of Data Sharing", available https://www.ccdc.cam.ac.uk/Community/depositastructure/cif-deposition-guidelines/benefits-of-data-sharing/.
[7] Based on Sane, J. and Edelstein, M. (2015). Overcoming Barriers to Data Sharing in Public Health: A Global Perspective.

3 Guidelines on applicable legal rules

3.1 GDPR

General Data Protection Regulation[8] (EU) 2016/67910 (GDPR) provides basic provisions constituting the general legal framework applicable in all Member States of the European Economic Area in relation to the protection of personal data[9].

The GDPR implies compliance with seven key principles:

- lawfulness, fairness and transparency – meaning that a legal basis for any data processing (including but not limited to consent) must be available, and that the persons concerned must be appropriately informed of how their data will be used;
- purpose limitation – meaning that data must be collected for specific purposes, and may thereafter only be used for compatible purposes;
- data minimisation – meaning that data collected and used for processing must be as minimal as possible, taking into account the intended purposes;
- accuracy – meaning that measures must be taken to ensure the quality and accuracy of the data, and that measures must be available to detect and remedy problems;
- storage limitation – meaning that data may only be retained for as long as necessary given the intended purposes, and that it must thereafter be deleted or anonymised;
- integrity and confidentiality – meaning that data must be protected by appropriate technical and organisational measures to ensure its confidentiality, integrity and availability;
- accountability – meaning that responsible entities must be identified, and that appropriate controls (such as logs) are available to ensure that any problems can be attributed to the correct entity.

In the context of health data, apart from the text of the GDPR, opinions of European Data Protection Supervisor (EHDS) and European Data Protection Board (EDPB) are relevant, in particular:

- European Data Protection Supervisor, A Preliminary Opinion on data protection and scientific research[10]

---

[8] General Data Protection Regulation (regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

[9] In the UK, the GDPR is retained in domestic law as the "UK GDPR." For now, the rules of the (EU) GDPR discussed below are also in place in the UK under the UK GDPR. However, for the future, UK will have the independence to revise its framework.

[10] European Data Protection Supervisor (EDPS), "A Preliminary Opinion on data protection and scientific research", adopted on 6 January 2020, available https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf.

- EDPB-EDPS Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space[11].

Below, we outline the considerations for the data sharing framework which arise on the basis of the said GDPR principles. However, the document does not aim to provide an exhaustive list of all potential privacy issues which need to be dealt with within INCISIVE project, which are carried out in the T7.1.

3.1.1 Lawfulness

Articles 6 and 9 GDPR provide possible legal basis for processing of personal data in general, and for sensitive personal data in particular. Moreover, most likely the data which the Data Providers may wish to contribute to Repository would not be collected specifically for the purpose of participating in INCISIVE Repository, but rather was collected in the context of other research projects or clinical studies. As follows from desk research, the landscape regarding use of the above listed legal bases for the reuse of health data collected for other purposes is very fragmented. More specifically, the permissible legal basis largely depends on national laws and practice.[12]

Given the above, it would not be possible to indicate to the Data Providers which legal basis is appropriate for their submission of their data, much less impose a particular basis (e.g., consent) for everyone. Ensuring a legal basis should be a responsibility of the Data Provider and the conditions and the applicable basis vary, depending on the national law and on the context in which the data were collected. If the Data Provider decides to collect consents from the data subjects it would need to ensure that such consent meets the requirements of the GDPR.

Guidelines: Each Data Provider must check whether they can assure that they have the appropriate legal basis to contribute Data to INCISIVE Repository.

3.1.2 Fairness and transparency

The rule of transparency states that data must be processed in a transparent matter in relation to the data subject. This rule is closely linked to information rights (Art. 13-14 GDPR) and data subject rights (Art. 15-21 GDPR). Under those provisions, in general, data subjects must be properly informed about the details of processing of their data for a specific purpose (also in case the data are not collected directly from the data subject).[13] There are very limited

[11] EDPB-EDPS Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space, adopted on 12 July 2022, available https://edps.europa.eu/system/files/2022-07/22-07-12_edpb_edps_joint-opinion_europeanhealthdataspace_en_.pdf.

[12] This conclusion is concurrent with the findings of the TEHDAS report of secondary use of health data through European case studies, available https://tehdas.eu/app/uploads/2022/08/tehdas-report-on-secondary-use-of-health-data-through-european-case-studies-.pdf.

[13] Detailed list of information to be provided is included in Articles 13 and 14 GDPR.

exceptions from this requirement.[14] For example, under Article 14(5)(b) GDPR, if the data are collected not directly from the data subject, the requirement to provide him/her with information does not apply if the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) GDPR or in so far as the obligation to provide information is likely to render impossible or seriously impair the achievement of the objectives of that processing.[15] If the data are collected directly from the data subject, this exception does not apply.

The transparency of the processing vis-à-vis the data subjects should be ensured through appropriate notices and policies, such as properly drafted information language made available to patients (unless exception applies), privacy notice on the Repository website and clear description in any agreements to be entered into by the Data Providers.

Guidelines: Where possible and legally required, privacy notices should be drafted and made available to the data subjects, unless specific exemption applies. This applies both to the patients (for pseudonymized data) and users of the platform. For the INCISIVE Data Providers, the prospective data collection templates included appropriate information about the goals of the project and consent for data submission. External Data Providers need to verify compliance with this obligation before submitting data. INCISIVE Platform will also include privacy notice for its uses. Moreover, each Data Provider which submits pseudonymized Data must allow its data subjects to exercise their rights stemming from Art. 15-21 GDPR, such as data access right.

3.1.3 Purpose limitation

The GDPR allows for special considerations for situations when personal data to be used in a research project were originally collected for a purpose other than scientific research. The basis for these considerations is related to the fundamental data protection principle of 'purpose limitation' enshrined in Article 5(1)(b) GDPR. According to this principle personal data must be collected for specified, explicit and legitimate purposes and may not be further processed in a way incompatible with those purposes. There is an important caveat to this rule: further processing for, inter alia, scientific research purposes shall, in accordance with Article 89(1) GDPR, not be considered to be incompatible with the initial purpose. Further explanation of

[14] Furthermore, according to Article 89(2) GDPR where personal data are processed for scientific or historical research purposes or statistical purposes, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18 and 21 GDPR subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.

[15] While whether the exception applies needs to be decided on a case-by-case basis, some arguments which may be invoked relate to consequences of providing information to the data subjects to the research objectives. In other cases, it may not be possible to contact the patients which have been treated long time ago or re-contacting them may be unethical.

purpose limitation principle is provided in recital 50 of the GDPR. This is often referred to as 'presumption of compatibility' under which 'in principle personal data collected in the commercial or healthcare context, for example, may be further used for scientific research purposes, by the original or a new controller, if appropriate safeguards are in place'.[16] On the basis of these provisions, and supported by the local law, some countries allow that - under defined conditions - the medical data collected for other purpose may be re-used for research without the explicit consent of the patients.

The conditions that allow data re-use vary greatly between the Data Providers' jurisdictions.[17] Usually, they relate to obtaining the approval of an ethics committee and providing a guarantee of appropriate safeguards.

Guidelines: Purpose of the processing of prospective Data submitted by INCISIVE Data Providers to the Repository was described in the informed consent forms (submitted in D7.2 Ethics Approvals) which are collected from the patients participating in the studies. The patients consented for INCISIVE beneficiaries to anonymize their health images and medical information for the purpose of depositing them in the INCISIVE Repository, so it can be used by other researchers outside the INCISIVE Project for the research and learning purposes of training and validating technologies related to cancer research and healthcare improvement in general. For external Data Providers, the selection of an appropriate legal basis for the submission of the Data must be tackled on a case-by-case basis for each Data Providers separately, taking into account compliance with the national law and practice on re-use of health data for research purposes. Data Providers must take into account that the Data in the Repository will be available to Data Users as outlined in the Data Sharing Agreement.

3.1.4 Data minimalization

Data minimisation means that data collected and used in the Project must be as minimal as possible, taking into account the intended purposes (Article 5.1(c) GDPR). One of the best ways to mitigate data protection and privacy harms and to reduce security risks, is to keep the processing of personal data at a minimum. This is connected with the concepts of anonymization and pseudonymization of personal data.

- Anonymous information is one which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly (recital 26 GDPR).

[16] European Data Protection Supervisor Preliminary opinion of 6 January 2020 on data protection and scientific research, https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf.
[17] Collection of retrospective data was conducted on the basis explained in D7.3 Initial Data Management Plan.

- Pseudonymization is the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person (Article 4(5) GDPR).

Furthermore, the principle of data minimalization implies that:

- Data should not be held for further use, unless this is essential for reasons that were stated in advance.
- Data should only include as much data as required to successfully answer the research question(s).
- Data collected for one purpose cannot be repurposed without further consent. However, certain exceptions to this rule apply, as discussed under Chapter 3.1.3 (Purpose limitation) above.

It has been observed that there is certain tension between complying with the principle of data minimalization and 'reaping the benefits of <<big data>>.'[18]

Guidelines: The need to ensure the usability of the Data in the INCISIVE repository for the development of artificial intelligence (AI) models has been carefully balanced with the requirements of data minimalization. In INCISIVE, the data minimalization principle is enacted through the use of: (i) tools for data de-identification, (ii) templates which allow only certain categories of Data to be submitted, (iii) curation tools. Furthermore, the proposed legal terms (see Chapter 8 below) also specify the purpose for which the data may be re-used and limit such re-use under the conditions of the INCISIVE Platform.

3.1.5 Accuracy

According to the accuracy principle, personal data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

The principle of accuracy is closely linked to the quality of data. It is argued that it applies to data itself, and not to further decisions made using the data (inferences drawn from that data).

Guidelines: Data Providers must take steps to ensure that Data are of representative quality and contain accurately annotated images and medical data. In particular the work undertaken in WP3 includes developing standards and guidelines for data submission and quality check tools to assist Data providers in correcting their data prior to the upload. For pseudonymous Data, in order to keep the data accurate and up-to-date, data subjects should have the

[18] Finck, Michèle & Biega, Asia. (2021). Reviving Purpose Limitation and Data Minimisation in Personalisation, Profiling and Decision-Making Systems, https://arxiv.org/ftp/arxiv/papers/2101/2101.06203.pdf.

opportunity to update their personal data when it is inaccurate, by contacting the relevant Data Provider.

3.1.6 Storage limitation

Under the storage limitation principle, personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. However, personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) GDPR subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of the data subject. This does not however imply that data stored for scientific research may be kept forever. Data Providers (and accordingly data subjects) must be informed about the retention period, or at least its basis and rationale. After this period lapses, the data must be removed or anonymized.

Guidelines: INCISIVE data sharing framework should include a limitation of storage term, which may be renewed for additional time. INCISIVE allows the Data Providers to withdraw the submitted Data in accordance with the data sharing agreement terms.

3.1.7 Integrity and confidentiality

Personal data must be protected by appropriate technical and organisational measures to ensure its confidentiality, integrity and availability, as provided in Article 32 GDPR[19]. For this, the state of the art must be considered, as well as the costs of implementation and the nature, scope, context and purposes of processing, including the risk of varying likelihood and severity for the rights and freedoms of natural persons.

Guidelines: In general, any research concerning the processing of health data presents significant risks to the data subjects. Due to novel federated learning approach and multiple data sources, the activities performed in INCISIVE present elevated privacy, security and ethics risks. For this reason, INCISIVE conducts several iterations of data protection impact assessments (DPIA), which result in mapping of the risks and outlining mitigations measures, to be implemented by the INCISIVE partners. INCISIVE also prepared a list of technical and organizational measures (TOMs) which protect the data in the Repository, as well as guidelines for the individual Data Providers for deployment of Federated Nodes.

[19] Measures that can be taken include: (i) the pseudonymization and encryption of personal data; (ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (iii) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; (iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

3.1.8 Roles of the involved parties

Moreover, under the general umbrella of accountability responsibility for addressing obligations under the GDPR with respect to handling Data should be assigned to involved parties.

The personal data processing operation must be conducted under the responsibility of a controller. A controller is, according to Article 4(7) GDPR '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.' If two or more entities participate in the determination of the purposes and means of a processing operation, they would qualify as 'joint controllers'.

A controller (or joint controllers) may use a processor, defined by Article 4(8) GDPR as 'a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.' Given the importance of the proper understanding of the roles of the involved actors, the EDPB provided further guidance on this matter in Guidelines 07/2020 on the concepts of controller and processor in the GDPR ('Guidelines 07/2020').[20] Some of the important points included in this guidance are:

- First, a data controller is usually the organisation as such, and not an individual within the organisation (such as the CEO, an employee or a member of the board), that acts as a controller.
- Second, the controller decides on the key elements i.e. determines the purposes (why?) and means (how?) of the processing operation. The controller must decide on both purposes and means. However, some more practical aspects of implementation ('non-essential means') can be left to the processor. Importantly, the controller does not necessarily need to *access* the data to be qualified as a controller.
- Third, as processing operations are becoming exceedingly complex, it is possible that multiple entities can be designated as joint controllers. As noted by the EDPB guidelines, joint participation can take the form of a common decision taken by two or more entities or result from converging decisions by two or more entities, where the decisions complement each other and are necessary for the processing to take place in such a manner that they have a tangible impact on the determination of the purposes and means of the processing. An important criterion is that the processing would not be possible without both parties' participation in the sense that the processing by each party is inseparable, i.e. inextricably linked.[21] Joint controllers should determine and agree on their respective responsibilities for compliance with the obligations under the GDPR in a binding document.[22] It is, however, important to distinguish the case where controllers act jointly for the same purpose from the situation where multiple entities each pursue their own means and purposes. As noted by the EDPB, the fact that several

[20] Guidelines 07/2020 on the concepts of controller and processor in the GDPR, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_en
[21] Guidelines 07/2020, pg. 3.
[22] Article 26 GDPR.

actors are involved in the same processing does not mean that they are necessarily acting as joint controllers of such processing.[23] For example, exchange of a set of data without jointly determined purposes or means of processing should be considered a transmission of data between two independent controllers. Using a shared infrastructure by different controllers does not necessarily entail joint controllership. On the other hand, existence of joint responsibility does not necessarily imply equal responsibility of the various operators involved in the processing of personal data. The Court of Justice of the European Union (CJEU) in its rulings[24] clarified that those operators may be involved at different stages of that processing and to different degrees so that the level of responsibility of each of them must be assessed with regard to all the relevant circumstances of the particular case.

- Forth, regarding the processor, the GDPR assumes this entity to act under delegation by the controller and cannot process the data otherwise than according to the controller's instructions. Such delegation should be governed by a controller-processor agreement (data processing agreement, DPA), construed in compliance with Article 28 GDPR. As noted, while the processor may have some leeway to determine the non-essential aspects of the means of the processing, they should have no say over the purposes of the processing.

In the Guidelines 07/2020, the EDPB provides several illustrative examples. On of those examples relates to research projects, where the guidelines state that 'Several research institutes decide to participate in a specific joint research project and to use to that end the existing platform of one of the institutes involved in the project. Each institute feeds personal data it already holds into the platform for the purpose of the joint research and uses the data provided by others through the platform for carrying out the research. In this case, all institutes qualify as joint controllers for the personal data processing that is done by storing and disclosing information from this platform since they have decided together the purpose of the processing and the means to be used (the existing platform). Each of the institutes however is a separate controller for any other processing that may be carried out outside the platform for their respective purposes.'

Guidelines: To impose a proper structure of data sharing framework in INCISIVE project it was necessary to carry out an assessment of roles of stakeholders of the data sharing, including Data Providers and Data Users. Once this was determined, the policy framework and data sharing agreements were drafted to follow to ensure clear allocation of the obligations and rights with respect to the collection, storage and sharing of Data. More details on the roles allocation and the agreements are provided below in Chapters 6 and 8.

[23] See Guidelines 07/2020, pg. 24.

[24] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie, (C- 210/16), Tietosuojavaltuutettu v Jehovan todistajat — uskonnollinen yhdyskunta (C-25/17), Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV (C-40/17).

3.2 Data Governance Act

The aim of Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act, DGA)[25] is to improve the conditions for data sharing in the EU internal market, by creating a harmonised framework for data exchanges and laying down certain basic requirements for data governance[26]. More specifically, DGA regulates:

- conditions for the re-use, within the EU, of certain categories of data held by public sector bodies;
- notification and supervisory framework for the provision of data intermediation services;
- a framework for voluntary registration of entities which collect, and process data made available for altruistic purposes (data altruism) and
- a framework for the establishment of European Data Innovation Board.[27]

DGA was adopted on 30 May 2022, entered into force on 23 June 2022 and, following a 15-month grace period, will be applicable from 24 September 2023. Both personal and non-personal data are in scope of the DGA, and wherever personal data is concerned, the GDPR applies.

Below, we describe the guidelines related to data intermediation services and data altruism, as most relevant for INCISIVE and its future sustainability planning.

3.2.1 Data intermediation services under the DGA

DGA defines 'data intermediation service' as a service which aims to establish commercial relationships for the purposes of data sharing between an undetermined number of data subjects and data holders on the one hand and data users on the other, through technical, legal or other means, including for the purpose of exercising the rights of data subjects in relation to personal data[28].

Recitals of the DGA provide that examples of such services can include:

- data marketplaces on which undertakings could make data available to others,
- orchestrators of data sharing ecosystems that are open to all interested parties, for instance in the context of common European data spaces,
- data pools established jointly by several legal or natural persons with the intention to license the use of such data pools to all interested parties in a manner that all

[25] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022R0868.
[26] See Recital 3 DGA.
[27] See Article 1.1 DGA.
[28] See Article 2(11) DGA.

participants that contribute to the data pools would receive a reward for their contribution.[29]

Importantly, the recitals indicate certain services which should be excluded from the scope of DGA's data intermediation services definition, such as:

- services that obtain data from data holders and aggregate, enrich or transform the data for the purpose of adding substantial value to it and license the use of the resulting data to data users, without establishing a commercial relationship between data holders and data users[30];
- services that are exclusively used by one data holder in order to enable the use of the data held by that data holder, or that are used by multiple legal persons in a closed group, including supplier or customer relationships or collaborations established by contract, in particular those that have as a main objective to ensure the functionalities of objects and devices connected to the Internet of Things[31];
- services that focus on the intermediation of copyright-protected content[32];
- data sharing services offered by public sector bodies that do not aim to establish commercial relationships[33].

3.2.2 Requirements for providing data intermediation services

Under DGA, a provider which intends to provide the data intermediation services (data intermediation services provider, DISP) must submit a notification to the competent authority in the Member State where it is established. DISPs located outside of EU will have to appoint a representative in the EU[34].

Further, DISP must observe a number of requirements when providing the service. They include[35]:

- provisions regarding DISP's independence:
  - DISP must provide data intermediation services through a separate legal person;
  - DISP's commercial terms, including pricing, cannot be dependent upon use of other services provided by the provider or by a related entity;
- restrictions on the use of data:
  - DISP cannot use the data for which it provides data intermediation services for purposes other than to put them at the disposal of data users;

[29] See Recital 28 DGA.
[30] See Recital 28 DGA.
[31] See Recital 28 DGA.
[32] See Recital 29 DGA.
[33] See Recital 29 DGA.
[34] See Article 11.1-4 DGA.
[35] See Article 12 DGA.

    - DISP is limited in using the data collected for the purpose of provision of the services; they may only use such data for the development of the data intermediation service, including detection of fraud or cybersecurity;
- provisions on data format and additional tools for the users:
    - DISP must facilitate the exchange of the data in the format in which it receives it from a data subject or a data holder;
    - DISP can convert the data into specific formats only to enhance interoperability within and across sectors or if requested by the data user or required by law; opt out possibility must be available;
    - DISP may offer additional specific tools and services to data holders or data subjects for the specific purpose of facilitating the exchange of data, such as temporary storage, curation, conversion, anonymisation and pseudonymisation. Those tools can only be used at the explicit request of the data holder or data subject;
- provisions on transparency and fairness towards data subjects, holders and users:
    - DISP must ensure that the procedure for access to its service is fair, transparent and non-discriminatory for both data subjects and data holders, as well as for data users, including with regard to prices and terms of service;
- provisions on tracking of intermediation activity, ensuring security of data, fraud prevention and continuity of services:
    - DISP must maintain a log record of the data intermediation activity;
    - DISP must put in place adequate technical, legal and organisational measures in order to prevent the transfer of or access to non-personal data that is unlawful;
    - DISP must inform data holders in the event of an unauthorised transfer, access or use of the non-personal data that they shared;
    - DISP must take necessary measures to ensure an appropriate level of security for the storage, processing and transmission of non-personal data and highest level of security when storing or sharing competitively sensitive information;
    - DISP must have procedures in place to prevent fraudulent or abusive practices in relation to parties which want to access the data;
    - in the event of its insolvency, DISP must ensure a reasonable continuity of the provision of its data intermediation services, including for the storage of data;
- provisions regarding interoperability:
    - DISP must take appropriate measures to ensure interoperability with other data intermediation services, for e.g. by means of commonly used open standards.

DISPs which offer services to data subjects must act in the data subjects' best interest where it facilitates the exercise of their rights. Additional requirements apply to DISPs which provide tools for obtaining consent from data subjects or permissions to process data made available by data holders.

A DISP which obtained confirmation from the authority that it provides the services in accordance with the DGA requirements may use the label of 'data intermediation services provider recognised in the Union' as well as a common logo (still to be developed)[36]. DISPs are subject to monitoring of compliance by competent authorities established in each Member State[37].

3.2.3 Data altruism under the DGA

Data altruism means voluntary sharing of data on the basis of: the consent of data subjects to process personal data pertaining to them, or permissions of data holders to allow the use of their non-personal data, without seeking or receiving a reward that goes beyond costs they incur where they make their data available and for objectives of general interest as provided for in national law[38]. Those objectives may include, where applicable, for example healthcare, combating climate change, improving mobility, facilitating the development, production and dissemination of official statistics, improving the provision of public services, public policy making or scientific research purposes in the general interest.

While DGA does not preclude national policies for data altruism, it sets down rules for recognised data altruism organisations. Organizations may apply for registration in the public national register of recognised data altruism organisations and use the label 'data altruism organisation recognised in the Union' in its written and spoken communication, as well as a common logo.

An organisation which carries out data altruism activities must fulfil a number of requirements to qualify for registration in a public national register of recognized data altruism organizations (RDAO), in particular, it must:

- operate on a not-for-profit basis;
- be a legal person established according to the national law and be legally independent from any entity that operates on a for-profit basis;
- carry out its data altruism activities through a structure that is functionally separate from its other activities;
- comply with the rulebook adopted by the EC[39].

Furthermore, during its operation a RDAO must also observe certain requirements, such as:

[36] See Article 11.9 DGA.
[37] See Article 14 DGA.
[38] Modified from definition in Article 1(16) DGA.
[39] See Article 18 DGA.

- comply with transparency requirements e.g. keep full and accurate records concerning the persons or entities which provided data, duration of the processing of this data, purpose of it and fees paid[40];
- file an annual activity report with the competent authority[41];
- inform the data subject and data holders about, *inter alia*, objectives of general interest, purpose for which their data will be processed[42] and tools for obtaining consent or permission for processing and withdrawing it[43];
- take measures to ensure an appropriate level of security for the storage and processing of non-personal data that it has collected based on data altruism[44] and inform about data holders about unauthorized disclose or breach of their non-personal data[45];
- refrain from using the entrusted data for other objectives than those of general interest for which the data subject or data holder allows the processing;
- refrain from using misleading marketing practices to solicit the provision of data.[46]

In order to facilitate the collection of data based on data altruism, EC will be empowered to adopt European data altruism consent form.[47]

3.2.4 Other relevant provisions of the DGA

DGA refers to European data spaces[48] and future specific rules applicable to them. EHDS (described below) is to be an example of such data space. Last but not least, DGA introduces the concept of secure processing environment[49] which - while mostly applicable to accessing data made available by public sector bodies - could be a standard which could be referred to by other data sharing infrastructures.

Guidelines: Currently the DGA is not yet applicable (it will become applicable from 24 September 2023). However bearing in mind the timeframe of the project, the requirements of DGA need to be observed during implementation and sustainability planning. It should be noted that if the INCISIVE Platform will aim to establish commercial relationships for the purposes of data sharing between the Data Providers and the Data Users, the requirements of

[40] See Article 20.1 DGA.
[41] See Article 20.2 DGA.
[42] See Article 21.1 DGA.
[43] See Article 21.3 DGA.
[44] See Article 21.4 DGA.
[45] See Article 21.5 DGA.
[46] See Article 21.2 DGA.
[47] See Article 25 DGA.
[48] See Recital 2 DGA.
[49] Under Article 1(2) secure processing environment means the physical or virtual environment and organisational means to provide the opportunity to re-use data in a manner that allows for the operator of the secure processing environment to determine and supervise all data processing actions, including to display, storage, download, export of the data and calculation of derivative data through computational algorithms.

data intermediation services provider (DISP) will apply. Since this is not presently the case, the requirements of DISP are not applicable in the present state of work. However, depending on the sustainability of model of INCISIVE, DGA may become applicable, if INCISIVE establishes an entity which provides data intermediation services or becomes a data altruism organization. Further recommendations will be provided in connection with the works of WP8 (sustainability planning).

3.3 European Health Data Space Regulation

The proposal for European Health Data Space Regulation[50] (EHDS) was published on 3 May 2022 and is currently undergoing the legislative process. When implemented, the regulation will be the most relevant EU act concerning health data. The overarching purpose of EHDS[51] is to strengthen patients' rights to their health data and to open up the registries containing electronic health data (see definition below), to make better use of it, both for the patients and the larger community.

3.3.1 Primary and secondary use of electronic health data

The term 'electronic health data' (EHD)[52] covers both personal electronic health data (i.e. data concerning health and genetic data as defined in the GDPR, as well as data referring to determinants of health, or data processed in relation to the provision of healthcare services, processed in an electronic form) and non-personal electronic health data (data concerning health and genetic data in electronic format that falls *outside* the definition of personal data provided in GDPR). Such broad definition is intended to capture all categories of health data, irrespective of the source of this data (from patient or from another person, such as a health professionals) and include also inferred and derived data, such as diagnostics, tests and medical examinations, as well as data observed and recorded by automatic means.[53]

EHDS builds of two pillars and regulates them separately, namely:

- Primary use of electronic health data[54] - referring to data in the context of healthcare. This would cover use of data for treating the patient, but also the prescription and

[50] Text of the EHDS Regulation proposal is available https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52022PC0197.

[51] Specific goals set by the proposal in Article 1 include: (i) reinforcing the rights of natural persons (patients) in relation to the availability and control of their electronic health data; (ii) providing rules and mechanisms supporting the research and fact-based policy making with the use of electronic health data; (iii) laying down harmonized requirements for electronic health records ("EHR") systems on the EU market; (iv) establishing mandatory cross-border infrastructure enabling the primary and secondary use of electronic health data across the EU

[52] See Article 2 (2) (a) - (c) EHDS Regulation proposal.

[53] See recital 5 EHDS Regulation proposal.

[54] See Article 2 (2) (d) EHDS Regulation proposal.

dispensation of medicinal products and medical devices, as well as for relevant social security, administrative or reimbursement services.

- Secondary use of electronic health data[55] - use of data for other purposes that benefit the society such as research, innovation, policy-making, patient safety, personalised medicine, official statistics or regulatory activities.

3.3.2 Sharing electronic health data for research purposes under EHDS

The eco-system for secondary use of electronic health data, which includes re-use of data for research, will be built on three actors: (i) health data access bodies, (ii) data holders and (iii) data users.[56]

(i) Health data access bodies (HDAB) will be authorities set up by the Member States. They will be responsible for - among other tasks[57] - granting access to electronic health data for secondary purposes[58]. These bodies will examine the applications from potential users and issue data permits i.e. administrative decisions which allow a data user to access data. Purposes for which the data can be used[59] and conditions for obtaining the data permit[60] are specified in the EHDS proposal. Those authorities can also pre-process the requested data to prepare it for the data user e.g. compile data from various data holders. They may also support the development of AI systems and development of harmonised standards under AI Act for the training, testing and validation of AI systems in health.[61] Health data access bodies will keep a national dataset catalogue with a list of available datasets, in which each dataset will be described, including: data source, the scope, the main characteristics, nature of electronic health data and conditions for making data available. The National catalogues will be connected by EU Datasets Catalogue.[62]

The HDAB will thus act as intermediaries between the data holders, potential users of the data (such as researchers or companies wishing to use the data for their research and development), but also patients. For example, they will informing the public about conditions under which electronic health data is made available.[63] Furthermore, if during the research there is a finding that may impact on the health of a natural person, the health data access body may inform the natural person and his/her health professional about that finding. Moreover, HDAB will enforce the obligations of the EHDS regulation with regard to data users and holders.[64]

---

[55] See Article 2 (2) (e) EHDS Regulation proposal.
[56] See Chapter IV of the EHDS Regulation proposal.
[57] See Article 37 EHDS Regulation proposal.
[58] See Article 37 EHDS Regulation proposal.
[59] See Article 34 EHDS Regulation proposal.
[60] See Article 44-47 EHDS Regulation proposal.
[61] See Article 37 (1) EHDS Regulation proposal.
[62] See Article 37 (1) (q) EHDS Regulation proposal.
[63] See Article 38 (1) EHDS Regulation proposal.
[64] See Article 43 EHDS Regulation proposal.

(ii) Data holder is a concept which is crucial for the EHDS. Under the proposed definition it is 'any natural or legal person, which is an entity or a body in the health or care sector, or performing research in relation to these sectors, as well as Union institutions, bodies, offices and agencies who has the right or obligation, in accordance with this Regulation, applicable Union law or national legislation implementing Union law, or in the case of non-personal data, through control of the technical design of a product and related services, the ability to make available, including to register, provide, restrict access or exchange certain data'.[65] As clarified in the EHDS recitals[66] 'data, collected and processed by data holders with the support of Union or national public funding, should be made available by data holders to health data access bodies, in order to maximise the impact of the public investment and support research, innovation, patient safety or policy making benefitting the society'.

Data holders will need to inform the HDAB about their datasets and their characteristics. Moreover, the data holders will be obligated to make certain categories of electronic data available for secondary use and cooperate in good faith with health data access bodies.[67] The data which will need to be made available includes not only the content of EHRs, but also, for example, social, environmental and behavioural determinants of health, electronic health data from biobanks and dedicated databases, health-related administrative data. In principle, the access to data will be provided with an intermediation of HDAB, however – according to the proposal - single data holder in a single Member State may also directly grant data permit and provide the user with access to data in a secure processing environment (described below).[68]

Data holders may also provide a Union data quality and utility label on their datasets[69], if they fulfil principles defined by the EHDS regulation and the delegated acts. For some data sets (for

[65] See Article 2 (2) (y) EHDS Regulation proposal.
[66] See recital 40 EHDS Regulation proposal.
[67] See Article 41 EHDS Regulation proposal.
[68] See Article 49 (1) EHDS Regulation proposal.
[69] In particular, the data quality and utility label shall comply with the following elements:

- for data documentation: meta-data, support documentation, data model, data dictionary, standards used, provenance;
- technical quality, showing the completeness, uniqueness, accuracy, validity, timeliness and consistency of the data;
- for data quality management processes: level of maturity of the data quality management processes, including review and audit processes, biases examination;
- coverage: representation of multi-disciplinary electronic health data, representativity of population sampled, average timeframe in which a natural person appears in a dataset;
- information on access and provision: time between the collection of the electronic health data and their addition to the dataset, time to provide electronic health data following electronic health data access application approval;
- information on data enrichments: merging and adding data to an existing dataset, including links with other datasets.

e.g., those created with public funding, such as EU Horizon projects), adherence to those principles will be mandatory. In such case, the data holder should have 'sufficient documentation' for the health data access body to confirm the accuracy of the label.[70]

(iii) Data user means a natural or legal person who has lawful access to personal or non-personal electronic health data for secondary use[71]. Applicants who wish to become data users will have to request access to data either directly by the data holder (for data from a single data holder in a single Member State) held by or via the intermediation of HDAB. To do so, they will need to apply for the issuance of a data permit.

The application should provide the HDAB with information elements that would help the body evaluate the request[72]. Once approved, the data users will have the right to access and process the electronic health data in accordance with the data permit delivered to them on the basis of the regulation.[73]

However, use of the data will come with certain obligations. Namely, no later than 18 months after the completion of the electronic health data processing, data users will be obligated to make public the results or output of the secondary use of electronic health data. Those results or output shall only contain anonymised data. The data users will have to inform the HDAB from which a data permit was obtained and support them to make the information public on health data access bodies' websites.[74] Furthermore, they will need to acknowledge the electronic health data sources and the fact that electronic health data has been obtained in the context of the EHDS.[31] If the data is enriched, the dataset with such improvements and a description of the changes will be made available free of charge to the original data holder. They will also have to inform the HDAB of any clinically significant findings that may influence the health status of the natural persons whose data are included in the dataset.[75]

3.3.3 Fees for providing access to data

HDAB and single data holders may charge reasonable fees for making electronic health data available for secondary use.[76]

The EC will be empowered to adopt delegated acts to amend this list. Also, the EC can issue implementing acts to set out "visual characteristics and technical specifications of the data quality and utility label", based on the elements referred above.

[70] See Article 41 (3) EHDS Regulation proposal.

[71] See Article 2.2 z) EHDS Regulation proposal.

[72] For example: (i) purposes for which the data would be used, description of the needed data and possible data sources, (ii) a description of the tools needed to process the data, as well as characteristics of the secure environment (further described below) that are needed, (iii) when data is requested in pseudonymised format, the data applicant should explain why this is necessary and why anonymous data would not suffice and indicate legal basis for the processing (in accordance with Article 6 (1) GDPR).

[73] See Article 46 (7) EHDS Regulation proposal.

[74] See Article 46 (11) EHDS Regulation proposal.

[75] See Article 46 (12) EHDS Regulation proposal.

[76] See Article 42 EHDS Regulation proposal.

The fees may include and be derived from the costs related to conducting the procedure for requests, including for assessing a data application, granting the data permit or providing an answer to data request. For 'private' data holders (i.e. where the data is not held by data access body or a public sector body), the fee may also include compensation for part of the costs for collecting the data.[77]

Such fees may take into account the situation and interest of SMEs, individual researchers or public bodies. Disagreements on the fee amount may be resolved in front of dispute settlement bodies, which are to be established under the Data Act[78] (when enacted).

In order to ensure a harmonised approach concerning fee policies and structure, the Commission may adopt implementing acts for the fee policies and fee structures.

3.3.4 Secure processing environments

According to the EHDS proposal, data for secondary use should be provided in anonymized format or in pseudonymized format (only if the purpose of the data user's processing cannot be achieved with anonymised data). The information necessary to reverse the pseudonymisation shall be available only to the health data access body.

Furthermore, the secondary use access to the requested electronic health data should be done through a secure processing environment, with technical and organisational measures and security and interoperability requirements. In particular, the secure processing environment should[79]:

- restrict access to the secure processing environment to authorised persons listed in the respective data permit;
- minimise the risk of the unauthorised reading, copying, modification or removal of electronic health data hosted in the secure processing environment through state-of-the-art technological means;
- limit the input of electronic health data and the inspection, modification or deletion of electronic health data hosted in the secure processing environment to a limited number of authorised identifiable individuals;
- ensure that data users have access only to the electronic health data covered by their data permit, by means of individual and unique user identities and confidential access modes only;
- keep identifiable logs of access to the secure processing environment for the period of time necessary to verify and audit all processing operations in that environment;

---

[77] See Article 42 EHDS Regulation proposal.

[78] See Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), COM/2022/68 final https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A68%3AFIN.

[79] See Article 50 EHDS Regulation proposal.

- ensure compliance and monitor the required security measures to mitigate potential security threats.

Those requirements are applicable to both the environments for access to data for secondary use provided by health data access bodies and the data holders. The data users will only be able to download non-personal electronic health data from the secure processing environment. The Commission will, by means of implementing acts, provide for the technical, information security and interoperability requirements for the secure processing environments.

Guidelines: EHDS Regulation is currently at a proposal stage. Hence, there is no legal obligation stemming from the draft. Still, given the importance of the initiative, INCISIVE should observe the legislative process and consider the obligations which may arise once the EHDS Regulation is passed. In particular, the described EHDS obligations could relevant for Data Providers (acting as the data holders), quality of the contributed Data and the infrastructure in which the Data is shared for research purposes. One of the potential benefits of aligning of INICISIVE Platform with the requirements of the 'secure processing environment' would be the possibility to use this platform as means of sharing data by data holders under EHDS, if such possibility is provided for in the final version of the Regulation.

3.4 Database and IP rights

Intellectual property (IP) is a type of intangible property created by the human mind, such as inventions, works of art and literature, computer programs, data bases. There are various IP rights which are recognized by different legal systems.[80] Database and copyrights may be considered as possible IP rights in the context of INCISIVE datasets.

In the EU the databases are protected under uniform regime of Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases (Database Directive).

The Database Directive protects collections, sometimes called 'compilations', of works, data or other materials which are arranged, stored and accessed by means which include electronic, electromagnetic or electro-optical processes or analogous processes. Protection extends to collections of independent works, data or other materials which are systematically or methodically arranged and can be individually accessed.

In accordance with the Database Directive, the Member States were obligated to provide for a right for the maker of a database which made investments in creation of the database. The objective of this *sui generis* right (specific property right for databases) is to ensure protection of any investment in obtaining, verifying or presenting the contents of a database for the limited duration of the right. This right encompasses the right to prohibit extraction and re-utilization of the database or its substantial part. This right may be transferred or licensed and applies

[80] Broadly speaking, they can be grouped in the following main categories: (i) patents, (ii) trademarks and designs, (iii) copyright, (iv) database rights. Patent, trademarks, and design protection cannot be applied to datasets.

irrespective of the eligibility of that database for protection by copyright or by other rights and irrespective of eligibility of the contents of that database for protection by copyright or by other rights. The right of protection of databases is without prejudice to rights existing in respect of their contents. It runs for 15 years from the first of January of the year following the date of completion of the database. Provisions of Database Directive are without prejudice to data protection legislation (GDPR).[81]

Moreover, the Database Directive protects databases by copyright if they are original by reason of the selection or arrangement of their content. A collection of data may potentially be recognized as copyrightable work, if the selection of the data entries is a result of original creation. The copyright protection is rather unlikely in case of medical datasets, which lack of personal originality.

Guidelines: While there is still ongoing discussion on who (and if anyone) is the 'owner' of a set of medical data[82], arguably the sets of Data contributed by Data Providers may be protected under *sui generis* database rights. Data Providers invest time and effort into selection of the records comprising the shared Data, their curation, annotation and formatting. Hence, the terms of sharing of Data in the data donation legal framework should address the IP rights aspect of the sharing of the Data for the purpose of INCISIVE.

3.4.1 Legal arrangements for use of IP rights

The holders of IP rights can make their creations available for use and exploitation by third parties by way of several legal arrangements: transfer of IP rights, licensing of IP rights or joint ownership arrangements.

3.4.2 Transfer of IP rights

The holder of IP rights (sometimes referred to as the 'owner') may transfer (assign) them to another entity or person. In principle, with an IP assignment, all rights initially held by the holder to the piece of IP concerned are irrevocably transferred to a new holder ('owner'). Some exceptions may apply to this rule[83].

Once the IP assignment is finalised, typically the previous owner will have no further responsibility for that IP and they would not benefit from the possible commercial success of

---

[81] See recital 48 Database Directive.

[82] Prainsack, B. (2019). Data Donation: How to Resist the iLeviathan. In: Krutzinna, J., Floridi, L. (eds) The Ethics of Medical Data Donation. Philosophical Studies Series, vol 137. Springer, Cham. https://doi.org/10.1007/978-3-030-04363-6_2.

[83] For example, copyright protects two types of rights. Economic rights allow right owners to derive financial reward from the use of their works by others. Moral rights allow authors to take certain actions to preserve and protect their link with their work (e.g. right to be recognized as author, right to integrity of the work). Economic copyrights may be transferred, but many countries do not allow assignment or waiver of moral rights.

the product or service containing such IP[84]. Additionally, they would not be allowed to use (exploit) the IP concerned, unless this was exceptionally allowed in the assignment agreement.

3.4.3 Licensing of IP

An IP license is an agreement in which the holder of intellectual property rights (licensor) gives permission to another entity (licensee) to use their IP. The licensor keeps their right over the IP, which means that there is no transfer of ownership. The license may be exclusive or non-exclusive.

- Exclusive license means that no person or entity other than the licensee can exploit the relevant IP rights. Importantly, the licensor is also excluded from exploiting the IP rights. If the licensor wishes to use the exclusively licensed IP rights (for example, for conducting its own research) or they had previously granted any license in relation to the same IP, the exclusive licence will need to expressly state that it is exclusive subject to those carve-outs. Some jurisdictions recognize a sub-type of an exclusive license ('sole license') i.e. agreement under which the owner of IP can grant only one license and is able to use the IP themselves.
- A non-exclusive licence allows the licensee to use the IP in an agreed way, but means that the licensor may exploit the same IP and/or to allow any number of other licensees to do so.

Additionally, licenses (either exclusive or non-exclusive), may be limited in scope, for example to use the IP for a certain purpose or within a specified geographical area. The license may be concluded for a specified time or for an indefinite term.

The licensor should also decide whether the licensee can grant further licenses (sub-licenses). Typically, in a non-exclusive license, the licensor retains the right to grant licenses and thus sub-licensing is not allowed.

In exchange for use of the IP rights, the licensor may receive royalties for giving permission; however free of charge licenses are also possible. Some recognized 'free' license terms are Creative Commons licenses[85] or different types of open licenses for software[86]. It should be mentioned, that while such licenses do not require compensation to be paid, they still impose certain restrictions on how the licensed asset can be used. For example, they may require the licensee to give credit to the licensor, use the IP rights only for non-commercial purpose or to license any new IP asset created on the basis of the licensed asset ('adaptation') under the same license terms to other users.

---

[84] Some exceptions may apply e.g. for certain types of copyrightable works under Directive 2001/84/EC of the European Parliament and of the Council of 27 September 2001 on the resale right for the benefit of the author of an original work of art.

[85] See https://creativecommons.org/about/cclicenses/

[86] See https://opensource.org/licenses

3.4.4 Joint-ownership (co-ownership) agreements

Joint ownership of an IP right may arise if there is more than one party which contributed to the creating of an IP asset. If such joint ownership is likely to arise, it is beneficial to pre-empt this and put in place a joint ownership agreement to regulate the use of the joint IP right. When joint-ownership is not regulated between the owners, this is likely to lead to disagreements and legal disputes.

Guidelines: The above models of legal arrangements were presented and discussed during the T7.4 work in the context of data donation legal framework and the Project DoA requirements. It was concluded that despite the use of the term 'donation' of Data in the DoA[87], transfer of ownership of the Data to INCISIVE Project (or individual Data Users) would not be desirable for the Data Providers, as they would then be deprived of the possibility to use their Data for other purposes. Also, it would be in contradiction to the DoA requirement of ensuring that the Data Providers keep control over the shared Data. Hence, the model which was selected as most appropriate for the data sharing legal framework was a non-exclusive license to use Data in the INCISIVE Repository.

3.5 Other acts

3.5.1 Digital Services Act

The Digital Services Act (DSA)[88] entered into force on 16 November 2022, but will be fully applicable from 17 February 2024. DSA applies to intermediary services, which include mere conduit services, caching services and hosting services[89]. Given the broad definition, it may potentially apply to a wide range of online intermediaries, however most of its provisions are aimed at consumer facing, large commercial platforms (such as online marketplaces, social networks, content-sharing platforms, app stores, and online travel and accommodation platforms).

Guidelines: DSA does not contain provisions on data governance in the research context. Some of the rules provided in the DSA for online platforms may be of relevance for INCISIVE, if the services are available to broader public (post-project). For example, the rules on liability of intermediary services[90] or transparency obligations regarding their terms and conditions.[91] However, very small platforms are exempt from the majority of obligations of the DSA.

---

[87] See also clarificatory comments in Chapter 2.1.

[88] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), https://eur-lex.europa.eu/search.html?scope=EURLEX&text=Digital+Services+Act&lang=en&type=quick&qid=1671104997848

[89] See Article 3(a) and (g) DSA.

[90] See Chapter II DSA.

[91] See Article 14 DSA.

3.5.2 Digital Markets Act

The aim of Digital Markets Act (DMA)[92], which entered into force on November 1, 2022[93], is to ensure that the large online platforms behave in a fair way. To this end, DMA sets rules for providers of core platform services[94] designated as a gatekeepers. Gatekeepers are large platforms that have a significant impact on the EU market, provide an important gateway for business users to reach end users and enjoy an entrenched and durable position (or will do so in the future).[95] All the qualitative criteria must be fulfilled simultaneously.[96] These gatekeeper platforms fall in the scope of DMA and will have to comply with a series of obligations and prohibitions. These include among others:[97] prohibitions on tying, on interoperability restrictions, on use of competitors' data or on self-preferencing and obligations on providing information on user data and on performance data or on access at FRAND conditions. The DMA also includes extensive reporting duties.

Guidelines: The INCISIVE Platform does <u>not</u> meet the conditions defined by the DMA and would <u>not</u> be considered a 'gatekeeper'. Thus, it is outside of the scope of requirements and restrictions provided for by the DMA.

3.5.3 P2B Regulation

Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services (P2B Regulation)[98] applies to (i) providers of online intermediation services (online platforms) and (ii) online search engines[99] provided to business users and corporate website users established in the EU, where those business users and corporate website users offer goods or services to consumers located in the EU through those online intermediate services or online search engines. The goal of P2B Regulation is to ensure a fair, predictable, sustainable and trusted online business environment that enables businesses to operate across borders in the internal

---

[92] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R1925&qid=1671105300967.

[93] Certain DMA rules will start to apply from 2 May, 2023, but most obligations will start applying later, with DMA fully applicable in March 2024.

[94] These services are: online intermediation services such as app stores, online search engines, social networking services, certain messaging services, video sharing platform services, virtual assistants, web browsers, cloud computing services, operating systems, online marketplaces, and advertising services provided together with the above listed services (Article 2(2) DMA).

[95] See detailed definitione in Article 3(1) DMA.

[96] For each of these qualitative criteria, the DMA provides certain quantitative thresholds that, if met, create a presumption that the qualitative criteria are met.

[97] See Chapter III DMA.

[98] Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019R1150

[99] As defined in Article 2(2) and (5) of the P2B Regulation respectively. .

market. To this end, P2B Regulation requires providers of online platforms to create a fair and transparent framework for their services, including: clear and transparent terms and conditions, rules for restriction, suspension and termination of services, internal complaints system. The P2B Regulation also provides certain limited obligations for search engines (Google search, Bing). In essence, the aim of the P2B Regulation is providing rules for commercial undertakings (e.g. Amazon Marketplace, eBay) which allow business users to offer goods or services to consumers.

In more detail, services qualify as 'online intermediation services'[100] if they meet all of the following requirements: (i) they constitute information society services within the meaning of point (b) of Article 1(1) of Directive (EU) 2015/153515, (ii) they allow 'business users' to offer goods or services to 'consumers', (iii) with a view to facilitating the initiating of 'direct transactions' between the business users and the consumers, regardless of where the direct transactions are ultimately concluded; and (iv) they are provided to 'business users' on the basis of contractual relationships between the provider of the services and the business users.[101]

Provider of search engine is a (i) a digital service, (ii) that allows users to input queries, (iii) to perform searches of, in principle, all websites, or all websites in a particular language, (iv) on the basis of a query on any subject, (v) in the form of a keyword, voice request, phrase or other input, and (vi) returns results in any format in which information to the requested content can be found.

Guidelines: The goal of INCISIVE Platform is to – among others - provide access to data for researchers. Despite it being a platform, it does not seem to fit the conditions of online intermediation service defined above. In particular, it does not facilitate direct transactions between data providers and consumers. Currently INCISIVE only provides search functionality limited to its own contents. Thus, it is also not an online search engine in the meaning of the Article 2(5) of P2B Regulation. Should the goals and functionalities of the Platform evolve during further stages of development (during sustainability phase), additional evaluation should be performed.

3.5.4 NIS 2

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148

[100] See Article 2(2) P2B Regulation.

[101] Questions and Answers: Establishing a Fair, Trusted and Innovation Driven Ecosystem in the Online Platform Economy, provided by the European Commission's services for information purposes only, https://digital-strategy.ec.europa.eu/en/library/qa-platform-business-small-businesses-and-other-online-operators

(NIS2)[102] was published on 27 December 2022. NIS2 will need to be transposed to national laws by October 2024.

NIS2 will replace the current directive on security of network and information systems (NIS Directive[103]). Current NIS Directive applies to operators providing essential services (certain entities in the sectors of energy, transport, finance, health sector, drinking water, digital infrastructure) and digital service providers. Specifically in the health sector, NIS Directive applies to 'health care settings (including hospitals and private clinics)', however exact applicability depends on the local implementation.[104] NIS Directive has been criticized for its ineffectiveness and not being par with the emerging cyber threats.

The newly adopted NIS2 will enhance and harmonise cybersecurity requirements in the EU countries, setting baseline rules for cybersecurity risk management measures and reporting obligations across the sectors that are covered by the directive. Compared with NIS Directive, NIS2 will expand the list of entities in scope, and those covered will be divided into categories of 'essential' and 'important' entities. In the sector of health, for example healthcare providers, EU reference laboratories, entities carrying out research and development activities of medicinal products, manufacturers of basic pharmaceutical products and critical medical devices, as well as research organizations[105] will fall into the scope of the enhanced cybersecurity requirements, provided that they fulfil the size thresholds specified in NIS2 ('size cap rule').

The covered entities will need to take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities use, for example: incident handling policies, supply chain security, policies on risk analysis and information system security and other. They will also have to report certain incidents[106] to computer security incident response teams (CSIRTs) or competent authorities. Management of the essential and important entities will be responsible for implementation and supervision of their organisation's compliance with the new rules.

---

[102] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

[103] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

[104] Healthcare providers as defined in point (g) of Article 3 of Directive 2011/24/EU of the European Parliament and of the Council.

[105] Annex I and Annex I of NIS 2. According to recital 36, research organisations should be understood to include entities which focus the essential part of their activities on the conduct of applied research or experimental development, within the meaning of the Organisation for Economic Cooperation and Development's Frascati Manual 2015: Guidelines for Collecting and Reporting Data on Research and Experimental Development, with a view to exploiting their results for commercial purposes, such as the manufacturing or development of a product or process, the provision of a service, or the marketing thereof.

[106] Under Article 6(6) 'incident' means an event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems.

Guidelines: NIS Directive does not apply to research platforms such as INCISIVE. Despite the broadened scope, also NIS2 will not apply to data sharing platforms/infrastructures as such. However, if in the post-project stage, the INCISIVE Platform is run by a research organisation, requirements of NIS2, when implemented into national laws, may be appliable to such organisation's cyber security risk compliance.

3.5.5 National laws

Although EU laws include harmonising rules, privacy and data protection law, ethics and security requirements in the health sector remain to a large extent a matter of national or state law and interpretation.

Guidelines: INCISIVE Project activities, including feasibility and prospective studies, are subject to supervision from the ethics committees or a similar bodies in line with national compliance requirements. This has been reported in D7.2. Notwithstanding this, Data Providers' sharing their Data with the INCISIVE Repository must do so in accordance with their national laws and should observe the rules of national compliance supervision, in particular seek necessary approvals from appropriate ethics committees.

4 Ethics of data donation

Ethics of data donation (provision) addresses the ethical issues that arise when individuals donate (share) their personal data for research purposes. This includes issues such as informed consent, data ownership, confidentiality, data security, and data anonymization.

One of the main reasons why ethics of data donation (provision) is important is because of the potential risks to individuals' privacy and autonomy.[107] Personal data can be used to identify individuals, and in some cases, sensitive personal information can be used to discriminate against certain groups of people.[108]

Additionally, individuals may not always be fully aware of the risks and benefits of data donation,[109] which raises questions about informed consent. Furthermore, the increasing reliance on personal data in research and other domains makes it more important than ever to ensure that ethical principles are upheld. Ethics of data donation can help ensure that individuals' rights and interests are protected, while also enabling important scientific and social progress[110]. By promoting ethical practices in data donation, we can help ensure that the benefits of data-driven research and innovation are realized while also respecting individuals' rights and privacy.[111]

There are several important ethical considerations[112] that should be taken into account when it comes to data donation. These include:

- Informed Consent: Individuals should be fully informed about the purpose and risks of data donation before providing their data. They should also have the right to withdraw their consent at any time.
- Data Ownership: Data donors should be informed about who will have ownership and control over their data, and how it will be used.

---

[107] Porsdam Mann S, Savulescu J, Sahakian BJ. Facilitating the ethical use of health data for the benefit of society: electronic health records, consent and the duty of easy rescue. Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences. 2016 Dec 28;374(2083):20160130.

[108] Mantelero A. Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection. Computer law & security review. 2016 Apr 1;32(2):238-55.

[109] Jones KH. Incongruities and Dilemmas in Data Donation: Juggling Our 1s and 0s. The Ethics of Medical Data Donation. 2019:75-93.

[110] Riso B, Tupasela A, Vears DF, Felzmann H, Cockbain J, Loi M, Kongsholm NC, Zullo S, Rakic V. Ethical sharing of health data in online platforms–which values should be considered?. Life sciences, society and policy. 2017 Dec;13:1-27.

[111] Vayena E, Tasioulas J. The dynamics of big data and human rights: The case of scientific research. Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences. 2016 Dec 28;374(2083):20160129.

[112] Krutzinna J, Floridi L. The ethics of medical data donation. Springer Nature; 2019.

- Confidentiality: Measures should be put in place to protect the confidentiality of data donors and prevent the unauthorized use or disclosure of their data.
- Data Security: Data donors should be assured that their data will be stored and transmitted securely, and that appropriate safeguards will be in place to prevent data breaches.
- Data Anonymization: In order to protect privacy, data should be anonymized whenever possible, so that it cannot be traced back to the individual.
- Fairness and Justice: Data donation should not lead to any unfair or discriminatory practices and should not result in harm to vulnerable populations.
- Transparency: Data donors should be informed about the use of their data, how it will be analysed, and who will have access to it.

The INCISIVE partners have been advised and supported to ensure that data donation is carried out in a responsible and ethical way that respects the privacy and rights of individuals by taking these ethical issues into account. For prospective data collection, this includes the process of obtaining informed consent which should be preceded by the provision of a participant information sheet. The latter includes information about research aims, risks and benefits. In order to avoid any illegal access, use, or disclosure of donated data, data privacy and security also necessitate sufficient safeguards. Data transparency is crucial because it helps to build trust in the research process and accountability by letting contributors know how their data is being used. Last but not least, fair, and equitable data use refers to the use of data in a way that respects the privacy and autonomy of the donor and makes sure that the benefits of the research are distributed fairly. To keep the public's trust and make sure that research is carried out in an ethical and responsible manner, data donation must adhere to ethical guidelines.

5 Standards in data donation

5.1 Data standards

In the inclusion of the FAIR principles in the INCISIVE platform, the use of worldwide standards (HL7 FHIR[113] message with SNOMED CT[114] and LOINC[115] codes, and DICOM[116], NIFTI[117] for medical images) is important to guarantee a common data model between several Data Providers under the same architecture in the Federated Nodes and the Central Node.

INCISIVE enables a virtual environment for all Data Providers with all the necessary systems and databases to ensure the same standardized process from multiple sources. Data and images are processed locally at the Federated Nodes (or Central Node, if chosen by the Data Provider) and must never leave their facilities, either to be processed or to be ingested into their local storage. Data providers Federated Nodes' ETL tool ensures the harmonization of Data in a common data model to share them in a standard way and enable federated AI training. More specifically, the Data Providers fill clinical data into an Excel template and upload it to the ETL tool. The same process takes place for medical images and annotations, which are compressed by Data Providers with DICOM files and NIFTI annotations and are also uploaded to the ETL tool of their Federated Node. It is the Data Provider's responsibility to use the quality check tool to validate that the uploaded data is correct and will be useful for AI training.

The ETL tool transforms the Excel template into an HL7 FHIR message with SNOMED CT and LOINC codes to preserve the semantic meaning of all clinical information exchanged. It also processes and stores medical images and annotations from DICOM and NIFTI files. The message with all clinical data is stored on the local FHIR server and the medical images and notes are stored on the local PACS, both of which ensure the localization, accessibility, interoperability and reuse of the Data within each Data Provider's Federated Node.

AI researchers run the AI training models that return the result and display it in the UI, the data used by the AI training models is fetched and processed within each Federated Node.

For more detail, the entire Common Data Model (CDM) will be explained in the INCISIVE Interoperability Framework.

[113] https://hl7.org/fhir/index.html
[114] https://www.snomed.org/
[115] https://loinc.org/
[116] https://www.dicomstandard.org/
[117] https://nifti.nimh.nih.gov/

5.2 Legal standards

5.2.1 Data Use Ontology (DUO)[118]

The (GA4GH) Data Use Ontology (DUO) includes terms describing data use conditions, particularly for research data in the health/clinical/biomedical domain. The goal of this resource is to allow large genomics and health data repositories to share the same terminology when describing data use conditions. DUO aims to support services that allow advanced search options by matching a research purpose to datasets tagged with compatible data use restrictions terms. In the context of INCISIVE the DUO codes are not used, as the selected model for data submission provides for uniform conditions of use of data in the Repository (See Chapter 6 below).

5.2.2 Framework for responsible sharing of genomic and health-related data[119]

The framework for responsible sharing of genomic and health-related data was developed under the auspices of the Global Alliance for Genomics and Health to establish a harmonized approach to enable effective and responsible sharing of genomic and clinical data and to catalyse data sharing projects that drive and demonstrate the value of data sharing. The vision of the framework was to establish a set of foundational principles[120] for responsible research conduct and oversight of research data systems in the realm of genomic and health-related data sharing. The foundational principles aid in the interpretation of the defined 'core elements of responsible data sharing'. Those core elements can be summarized[121]as follows:

- **Transparency**, which includes developing:
    - clearly defined and accessible information on the purposes, processes, procedures and governance frameworks for data sharing,
    - clear information on the purpose, collection, use and exchange of genomic and health-related data[122],
    - procedures for fairly determining requests for data access and/or exchange.
- **Accountability**, including:

---

[118] Available: https://github.com/EBISPOT/DUO.

[119] Knoppers BM. Framework for responsible sharing of genomic and health-related data. Hugo J. 2014 Dec;8(1):3. doi: 10.1186/s11568-014-0003-1. Epub 2014 Oct 17. PMID: 27090251; PMCID: PMC4685158.

[120] Foundational principles for responsible sharing of genomic and health-related data are: (i) Respect Individuals, Families and Communities, (ii) Advance Research and Scientific Knowledge, (iii) Promote Health, Wellbeing and the Fair Distribution of Benefits, (iv) Foster Trust, Integrity and Reciprocity.

[121] Full explanations of the core principles are provided in the cited article.

[122] Including, but not limited to: data transfer to third parties; international transfer of data; terms of access; duration of data storage; identifiability of individuals and data and limits to anonymity or confidentiality of data; communication of results to individuals and/or groups; oversight of downstream uses of data; commercial involvement; proprietary claims; and processes of withdrawal from data sharing.

    - Implementing systems for data sharing, tracking the chain of data access and/or exchange to its source and complaints regarding data misuse;
- **Engagement**, in particular:
    - allowing deliberation regarding implications of data sharing, with various stakeholders including patients;
- **Data quality and security**, in particular:
    - data security measures that mitigate the risk of unauthorized access, data loss and misuse,
    - enhancing data interoperability and replicability and also preserving long-term searchability and integrity of data; feedback mechanisms on the utility, quality, security, and accuracy of data, and their annotation;
- **Privacy, data protection and confidentiality**
    - compliance with applicable privacy and data protection regulations at every stage of data sharing,
    - data protection safeguards proportionate to the nature and use of the data, whether identifiable, coded or anonymized; no re-identification of patients unless explicitly required by the law;
- **Risk-benefit analysis**
    - Including conducting a proportionate assessment of the benefits and risks of harm in data sharing, which is periodically monitored according to the reasonable foreseeability of such harms and benefits;
- **Recognition and attribution**
    - Design of systems of data sharing with a view towards recognition and attribution that are meaningful and appropriate to the medium or discipline concerned and which provide due credit and acknowledgement of all who contributed to the results;
- **Sustainability**
    - Ensuring sustainability of the data generated for future use;
- **Education and training**
    - Dedicating education and training resources so as to advance data sharing and data management and to constantly improve data quality and integrity;
- **Accessibility and dissemination**
    - Dedicating reasonable efforts to maximize the accessibility of data for research through lawful and proportionate data sharing, this includes participation in collaborative partnership.

INCISIVE included the above core elements in its data sharing model, as further described in Chapter 6.

5.3 Existing platforms for sharing biomedical data

The following examples of terms of sharing of data biomedical in the existing platforms were investigated during the work on INICISVE data sharing model:

Name and website	Type of access	Additional details
LUNG CANCER EXPLORER (US)	Open access - does not require registration to view the content	terms and conditions / privacy information not available
LUNG CANCER EXPLORER (US) https://lce.biohpc.swmed.edu/lungcancer/	Open access - does not require registration to view the content	terms and conditions / privacy information not available
Medical Segmentation Decathlon http://medicaldecathlon.com/	Open access - data available for download, no registration is necessary.	All data is made available online with a permissive copyright-license (CC-BY-SA 4.0), allowing for data to be shared, distributed and improved upon.
Virtual Pathology at the University of Leeds https://www.virtualpathology.leeds.ac.uk/Public/example/common.php	Open access - slides can be viewed without registration	-
BREAST CANCER DIGITAL REPOSITORY (BCDR) - Spain https://bcdr.eu/	Must be a registered user to see the content.	terms and conditions / privacy information not available
BIMCV-COVID19 /EU funding https://bimcv.cipf.es/bimcv-projects/bimcv-covid19/	Researchers seeking to use the full Clinical Database must formally request access.	The BIMCV-COVID19, although de-identified, still contains information regarding the clinical care of patients, and must be treated with appropriate respect. Terms of use https://bimcv.cipf.es/bimcv-projects/bimcv-covid19/bimcv-covid19-dataset-research-use-agreement-2/
Lung Cancer Registry https://lungcancerregistry.org/what-	Restricted access for approved researchers.	Third parties may seek access to deidentified data in the Lung Cancer Registry. Third parties may include, but are not limited to, academic or non-profit researchers or companies conducting

to-expect/privacy-security/		retrospective studies, which are studies that analyse data after it has been collected, or conducting research and/or clinical trials on new therapies. Third parties will only be granted access to deidentified data in the Registry upon review of a detailed proposal and approval by the Lung Cancer Registry. Submissions require a research proposal, application and budget. Approvals are based on the scientific quality and validity of the study as discussed in the application. Data requests for studies related to lung cancer are NOT guaranteed approval, and all approvals are documented. Third parties seeking access to registry data must demonstrate evidence of IRB approval or exemption. Also patients can upload their data https://www.connection.solutions.iqvia.com/Desktop/Portal/Signup?&ts=637695410213743162&lang=en&id=LungCancerRegistry Terms and conditions: https://lungcancerregistry.org/terms-conditions/ FAQ for researchers: https://lungcancerregistry.org/what-to-expect/researchers/
OPTIMAM MAMMOGRAPHY IMAGING https://medphys.royalsurrey.nhs.uk/omidb/	Applications for access made via a web form and considered by an internal sub-committee made up of members of the OPTIMAM steering committee. The web form will alert the team of the applicant's interest, and they will send out a more detailed application form to be completed in full.	Access process described here and the access criteria are defined: https://medphys.royalsurrey.nhs.uk/omidb/what-is-the-process/ OPTIMAM has ethical approval which enables the sharing of the de-identified data with other researchers, academics and organisations.
Eurobioimaging https://www.eurobioimaging.eu/	Restricted access for approved researchers: Use of general Euro-BioImaging data services does not require applying, but a researcher wishes to get data, analysis tool or workflow included in these services, they need to contact Euro-BioImaging first and submit an access proposal. Euro-BioImaging uses Life Science Login to identify the researchers. As part of the evaluation procedure, Euro-BioImaging technology access proposals are reviewed by the Node(s) access is being applied to. While access to data services is normally free of charge, access to technologies generally involves a fee. However EMBL also launched a new central, open data resource for biological images, called BioImage Archive: https://www.ebi.ac.uk/biostudies/BioImages/studies. It is also possible to submit data to the BioImage Archive: https://www.ebi.ac.uk/bioimage-archive/help-faq/.	Euro-BioImaging is managed by its Hub and governed by the Euro-BioImaging Board. Euro-BioImaging ERIC's governance also includes a Scientific Advisory Board (SAB), whose role is to oversee the scientific, ethical, technical and management quality of the Euro-BioImaging ERIC activities. In addition, the Panel of Nodes, made up of Node representatives, advises the Euro-BioImaging Directorate in relation to Euro-BioImaging activities. Finally, the Euro-BioImaging Industry Board Advisory Panel provides advice to the Euro-BioImaging Directorate on any industry relevant needs or initiatives that Euro-BioImaging should address. Details: https://www.eurobioimaging.eu/about-us/how-to-access Terms and conditions: https://www.eurobioimaging.eu/content/terms-

	Datasets are also available via Image Data Resource (IDR), a public repository of reference image datasets from published scientific studies, available here: https://idr.openmicroscopy.org/about/. They are made available on a Creative Commons Attribution 4.0 International License.	and-conditions FAQ: https://www.eurobioimaging.eu/about-us/faq Privacy policy: https://www.eurobioimaging.eu/content/privacy-policy
BBMRI https://www.bbmri-eric.eu/	Data and samples are available based on restricted access for approved researchers.	BBMRI-ERIC is a European research infrastructure for biobanking. It offers a catalogue of samples and data - anyone can use it to identify candidate biobanks to get access to samples and data sets. While general access policy is available online, due to the diversity of the BBMRI-ERIC Partner Biobanks, access units and modes are to be defined by each biobank Material Transfer Agreements (MTAs), Data Transfer Agreements (DTAs) or Data Access Agreements (DAAs) should always be used to govern material transfer between parties. Access policy: https://www.bbmri-eric.eu/wp-content/uploads/AoM_10_8_Access-Policy_FINAL_EU.pdf BBMRI-ERIC verifies the identity of each requester and his/her institutional affiliation (employee status). A requester files a request for access to samples/data via the BBMRI-ERIC IT services. Each request must include information about the approved/proposed research project including its ethical approval status, expected properties of and amount of samples/data and their anticipated use, as well as the destination of the samples (if different from the location of the requester). A provider may either request refinement of the request or provide Availability Information to the requester via BBMRI-ERIC. After receiving adequate Availability Information, the requester follows up directly with the provider (biobank) in order to provide any additional information needed to assess whether access can be granted. The provider has to decide whether samples/data are released for the project requested. Similarly, access to deliverable/extraditable samples may be subject to prioritisation. For approved requests, the MTA/DTA will need to be executed and access charges paid before samples/data are released to the requester.
Elixir Luxembourg Translational Data Catalog Data	The data portal allows different types of access models: open access (for anonymous data) or controlled access. In the latter mode, Data Access	Terms for the data provider: https://elixir-luxembourg.org/services/get-started/data-provider/

Catalog https://datacatalog.elixir-luxembourg.org/	Committee reviews and approves user request.	Terms for the data user: https://elixir-luxembourg.org/services/get-started/data-user/
European Genome-phenome Archive (EGA) https://ega-archive.org/	EGA follows controlled access policy. The user has to apply for access to Data Access Committee appointed by the data provider.	Data processing agreement https://ega-archive.org/files/EGA_Data_Processing_Agreement_v1.1.pdf https://ega-archive.org/privacy-notice

5.4 Types of data sharing/access models in the biomedical platforms

Based on the review of the existing health data platforms, it was concluded that there is no single model that is followed. On the contrary, several types of access model[123] can be distinguished: open, registered (safeguarded) and controlled access. While the details of each application may vary (see examples above), generally they can be described as following:

5.4.1 Open data model

In the open data model, no registration in the database is required. This approach is used usually for fully anonymized data. In such case, the users can browse the data catalogue for open data collections and then download or access them directly. Use of the data may be subject to certain license terms (for example, Creative Commons license).

5.4.2 Registered access model

In the registered access model, user must register in the platform before using the data. This approach may be used for de-identified data, when the contributor considers that there is risk in linking the provided data with other datasets. For this reason, to use the platform the user needs to be registered and authenticated (user identity is verified).

5.4.3 Controlled access

In the controlled access model users have to register in the platform and then apply to the data owner (data provider) or a Data Access Committee to access (use) the controlled data. This model is usually accompanied by application criteria. For example, the users that apply for data access must provide name of the project lead, team members, project title and abstract descripting intended use of the data and demonstrate expertise in similar research. They also need to agree to specific terms of use (license terms). This model allows the most stringent control over who uses the data and for which purpose. The access request needs to be often filed to the individual data provider of the set or a Data Access Committee established by this

[123] For example, https://datahub.aida.scilifelab.se/search/.

provider. Even if the access to the data is controlled, in some repositories the search for the appropriate dataset is possible without prior registration or permission.

There may be platforms offering all three 'tiers' (such as UK data service), the type of access is agreed with the data owner (provider). This approach is followed, for example, by UK data service[124]. In other repositories, only two tiers (open and controlled access) are available[125]. Finally, there are repositories which only offer one tier. It is easier to enforce the license terms in registered access and controlled access, as then the identity of the user is known, and they can be prompted to accept the terms of use and license terms when logging into the platform and accessing particular dataset.

Irrespective of the model, there may be specific measures to secure the data in the repository. They may include that the data is not downloadable and can be viewed only via a dedicated software tool.[126]

Usually the datasets are licensed under a defined licensing agreement. However, it is possible that there may also be additional conditions for use of specific datasets. Such conditions may be, for example, special agreements, depositor permission, limited to non-commercial or academic users, data destruction clauses, specific forms of citation.

[124] https://ukdataservice.ac.uk/

[125] https://ocg.cancer.gov/resources/open-versus-controlled-access-data

[126] For example, UK Data Service uses the Safe Room. In this case, each session is recorded. Details here: https://ukdataservice.ac.uk/app/uploads/sa_user_guide.pdf

6 Data sharing model in INCISIVE

The following Chapter provides an overview of the work on developing the data sharing model in INCISIVE, taking into account the requirements, standards and precedents, defined in the previous chapters.

6.1 Sharing of data between INCISIVE beneficiaries

In order to allow the sharing of the de-identified (pseudonymized) medical data between the INCISIVE beneficiaries for the purpose of implementation of the Action in line with the legal requirements provided above, in particular stemming from GDPR requirements (see Chapter 3.1), INCISIVE Beneficiaries entered into the following intra-partner agreements:

- joint controller agreement (JCA) between the beneficiaries which collect and upload the Data to the INCISIVE Platform (INCISIVE Data Providers) and the technical partners responsible, jointly with the Data Providers, for defining the functionality of the Platform, for conducting AI training and studies described in the DoA. The JCA initially entered into effect as of 1 July 2021 and was later amended by Amendment 1 and 2. Main purpose of Amendment 1 was including a new partner, ADAPTIT, who entered into the Project consortium. Amendment 2 addressed changes in the Project related to storage and use of Data in the Hybrid Repository, terms of use of Data for Inference Services, as well as new legal requirements (new EU standard contractual clauses[127]);
- data processing agreements with MDT and FTSS[128], who were considered processors, acting only on instructions of INCISIVE joint controllers.

These agreements are described in deliverables D7.1 and D7.2. Building on the legal framework defined between the INCISIVE Data Providers, the data sharing terms defined in this document focus on the roles and responsibilities the external Data Providers and future external Data Users of the Data. However, during the term of the project, the INCISIVE Technical Partners would remain the users of the Data, once the data is shared with them through the INCISIVE Platform.

6.2 Towards the development of the INCISIVE data donation legal framework

The work on the INCISIVE data sharing legal framework required close alignment with T5.3, which dealt with the data sharing schema i.e. technical and procedural issues regarding the submission and use of the data in the repository (described in D5.2), as well as extensive

[127] Further to Commission Implementing Decision on standard contractual clauses between controllers and processors under Article 28 (7) of Regulation (EU) 2016/679 and Article 29 (7) of Regulation (EU) 2018/1725 of 4 June 2020.

[128] For FTSS this role was only limited to temporary infrastructure in the earlier stage of the project.

consultation and discussions between the INCISIVE partners to understand the needs and requirements of the stakeholders of the INCISIVE data sharing (later defined as 'Data Providers' and 'Data Users', see Chapter 6.3 below).

After desk research and review of the existing materials was performed, WP7 organized workshops on 12 & 24 January, 1 February 2022 for all INCISIVE partners. The aim of those workshops was to outline the roles and obligations of the INCISIVE stakeholders in the legal framework model and discuss the requirements for compliant and secure data sharing.

Following the outcome from the workshops, further work concentrated on the review of approaches followed by other biomedical databases (See Chapter 5.3) and explanation of IP licensing (Chapter 3.4.1). Notes on these topics were presented to the partners.

Next, in line with the principles of Transparency and Engagement (stemming from 'Framework for responsible sharing of genomic and health-related data' mentioned in Chapter 5.2), to determine the requirements and expectations of the stakeholders in terms of data access model, WP7 circulated questionnaires to the INCISIVE Data Providers to obtain their input to questions regarding: (i) approval process of the users of the data, (ii) deployment of Data Access Committee, (iii) conditions to be imposed on the users, (iv) functionalities of the Platform (searchability, availability for AI training and viewing of the data), (v) permissibility of downloading the Data and (vi) opt-out conditions. Inputs on those topics were collected between July - September 2022 from the following INICSIVE Data Providers: GOC, HCS, UNITOV, UNS, UOA, DISBA.

In parallel, within T5.3 work ADAPTIT collected input from AI developers (potential Data Users) on their requirements and usefulness of the Data in the repository for the AI research. The questions regarded: (i) search criteria, (ii) access levels (display of search results, use for AI training, data available for viewing), (iii) perspectives on data users' approval process, (iv) selection of data for training, (v) rewards and acknowledgement of the Data Providers, (vi) desired functionalities of the Platform. Potential Data Users from FTSS, ICCS, UNS, CERTH, UNS, VIS, AUTH, MAG participated in the workshop and provided input to the questionnaires.

Outputs of those questionnaires were digested and discussed during joint meetings of T5.3 and T7.4. The most important point of the discussions at this stage was ensuring the privacy of the Data, while maintaining the Data useful for the AI developers. In INCISIVE, the discussions in particular concerned Data accessibility for the AI developers. In the questionnaires mentioned above, the AI developers indicated that the functionality enabling them to view the Data is highly desired. Respondents indicated that developing a model without the possibility to view the data would be a very tedious and frustrating process, unless very extensive descriptions and examples for the data are provided. Not being able to view the data would discourage future AI developers from using the INCISIVE platform.[129] Majority of the Data Providers who

[129] For instance, the AI developers' responses indicated that viewing the Data is "as useful as the searchable access level", is a "better option, together with some statistics on images would be acceptable" and they strongly suggested to be able to view and process the data for harmonisation and quality checking purposes". Moreover,

participated in the questionnaires mentioned above did not object to ensuring viewability of the Data, as long as the Data is not downloaded from the Platform. At the same time, concerns about GDPR compliance were raised and some mitigating solutions were proposed.[130]

Another topic discussed concerned the extent of control over the Data to be exercised by the Data Providers. It was observed that with more fragmented and bureaucratic process of Data application, the less appealing the Repository is for the AI developers.[131] Moreover, if each of the Data Providers was able to define separate conditions and access terms (as permitted in many controlled-access repositories), the AI developers' access to Data (especially for Federated Learning) may be hindered by the conflicting requirements for various datasets to be used for training. As result, the AI developer may not be able to benefit from the diversity of datasets available in INCISIVE. At the same time, majority of the Data Providers who participated in the questionnaires mentioned above, indicated willingness to delegate the decision on admission of new users to a Data Access Committee further to terms defined by the INCISIVE project.

During the plenary meeting in Athens on 19 October 2022 the principles of INCISIVE data sharing framework draft were presented to all INICSIVE partners and open questions were discussed by all the members of the consortium. These discussions led to outlining the 'pros' and 'cons' of the three basic types of the data access models:

	Repository is fully open = Open access	Registered access = researcher applies for access to the repository content; use of data is recorded	Controlled access = researcher must apply to use specific data set
PRO	Simpler to use by the AI developers No governance required	Acceptance of the terms of use is tracked Possibility to record transactions made by the user Approach followed by many health repositories	More control over data for the data provider Easier to obtain ethical approval to contribute data Potentially easier to align with the future DGA requirements and (potential) requirements of EHDS secure processing environments Approach followed by many health repositories

some respondents stated that "it is mandatory to view the data in order to have the best results. Of course, you can train an AI algorithm without viewing the data, however, at some point it may be necessary to see some specific samples in order to understand how is the model working or in order to debug the code" and the "having a black box system without inspecting your inputs doesn't really seem like a productive way for model creation."

[130] Some AI developers indicated that "If the data are not available for viewing, then the data would need to be in the form of already pre-processed, clean datasets instead of a big collection of data." Another possible solution would be "sample overview of the database / thumbnail images that are similar with the data and are GDPR compliant".

[131] This tension was also described in the eTRIKS (Dyke S.O.M., Kirby E., Shabani M., Thorogood A., Kato K. and Knoppers B.M. Registered access: a 'Triple-A' approach. Eur J Hum Genet. 2016 Sep 28. doi: 10.1038/ejhg.2016.115) project, which developed a registered access model based on "triple-A" process: Authentication, Attestation and Authorization.

C O N	No means of control over data use Higher security risk May raise objections of ethics committees INCISIVE DoA described identity management and TEE	Longer time for users to obtain access Requires to determine process for admission of the users based on set criteria Requires to put in place a governance structure	Additional layer of technical complexity Even longer time to obtain access

As a result of the analysis of the presented access models for biomedical data repositories by the INCISIVE consortium, in view of the INCISIVE Project goals and limitations, the 'registered access' model was selected as most suitable for the sharing of Data on the INCISIVE Platform, when applied in combination with privacy-and security features in the Platform, including that:

- to access the Data the potential user needs to not only register to the Platform, but apply for obtaining access,
- the Data will be de-identified (pseudonymized or anonymized) either via tools made available to the Data Providers or with the use of external tools;
- by design, the Data can only be used in the secure environment of the Platform, without downloading or copying the data to external locations;
- the primary objective of the Platform is to make the Data available for AI training, including Federated Learning (FL). FL is indicated as a privacy enhancing technology (PET) which allows AI training without moving the Data[132], however, it is understood that, in some cases, it may downgrade quality and performance of trained AI models due to the fact that the data cannot be viewed or otherwise processed by the AI developer;
- INCISIVE Platform registers Data use transactions with blockchain technology, providing an extra layer of accountability for the Data use.

Given those additional features, the data sharing model was named as '**Registered Access Plus**'.

The selected approach was validated during the meeting with potential Data Providers in Belgrade (17 November 2022).

6.3 INCISIVE Platform stakeholders and their roles

The data sharing model in INCISIVE is based on following roles and responsibilities of the stakeholders:

---

[132] Rachakonda AS, Moorthy BS, Jain CA, Bukharev DA, Bucur EA, Manni FF, Quiterio GTM, Joosten HL, Mendez INI. Privacy enhancing and scalable federated learning to accelerate AI implementation in cross-silo and IoMT environments. IEEE J Biomed Health Inform. 2022 Jun 22;PP. doi: 10.1109/JBHI.2022.3185418. Epub ahead of print. PMID: 35731757; Liu JC, Goetz J, Sen S, Tewari A, Learning From Others Without Sacrificing Privacy: Simulation Comparing Centralized and Federated Machine Learning on Mobile Health Data, JMIR Mhealth Uhealth; Piamrat K, Marchetto G. Handling Privacy-Sensitive Medical Data With Federated Learning: Challenges and Future Directions. IEEE J Biomed Health Inform. 2022 Jun 23;PP. doi: 10.1109/JBHI.2022.3185673. Epub ahead of print. PMID: 35737624.

Data Providers (earlier referred to as 'data donors') - The institutions with the right to grant access to certain images and health-related data (Data). They are the controllers of the original medical records containing images and related health data. They are solely responsible for meeting the obligations ascribed to the Data Provider i.e. for the lawful collection of Data, its pre-preparation (de-identification, annotation and quality check), contribution to the INCISIVE Platform and correctly describing the Data (providing metadata). If the Data Provider will receive the data from another entity (e.g. hospital, clinic, another organization), their compliance with those obligation must be coordinated with this provider. Each Data Provider maintains (stores) the shared data at a chosen location, which includes either a local Federated Node set up at own premises or at premises selected by the Data Provider (e.g. cloud storage), or the Central node. Data Provider needs to accept the Data Sharing Agreement (defined below)

Data Users - The individuals and/or institutions which have been granted access to data for a specific research project. Data Users will be using the data for AI training in infrastructure provided by INCISIVE Platform. The potential Data Users need to first assess the suitability of resources in the INCISIVE Platform for the purpose of their research via a publicly available interface (web-page) of the Platform. Then, they apply to become Data Users and their research proposal will be evaluated in data access procedure. When they are accepted to use the INCISIVE Platform, they are referred to as Data Users. They need to accept the ToU of the Platform and Data User Terms (defined below) as well as to follow them during their research project. Data Users need to also acknowledge having read the privacy policy of the Platform.

INCISIVE Platform – hybrid platform allowing sharing of medical images and data to and use of data from the Pan-European repository. On one hand, the INCISIVE Platform provides a standardized manner of joining the repository as a Data Provider and tools for the pre-processing of Data by the Data Providers. On the other hand, it provides infrastructure for the Data Users to make the Data discoverable and accessible for the Data Users to allow them to train their AI models on the data from the repository. Currently, the INCISIVE Platform is a result of the Project and there is no separate legal entity which is responsible for the management and operation of the INCISIVE Platform. Thus, the obligations regarding the INCISIVE Platform are assigned to relevant the INCISIVE Partners.

The INCISIVE Platform also provides Inference Services. These are processes of using the AI Models over input data to obtain the targeted results, e.g., predictions or tumour segmentations. While Inference Services are available through a dedicated part of the Platform, the data provided by the Data Provider within data sharing legal framework will not be used for those services and thus they will be regulated by separate legal terms.

Data Access Committee ('**DAC**') – the role of DAC is to assist in the Data User and Data Provider approval process during (mostly) post project INCISIVE Platform deployment. DAC will be set up as a multi-stakeholder body which receives access requests from the potential users and assesses whether they are relevant and meet the established access and use conditions and can be accepted as Data Users.

6.4 Principles of INCISIVE data framework

The 'Registered Access Plus' data sharing framework is based on core principles described in 'Framework for responsible sharing of genomic and health-related data' (Chapter 5.5.2).

- As mentioned in Chapter 6.2 above, the preparatory work on the framework was aligned with the principles of Transparency and Engagement;
- Next, the legal framework described below, as well as the INCISIVE Platform features, incorporate the principles of Accountability, Data quality and security, Privacy, data protection and confidentiality, Risk-benefit analysis, Recognition and attribution.
- Further principles (Sustainability, Education and training, Accessibility and dissemination) are incorporated through actions included in WP6, WP8 and WP9.

In addition to following the above core principles, INCISIVE framework pays particular attention to addressing the requirements of both Data Providers and Data Users in the context of AI training. It strives to find a balance between the privacy of the Data and control exercised by the Data Provider and usability of the Data for the Data Users.

The legal framework design provides means for the Data Providers to ensure control over the use of their Data through:

- Transparent terms of Data contribution (Data Sharing Agreement);
- Allowing only registered Data Users to use the Data in the INCISIVE repository, with planned verification and admission of Data Users with the participation of Data Access Committee;
- Recording of information about Data use through blockchain and allowing the Data Provider to access those records;
- Possibility for the Data Provider to opt out from the Repository and remove its Data from the Platform.

It is the responsibility of the Data Providers to define the Data which they wish to share and obtain any permissions which are required to provide it to the Repository (including patient consents or ethics approvals). At all times, the Data needs to be de-identified and shared in a pre-defined format as agreed within the project. INCISIVE anticipates that some of the Data shared will be considered as 'anonymous' by the Data Provider and – in that case - the GDPR would not apply directly to anonymous data. However, considering the technological progress which may potentially lead to novel privacy risks (for example, linking of the de-identified medical data with the patient based on information available in the public domain) and the challenges in relation to data anonymization (see Chapter 7), INCISIVE Platform applies strict security measures to anonymous data and uses the model of 'Restricted Access Plus' to enable only verified researchers to access all the Data available within the INCISIVE Platform environment.

From Data Users' (AI developers) perspective, the requirements of transparency and facilitation of access were taken into account. Thus, in the proposed framework:

- Data in the INCISIVE repository is stored in a controlled environment, however the description of Data is available openly - open data sharing portal will present the information (description) about all the Data available in the closed part of the Platform;
- Users apply for access to the Platform only once and – when approved – may use the entire dataset for AI training. However, each time they must authenticate themselves and log in (trusted access) before entering the Platform;
- The Data is provided under uniform terms for use (Data User Terms), eliminating the patched and possibly conflicting requirements imposed by individual Data Providers;
- Users must accept terms of use under which the AI developer is prohibited from:
    - Attempting to re-identify the data subjects,
    - Downloading and coping Data outside the Repository environment,
    - Circumventing security measures,
    - Modifying original Data,
    - Use of AI models, which may compromise or copy the Data.

The Data provided by the Data Providers is shared according to the following conditions which are defined in Data Sharing Agreement:

- The rights or ownership of the Data are not transferred to Data Users or the INCISIVE Platform (only limited license is provided to the Data User),
- The Data Provider may withdraw their Data from the INCISIVE Repository in accordance with the Data Sharing Agreement conditions,
- Data User does not have the right to sublicense the Data nor exclusivity rights to use it,
- Data User is required to acknowledge the Data Provider as the source of Data (citation requirement),
- Data Provider does not have IP claims to results (AI Models) trained on the Data.

From the procedural side, in order to start sharing the Data:

- Data Providers contact the INCISIVE platform to contribute the Data,
- After the discussions to ensure eligibility of the Data Provider are complete, prior to sharing Data, Data Providers have to sign the Data Sharing Agreement and provide description of the Data (including the metadata of the contributed Data).

From the perspective of the Data Users:

- Information about Data and the Platform's terms of use available openly (according to the FAIR rules),
- Potential users have to apply to be admitted to INCISIVE secure platform environment and present research proposal and accept the terms of Platform, including Data User Terms,
- User acceptance process takes place with an advisory role of a Data Access Committee,
- If AI developer is accepted, he/she can use the Data in the repository available for AI training.

The principles agreed above were translated into legal terms for the users of the Platform and data sharing agreement (Chapter 8). For easier understanding, a summary of the conditions (Chapter 8.1) is made available in addition to the detailed legal documents.

7 Lessons learned and future work

7.1 Challenges, lessons learned and open issues

The Chapter below presents challenges faced by INCISIVE in the work on the definition of the data sharing legal framework, as well as lessons learned from this process and outlines the future steps.

Incorporation of the identified standards, as well as legal and ethical requirements is not a straightforward task, given the limitations of the project scope, complexity of the technologies involved and evolving regulatory landscape. In particular, the following challenges had to be tackled during the preparation of the data sharing framework:

- **Lack of clarity on standards regarding anonymization of medical data, in particular image data.** Recital 26 GDPR states that 'anonymous information' is information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. In contrast, any information relating to an identified or identifiable natural person (data subject) is considered 'personal data', even if the information is pseudonymized (de-identified in a manner which is reversible). However, in practice, the understanding of the terms 'anonymized' and 'pseudonymized' both among privacy practitioners and in the medical community is not uniform. Moreover, the translation of the legal requirements for data anonymization into concrete technical standards is not an easy task. In particular, questions arise regarding potential linkability of the de-identified images with the raw data by the original controllers, who have access to full medical records. This leads to lack of clarity on how to classify de-identified medical images and data, even if multiple direct identifiers (patient names, identification numbers) and indirect information (time of visit, age of the patient) have been carefully removed, as recommended by international standards and protocols.[133] At the same time, implications of the assessment of a data set as 'personal data' (or non-personal data) under GDPR framework are crucial, as they determine the applicability of GDPR or the lack of it. Still, the paradox is that if the data is considered anonymized during its initial submission and it is determined that GDPR does not apply to it, the data theoretically can be shared with a wider public. If this sharing is done without any controls and restrictions, this may lead to the risk of re-identification. With this in mind, INCISIVE legal framework was designed to protect all the contributed data (even if considered as 'anonymous' during the data submission), taking into account the sensitivity of the shared medical information and potential of linking the data to the patient (for example, with use of future technologies). In the experience of INCISIVE, the 'Registered Access Plus' model was considered as more appropriate than a totally 'open' one to ensure that the Data is used for ethically and legally permissible purposes only. This solution was accepted by the INCISIVE Data Providers and Data Users.

[133] https://dicom.nema.org/medical/dicom/current/output/html/part15.html#table_E.1-1

- **Qualification and assignment of GDPR roles in complex research infrastructures and in data sharing platforms.** The perception of GDPR roles (controller, processor or joint controller) of the partners and participants in data sharing, also in the context of research projects, is not straight forward[134]. INCISIVE also faced discussions regarding GDPR status of the individual stakeholders in the data sharing. In particular, for the sharing of Data between a defined group of beneficiaries (i.e. INCISIVE Data Providers and Data Users) bound by a clear purpose of implementation of the DoA and using defined means of processing, the joint controllership arrangement seemed most appropriate. In the experience of INCISIVE, this agreement model proved effective to provide legal safeguards and yet flexible enough to allow necessary sharing of Data between the partners. However, as the pool of the Data Providers is planned to expand to Data Providers from external organizations, the roles need to be changed. For the legal framework proposal we assumed that the external Data Provider will remain the controller of the data stored in Federated and Central Node, while the Data User applying for access to the Platform will become an independent controller (for the processing of data in connection with their research use). In INCISIVE, the Data Providers accepted this solution, however appreciated a proposal to create a Data Access Committee to assist in the approval of the new users. These roles may need to be adjusted again, if the management of data on the INCISIVE Platform and operation of DAC is carried out by a separate entity or together with another project.
- **Striking the right balance between the privacy of the Data and its usability.** It is a known dilemma that too stringent security measures likely lead to data non-use. In the ethics literature[135] this is referred to as 'privacy perfectionism' where superfluous controls are applied to datasets diminishing data utility but without providing additional safeguards. Furthermore, recent studies based on the analysis of publicly available information about data leaks connected to scientific use of data argue that 'cost—measured in terms of access to future medical innovations and clinical software while potentiating bias—of slowing machine learning progress is too great to stop sharing data through large publicly available databases for concerns over imperfect anonymization and potential linkage risks.' [136] Yet, from the GDPR compliance perspective, privacy-by-design principle requires to minimize the

---

[134] For example, see: Regina Becker, Adrian Thorogood, Jasper Bovenberg, Colin Mitchell, Alison Hall, Applying GDPR roles and responsibilities to scientific data sharing, International Data Privacy Law, Volume 12, Issue 3, August 2022, Pages 207–219, https://doi.org/10.1093/idpl/ipac011; Van Veen EB, Boeckhout M, Schlünder I et al. Joint controllers in large research consortia: a funnel model to distinguish controllers in the sense of the GDPR from other partners in the consortium [version 1; peer review: 1 approved]. Open Res Europe 2022, 2:80 (https://doi.org/10.12688/openreseurope.14825.1)

[135] Allen, J., C.D.J. Holman, E.M. Meslin, and F. Stanley. 2013. Privacy protectionism and health information: Any redress for harms to health? Journal of Law and Medicine 21 (2): 473–485. https://www.researchgate.net/profile/Judy_Allen3/publication/260561318_Privacy_protectionism_and_health_information_Is_there_any_redress_for_harms_to_health/links/55489a9e0cf2e2031b388b1a.pdf

[136] Seastedt, Kenneth & Schwab, Patrick & O'Brien, Zachary & Wakida, Edith & Herrera, Karen & Marcelo, Portia & Agha-Mir-Salim, Louis & Frigola, Xavier & Ndulue, Emily & Marcelo, Alvin & Celi, Leo. (2022). Global healthcare fairness: We should be sharing more, not less, data. PLOS Digital Health. 1. e0000102. 10.1371/journal.pdig.0000102.

amount of data processed. To tackle these conflicting positions, INCISIVE conducted multiple consultations and discussions between the beneficiaries regarding scope of the data required for AI Models training and the manner of privacy compliant data sharing[137]. One of the most heavily discussed aspects was the requirement for the data to be visible (viewable) to the AI developers. In INCISIVE, the interviewed Data Providers were not in general concerned about visibility of the de-identified images and Data to the approved Users, assuming they use the Data for legitimate purposes within the boundaries of the Platform. The solution which was selected was a restricted sandbox hosted in each Federated Node, through an installation of an optional viewer component. Additional safeguards may be added in the future, if required. A lesson which may be learned from INCISIVE experience is to start these discussions early in the project and to dive deep into specific technical requirements of the users during the product design studies.

- **Limitations stemming from the ethics approvals and consents of the patients.** One of the most important requirements for the Data Providers to be able to participate in the data sharing is ensuring that the Data can be contributed in compliance with statutory requirements. This typically entails securing the approval of the hospital's bioethics committee and consents from the patients (unless other GDPR legal basis applies). In INCISIVE, the Data Providers obtained ethics approvals, which allowed then to submit Data to the Project for the implementation of Action (see Deliverable D7.2). The obtained ethics approvals will be re-evaluated to determine if they need to be updated to cover post-project use of Data in the repository by external Data Users under the conditions determined by the developed data sharing framework. From the patient consent side, the prospective studies which involved collection of patient Data included specific consent of the patients for the re-use of their data for AI training, after anonymization of this Data. In retrospect, we can conclude that it was helpful for the Data Providers to rely on coordinated efforts for drafting ethics applications and patient consent forms based on a common template.
- **Legal entity responsible for providing Platform services.** At this stage of the project, INCISIVE Platform is not a legal entity, but rather a research prototype which is operated jointly by beneficiaries. As result, the Platform as such cannot be party to the data sharing agreement with the Data Provider, as it cannot be tasked with legal obligations nor can it benefit from certain rights; those can only be attributed to individual partners of the consortium. This is reflected in the proposed legal terms. In the future work, INCISIVE partners will need to consider different options for sustainability planning; those could include transferring the repository to an organization which already administers such repositories or setting up of a dedicated legal entity. In particular, if the administrator of INCISIVE Platform would aim to provide commercial 'data intermediation services', as defined by the Data Governance Act (DGA), establishment of separate legal entity would be required. In terms of lessons learned, it should be noted that the DGA is a new legal act, which was passed after the INCISIVE launch and which impacts the sustainability planning of the project. Future actions should already at the outset of building a data repository

[137] Those discussions are summarized above in Chapter 6.2.

evaluate how their proposition and design will align with the new legal rules on data governance.

Other lessons learned which may be helpful for data providers, data users and other partners involved in data sharing repositories include:

- Design and development of the data sharing framework is a gradual and tiered process, which involves not only analysis of the legal framework, but also a thorough understanding of the purpose and functioning of the data repository, as well as expectations and limitations of data providers (including patient representatives) and data users.
- Legal work, data collection and AI training in the project cannot be considered in silos. Frequent discussions, in person meetings and workshops, as well as questionnaires collecting views and needs of the involved stakeholders have been proven to bring the discussion forward and help with the decision making process.
- Including legal team in various discussions about the technical design of the data sharing solutions and seeking legal input is a requirement for implementation of the privacy-by-design principle.
- The builders of the repository and also data providers need to understand and – if needed- openly discuss the possible limitations and consequences of selected method of de-identification of the data (pseudonymization vs anonymization). The use of the term 'anonymized data' if done incorrectly can have important legal and data usability implications.
- Data providers need to have a good understanding of the whole 'life cycle' of the collected medical data to be able to appropriately prepare consents and ethics applications. This means that planned use of the data within the project and beyond it, especially potential re-use of the data for other purposes, should be discussed early in the project and should be described in the platform documents.
- To design and test the repository intended for storage and use of personal data, the beneficiaries need to consider putting in place agreement(s) for the transfer and use of the data. Those agreements need to be tailored to the specific circumstances of the project. Also, as the circumstances (for example, place of storage of data) may evolve, thus the project needs to anticipate the need to update the agreements, if needed.

7.2 Next steps

The proposal for INCISIVE terms of data sharing and terms of use are included in Chapter 8. The next steps will be the upload of the terms to the Platform. The documents for the Data Users (General ToU and Data User Terms) will be uploaded on the Platform as part of design of the UI (user interface). Additionally, a privacy policy for the Platform (describing the processing of Data User data) has been prepared and will be uploaded as well. The template of the Data Sharing Agreement will be available for the potential external Data Providers. In case of conclusion of agreement for the sharing of Data, the beneficiaries will provide power of attorney to the Project Coordinator to sign the agreement on behalf of the Project partners. INCISIVE decided to harmonize the terms under which the Data Providers could share their data and simplify the

data request process. This solution was consulted with the INCISIVE Data Providers and was accepted by them. Depending on the sustainability planning, as well as based on the feedback to or adaptations of the Platform after the release of this proposal of the legal framework, further improvements will be performed, in particular to prepare the INCISIVE repository to be used by external Data Users.

INCISIVE legal framework includes a Data Access Committee (DAC). The role of the DAC will be to evaluate the potential new Data Users and engage in discussions with Data Providers about the contributed Data sets. The next step for the project is to establish the DAC for the duration of the project. For sustainability purposes, INCISIVE will also consider cooperation with another project (see more about EUCAIM below) or existing infrastructure to ensure that the DAC is operational beyond the lifetime of the action.

7.3 Sharing of data beyond the INCISIVE project (cooperation with EUCAIM project)

INCISIVE acknowledges the launch of EUCAIM Project EUropean Federation for CAncer IMages (EUCAIM) funded as a flagship project by the Digital Europe Programme. Among other objectives, EUCAIM aims at enabling the interoperability at technical and semantic level between several existing data infrastructures, including the AI4HI repositories. As such, it is expected to make a major contribution to the European Health Data Space (EHDS) as indicated in the EC's press release[138] on the launch of the EHDS. Given that EUCAIM can significantly help in the sustainability of the INCISIVE data repository, INCISIVE aims at facilitating the sharing of its Data through the EUCAIM pan-European digital federated infrastructure of FAIR pan-cancer images. It also aims at facilitating technical interoperability of the INCISIVE data repository with other cancer imaging repositories, such as the AI4HI repositories. The proposed legal framework terms already anticipate such cooperation. Further details and complementarities will be defined as both projects progress.

[138] https://ec.europa.eu/commission/presscorner/detail/en/ip_23_286

8 Terms of use, policies and guidelines

8.1 Summary of the General ToU of the Platform

[Explanation: The intent of this section is to provide a brief overview of the applicable terms, for easier understanding of the main rules of data sharing and use on the INCISIVE platform.]

This Summary is provided for convenience purposes only. Please read and review the full General ToU, Data User Terms and/or Data Sharing Agreement before sharing the Data or using the Platform.

1 The INCISIVE repository (which is available on the INCISIVE Platform) is currently populated with Data (including medical images and clinical metadata) shared by a number of beneficiaries of the INCISIVE Project (INCISIVE Data Providers). The repository may be enriched by Data shared by additional Data Providers further to the conditions stated below and in the applicable Data Sharing Agreement.

2 The INCISIVE Platform permits the Data Users to use the shared Data for conducting training of AI, including Federated Learning, for the purpose of AI research. Currently, the INCISIVE Data Users are INCISIVE beneficiaries which perform AI research according to the INCISIVE DoA.

3 In time, INCISIVE repository will become open to cooperation with external Data Users. If necessary, Terms of use of the Data and terms of Data Sharing Agreement may be updated before the Data is shared with such external Data Users. Before we do this, we will inform the Data Providers of the updated terms and obtain their consent for further sharing.

4 Only de-identified Data that is compatible with INCISIVE goals and format can be submitted for sharing on the Platform. The Data Provider has to ensure this Data is provided in a structured and usable format and in accordance with guidelines INCISIVE may issue from time to time. To share Data on the Platform, the Data Provider needs to conclude a Data Sharing Agreement with us and select where the Data will be hosted (Federated Node or Central Node)

5 Data shared by the Data Providers must be de-identified by the respective Data Provider and should be kept separate from the original medical records. Data Provider is responsible for making a back-up copy of the Data which they share in the Federated Node or Central Node.

6 In the course of the AI training no download or export of this Data outside the Platform will be permitted. If Data Provider agrees, the Data that they share may need to be visible to the Data Users admitted to the Platform. All relevant transactions regarding the Data will be tracked via blockchain and other tracking mechanisms. Data User should acknowledge the source of Data in their publications.

7 Once shared, Data on the Platform will be accessible to all Data Users approved on the Platform. If the Data Provider does not agree with such access rights or other conditions

provided by the Data Sharing Agreement, they may indicate this during the application process. In such a case, the Data may be listed in the Platform webpage as available based on different conditions.

8 INCISIVE Project is a research and innovation action and its final results will be prototypes and not fully deployable technologies. The content or outcomes generated by the project (including predictions of the AI Models available on the Platform) cannot be used to make diagnostic or therapeutic decisions or construed as medical or other professional advice.

9 To the extent permitted by law, the INCISIVE Beneficiaries will not be liable for any damage, direct or indirect that the user may suffer in relation to their use of the Platform, Data or any of the tools, unless the damage has been caused intentionally or by serious error. INCISIVE Beneficiaries will make all reasonable efforts to maintain continuity of the Platform infrastructure and will provide, on a best effort basis, warning of changes or discontinuities. However, as some Data may be stored in Federated Nodes, availability of this data if shared by external Data Providers is beyond the responsibility of INCISIVE.

10 INCISIVE Beneficiaries have a right to refuse any Data offered by an external Data Provider and/or – in specific circumstances specified in the Data Sharing Agreement - to discontinue with immediate effect the linking of Federated Node or storage of Data in the Central Node.

11 INCISIVE Beneficiaries provide tools supporting data preparation and quality checking, however, they do not determine, nor have knowledge or control on, the quality of Data provided by the external Data Providers. They take no responsibility and assume no liability towards Data Users for any Data or other materials posted, stored, or uploaded by such Data Provider to the Central Node or shared via the Federated Node.

12 INCISIVE may publish the title and a short summary of successful Data user stories and publications on the INCISIVE Platform of INCISIVE website.

13 INCISIVE Project reserves the right to update the General ToU and Data User Terms; therefore, any User should consult them regularly.

14 INCISIVE acknowledges the launch of EUCAIM Project EUropean Federation for CAncer IMages (EUCAIM) funded as a flagship project by the Digital Europe Programme. Among other objectives, EUCAIM aims at enabling the interoperability at technical and semantic level between several existing data infrastructures, including the AI4HI repositories. As such, it is expected to make a major contribution to the European Health Data Space (EHDS) as indicated in the EC's press release[139] on the launch of the EHDS. Given that EUCAIM can significantly help in the sustainability of the INCISIVE data repository, INCISIVE aims at facilitating the sharing of its Data through the EUCAIM pan-European digital federated infrastructure of FAIR pan-cancer images. It also aims at facilitating technical interoperability of the INCISIVE data repository with other cancer imaging repositories, such as the AI4HI repositories. The proposed legal terms already anticipate such cooperation.

[139] https://ec.europa.eu/commission/presscorner/detail/en/ip_23_286

8.2 General Terms of Service of the INCISIVE Platform ('General ToU')

[Explanation: These are intended to be posted on the Incisive Platform to be accepted by any user of the Platform, either data provider, data user or person using any tools or services on the INCISIVE platform.]

1 Definitions

1.1 '**AI Models**' – Artificial intelligence models (AI models) available for use on the Platform.

1.2 '**Central Node**' - Central data storage space that will host Data from the Data Providers, technically acting in the same way as the Federated nodes. The Central Node can be used as one node of the several INCISIVE Federated Nodes and/or as a centralised data repository where AI training can take place.

1.3 '**Central infrastructure**' - The cloud infrastructure of INCISIVE, provided using Azure technology, comprised by 4 Virtual Machines, located in Central France that contains the centralized services required to make the INCISIVE platform work.

1.4 '**Consortium Agreement**' - Consortium Agreement signed between INCISIVE Beneficiaries on 15 July 2020, and any future amendment of this agreement that will be signed.

1.5 '**Data Protection Laws**' - GDPR and any additional locally applicable data protection legislation.

1.6 '**Data Provider**' - An entity which contributes Data to the INCISIVE repository. Data Providers include INCISIVE Data Providers, on the basis of internal data sharing agreement between INCISIVE Beneficiaries, and third-parties, on the basis of respective Data Sharing Agreements.

1.7 '**Data Subject**' or '**Subject**' - The patient or another person from whom the Data was obtained.

1.8 '**Data User**' – The entity or a person who uses the Data available in the INCISIVE repository for Federated Learning and/or AI training. During the term of the Project, Data Users will be INCISIVE Data Users. In time, INCISIVE repository will become open to cooperation with external Data Users

1.9 '**Data**' - Medical data and images made available in the INCISIVE repository, once made available for sharing.

1.10 '**Federated Learning**' - Means that AI model is trained in a distributed way using the required Federated nodes, i.e., the nodes that have the Data that matched with the user query. Each Federated or Central node contains a particular set of Data that may be required for training, and it will not leave the node to ensure privacy. The model is trained in each Federated node, including Central node, and then it is sent to the Central infrastructure to be merged to gather 'central knowledge'. This training-merging process can be repeated more than once for the same model as the more times this is done, the more robust is the solution.

1.11 '**Federated Node**' - Dedicated infrastructure (cloud or local) in which the Data Provider stores the Data which they contribute to the INCISIVE repository.

1.12 '**GDPR**' - Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).

1.13 '**General ToU**' – These General Terms of Service.

1.14 '**Grant Agreement**' - grant agreement number 952179 – INCISIVE signed by the INCISIVE Beneficiaries being Consortium Members and the European Union as the funding authority, and any future amendment of this agreement that will be signed.

1.15 '**INCISIVE Beneficiaries**' – Consortium Members under Grant Agreement; full list of INCISIVE Beneficiaries provided on the INCISIVE website.

1.16 '**INCISIVE Data Provider**' - Data Provider who is an INCISIVE Beneficiary.

1.17 '**INCISIVE Data User**' – The following INCISIVE Beneficiaries acting as the Data Users in during the INCISIVE Project:

a) AI developers working in INCISIVE Project for the training and validation of AI solutions: INSTITUTE OF COMMUNICATION & COMPUTER SYSTEMS, CENTER FOR RESEARCH AND TECHNOLOGY HELLAS, ARISTOTLE UNIVERSITY OF THESSALONIKI, FUNDACIO TSCALUT, SQUAREDEV, UNIVERSITY OF HELSINKI, UNIVERSITY OF NOVI SAD, CENTRO REGIONALE ICT SCRL, VISARIS D.O.O.

b) Beneficiaries working on INCISIVE development and testing of the repository: MAGGIOLI S.P.A., CENTRO REGIONALE INFORMATION AND COMMUNICATION TECHNOLOGY SCRL, BARCELONA SUPERCOMPUTING CENTER - CENTRO NACIONAL DE SUPERCOMPUTACION, EUROPEAN DYNAMICS LUXEMBOURG SA, TELESTO IOT SOLUTIONS LTD.

1.18 '**INCISIVE Project**' or '**INCISIVE Action**' – project conducted in accordance with Grant Agreement no. 952179; details of the INCISIVE Project and INCISIVE Beneficiaries can be found at INCISIVE website.

1.19 '**INCISIVE Repository**' or '**Repository**' - Pan-European repository of medical images and data, where each Data Provider maintains (stores) their data locally at chosen location, which includes either a Federated Node set up at own premises or premises selected by the Data Provider, or Central node, or both. The term encompasses both federated and hybrid data sharing.

1.20 '**INCISIVE website**' – Webpage available at https://incisive-project.eu/.

1.21 '**Platform**' - Platform (technical infrastructure integrating several components) provided by the Project which includes the INCISIVE repository, AI development workspaces for AI training, AI Models and the Inference services.

1.22 '**User**' or '**user**' - Any person making use of the Platform or any services offered on the Platform, including the INCISIVE Data Providers and the INCISIVE Data Users as well as external users.

1.23 '**User Institution**' means organization or institution where individual Users are employed or otherwise members of.

2 General obligations

2.1 These General ToU apply to all Users of the Platform, including Data Users and Data Providers.

2.2 Users are required to provide accurate, complete and truthful information about themselves, their organization, their Data and AI Models and other details relevant to the use of Platform tools and services.

3 Technical requirements to use the Platform

3.1 Minimal technical requirements to the use of the Platform:

a) To make use of the INCISIVE platform on any system, an active internet connection is required.

b) To use the INCISIVE platform through a browser on Windows, User will need: Windows 7 (or later) or Mac.

c) To use the INCISIVE platform through a browser on Mac, User will need: MacOS High Sierra 10.12 (or later) or Linux.

d) To use the INCISIVE platform through a browser on Linux, User will need: 64-bit Ubuntu 16.04+, Debian 10+, openSUSE 15.2+, or Fedora Linux 32+.

3.2 Minimum Hardware requirements:

a) Pentium 4 or newer processor that supports SSE2

b) 512MB of RAM / 2GB of RAM for the 64-bit OS

c) 200MB+ of hard drive space

3.3 Recommended Hardware

a) Pentium 4 or newer processor that supports SSE3

b) 2GB of RAM / 8GB of RAM for a 64-bit OS

c) 500MB+ of hard drive space

4 Registration in the INCISIVE Platform

4.1 User can only use Platform after having registered, and upon registration, the user accepts these General ToU, on behalf of himself (herself) and – when acting as an administrator – on behalf of their organization, in their entirety and without reservation, as well as he/she acknowledges the Privacy Policy. In addition, depending on the applicable role, the user needs to accept the terms of the Data Sharing Agreement, terms applicable for the Data Users or specific conditions of the AI tool provided on the Platform.

4.2 In order to use the Platform, the potential user must apply for access to the Platform. The approval of the user will be provided in accordance with the requirements and processes

defined by the INCISIVE Project. This may include a process agreed to by IINCISIVE Project with EU funded initiatives, such as EUropean Federation for CAncer IMages (EUCAIM).

4.3 In order to use the Platform the person representing the User Institution (acting as the administrator) will need to register, create an account and appoint users from the User Institution. By registering a user, the individual declares that they are legally competent in their own jurisdiction to enter into binding agreements, are at least 18 years and that they are the person whose details are provided in connection with their user account.

4.4 User is not allowed to transfer their rights and obligations under these General ToU to any third party.

5 Rights and obligations of users of the Platform

5.1 User must only use the Platform in good faith and in compliance with the applicable law.

5.2 User must use all reasonable security measures when using the Platform.

5.3 User must follow good practice within their institution in relation to the disclosure of (confidential) information on or through the Platform.

5.4 User must keep their login credentials for gaining access to their account confidential and may not share them with others. Any unauthorised use of user's login credentials not resulting from a security breach at the Platform side, shall be the user's own responsibility and happen at their own risk. User is responsible to keep their information up-to-date and to back up any information they may require in the future.

5.5 User is solely responsible for the use of the Platform through their account, whether or not authorised by the user, by any employee or co-worker of the user, any person to whom the user has given access to the services and/or any person who gains access to user's Data or services as a result of a failure by the user to use reasonable security precautions.

5.6 Notwithstanding any provisions of Consortium Agreement applicable between INCISIVE Beneficiaries, the user shall only use information obtained through the Platform for their own lawful purposes and with respect to any limits set in relation to that particular piece of information. Data Users shall observe limitations of the use of Data, as provided for in these General ToU and the Data User Terms.

5.7 Unless otherwise provided for in the General ToU or the Consortium Agreement (when applicable), the user cannot share any information obtained through the Platform without the prior, explicit and written consent of all involved parties, including Data Providers.

6 Restrictions on the use of the Platform

6.1 When using the Platform, the users must do so for lawful purposes only and cannot:

a) use the Platform to share information and material infringing on anyone else's rights;

b) use the Platform or share any information or Data in a manner that would constitute a breach of other persons intellectual property rights or individual's privacy (including

uploading Data Subject's private or personal information without a legal basis) or any other legal rights;

c) attempt to re-identify any Data Subject's whose Data is available on the Platform;

d) use the Platform in any way that is or may be damaging to other users, INCISIVE Beneficiaries or in any way contrary to applicable laws and regulations, or that may cause harm to the Platform, or to any person or entity using the Platform;

e) use the Platform to use, extract or disclose another user's or third party's data in any manner that is beyond or contrary to the General ToU, Data User Terms or any other terms and conditions of the Platform or to harm the intellectual property rights of INCISIVE Beneficiaries or third parties;

f) modify, reverse engineer, decompile, or create derivative works from the Platform, or any of its elements (contrary to these General ToU, Data User Terms or without a specific permission) nor to remove or alter any copyright or other proprietary notices in the Platform, unless specifically authorized by the provider of the service or the tool;

g) tamper with or modify the Platform, use or instal any viruses, spyware, malware, data gathering tools or any other malicious code or programming routines that may damage or interfere with the Platform, or any of its Data or tools, in connection with use of the Platform;

h) disrupt the functioning of the Platform or make any changes to the Data shared in the Platform; this does not prevent conducting AI Model training on the Data, as long as the original Data hosted in the Federated Node or the Central Node (depending where the Data is stored) is not modified nor copied outside the relevant node;

i) copy, modify, download, sell or exploit the Data or other content of the Platform (including and not limited to text, images, logos, etc.) in any other manner than permitted in these General ToU or Terms and Conditions for the Users without INCISIVE Project consent;

j) take any action that imposes an unreasonable burden upon the infrastructure used to support the Platform, including but not limited to unsolicited e-mail, also called SPAM;

k) facilitate or assist a third party to do any of the above acts.

7 Rights and obligations of the INCISIVE Beneficiaries

7.1 INCISIVE Project and/or respective INCISIVE Beneficiaries reserve the right to:

a) To remove or modify any of the Data, AI models or guidelines or other content that is infringing or otherwise deemed to be inappropriate or outdated. Data shared by an external Data Provider will not be modified by the INCISIVE Beneficiaries, however INCISIVE Project may decide to remove this Data from the Repository;

b) To change or update the functionalities of the Platform;

c) To restrict user's access to their account or to suspend or delete their account in the event of infringement of these General ToU, other applicable terms or justified suspicion of the infringement;

d) To change these General ToU, however the changes will not contradict the requirements of the INCISIVE project as provided for in the DoA (in particular, will not pertain to the core functionality of the Platform or the agreed use of Data);

e) To record and monitor data traffic generated by users to verify compliance with the conditions of use as well as to track the use of the Data on the Platform. The activity of the users will be monitored in accordance with the Privacy Policy.

7.2 INCISIVE Beneficiaries can take any of the above actions at any time and at their full discretion. User will be informed about these actions, as appropriate.

7.3 INCISIVE Project is a research and innovation action and its results will be prototypes and not fully deployable technologies. In particular, AI Models, Inference Services or any other tools available on the Platform are research results and have not been the subject matter of clinical evaluation or conformity assessment. Platform or any of its services or tools must not be used for diagnostic or therapeutic decisions.

7.4 The content or outcomes generated on the Platform (including predictions of the AI Models available on the Platform or Inference Services) cannot be construed as a legal, medical or other professional advice. The information or materials on this Platform are made available to provide general information only and no reliance should be placed upon it for any specific purpose. While care has been taken to ensure that such information on this Platform is accurate and complete INCISIVE Beneficiaries do not accept any liability where this is found not to be the case.

7.5 The accuracy of the information and outcomes provided by the Platform and/or each respective tool or service is the result of best effort but cannot be guaranteed. Any use of the Platform, Data, AI Models, other tools and services or information provided through the Platform by INCISIVE Beneficiaries, or another party is at user's sole discretion and at user's own risk. INCISIVE Beneficiaries cannot be held liable for any damage caused by external user content, Data or information, as well as for the unless damage was caused by their wilful act or gross negligence.

7.6 INCISIVE platform may be periodically unavailable, due to development work, maintenance or other unforeseen circumstances. INCISIVE will strive to inform the users in advance of the scheduled maintenance work. If the Data is stored in the Federated Node by its Data Provider, the Beneficiaries cannot guarantee uninterrupted access to Data. User is responsible for backing up any information for long term storage.

8 Liability

8.1 All users and INCISIVE Beneficiaries are liable for their respective obligations under the GDPR and/or other Data Protection Laws applicable to them. External users shall be responsible and liable for any damages, losses and fines resulting from its own actions or failures to adhere to these terms and applicable Data Protection Law and shall indemnify

and hold harmless INCISIVE Beneficiaries for any of such damages. For the purposes of this sub clause, actions or omissions of co-workers, or other employees contracted by users, shall be attributed to the user.

8.2 Neither INCISIVE Beneficiaries nor the external Data Providers:

a) are liable for any use by the Data User of the Data and/or Results created with the use of the Data, or any loss, claim, damage or liability of whatsoever kind of nature, which may arise from or in connection with the use, handling, storage or deletion of the Data and/or Results mentioned above, unless damage was caused by a wilful act or gross negligence;

b) warrant or guarantee that the Data will be accurate, be merchantable or useful for any particular purpose, including the Data User's research purpose.

8.3 Should any liability arise, each INCISIVE Beneficiary shall be solely liable for any loss, damage or injury to third parties (including external Data Providers, Data Users or other users of services provided on the Platform) resulting from the performance of that Partner's obligations by them or on their behalf under the Consortium Agreement or from its use of Results or Background.

8.4 INCISIVE will make every effort to operate the Platform with reasonable care and skill, however these services and tools of Platform are brought by INCISIVE Beneficiaries, 'as is' and 'as available'. INCISIVE Beneficiaries make no warranties as to the Results that may be obtained by using the Platform or the correctness of the information shared on the Platform. INCISIVE Beneficiaries are not responsible for verifying the Data provided by the external Data Providers. To the extent permitted by law, the INCISIVE Beneficiaries will not be liable for any damage, direct or indirect that the user may suffer in relation to their use of the Platform, any of its tools or services, or Data, unless the damage has been caused intentionally or by gross negligence. In the event of any default or liability between the INCISIVE Beneficiaries, the terms of Consortium Agreement will apply.

8.5 The Platform may contain links to one or more third party websites. Those links are provided solely as a convenience to users and INCISIVE Beneficiaries are not responsible for the content or practices of third party websites or their operators and are not liable or responsible in any way for any loss or inconvenience in connection with use of a third party website.

9 Additional terms of use of the AI Models

9.1 The User is responsible for reviewing the guidelines and terms and conditions of use of each AI Model which may be provided by the AI Model owner.

9.2 User may use the AI Models available in the Platform only for purposes described below. User may not copy the AI Models.

9.3 When uploading the AI Models to the Platform, unless otherwise specified, AI Model owner hereby grants to permitted Users a non-exclusive, perpetual and royalty free right

to use Models for non-commercial research, teaching and patient care purposes within the Platform, for as long as the AI Model is available on the Platform.

10 Data Access Committee

10.1 INCISIVE Project may establish a Data Access Committee to streamline the management and governance of the Data in the Platform. In particular, the Data Access Committee may verify the user requests and provide recommendations to the Data Providers on the user requests approval.

10.2 Data Access Committee will act in accordance with the instructions of the Data Providers.

10.3 INCISIVE is planning to connect to the pan-European infrastructure developed by the EUropean Federation for CAncer IMages (EUCAIM) and may cooperate or delegate certain administrative functions (such as maintaining of DAC) to this infrastructure to the extent that such functions will cover the required ethical and legal requirements at the local (Data Provider level), national and EU level. Further details of this cooperation will be developed and shared with the Data Providers and Users.

11 Termination

11.1 The user may use the Platform for indefinite time, unless otherwise stated in his/her research proposal or in case the Platform services or operation are terminated or discontinued.

11.2 If the user is violating the General ToU or Data User Terms, their account will be terminated with or without notice. INCISIVE Beneficiaries may pursue claims related to infringement of the General ToU by the user.

12 Governing Law and Jurisdiction

12.1 These General ToU are governed by the Belgian Law. Whenever possible, the provisions of these General ToU shall be interpreted in such a manner as to be valid and enforceable under the applicable law. However, if one or more provisions of these General ToU are found to be invalid, illegal or unenforceable, in whole or in part, the remainder of that provision and of these General ToU shall remain in full force and effect as if such invalid, illegal or unenforceable provision had never been contained herein.

12.2 The user agrees to try and solve any dispute regarding the use of the Platform and these General ToU through negotiations. Should negotiations fail, then all disputes concerning the validity, interpretation, enforcement, performance and termination of these General ToU shall be submitted to the jurisdiction of the courts of Brussels.

13 Miscellaneous

13.1 During the Project term, INCISIVE Platform is financed by the European Union's Horizon 2020 research and innovation programme under grant agreement No 952179 and the use of the INCISIVE Platform by the approved Users is free of charge.

13.2 INCISIVE Beneficiaries reserve the right to update these General ToU; therefore, the user should consult them regularly. The Platform content (including the Data) is subject to change without notice.

13.3 The use of the Data provided by the INCISIVE Data Providers and used by the INCISIVE Data Users is governed by the Consortium Agreement and INCISIVE data sharing agreements (data processing agreement and joint controller agreement as amended from time to time) as concluded between those Beneficiaries. These General ToU terms do not modify the terms of those Agreements.

8.3 Terms and conditions for the Data Users (Data User Terms)

[Explanation: These are specific terms that apply to AI developers which train AI Models on the shared Data. When registering the organization, the administrator will be prompted to accept the General ToU and T&C for the Data Users on behalf of the organization. Individual data users (appointed by the administrator) will be required to accept those terms when first accessing the Platform.]

1 Relationship with General ToU

1.1 These Data User Terms apply in addition to General ToU of the Platform and regulate the terms of use of Data by the users acting as Data Users.

1.2 Data User Terms are accepted by administrator of the Data User Institution, on behalf of that Institution, when registering the Institution in the Platform, and by individual Data Users, when using the Platform.

2 Data User request for Data

2.1 During the INCISIVE project, the Data Users are only members of the INCISIVE Beneficiaries (INCISIVE Data Users).

2.2 Each INCISIVE Beneficiary will provide a list of individuals which need to access the INCISIVE Platform during the term of the INCISIVE Project and will update this list constantly, as necessary to reflect changes or departures in affiliated researchers and personnel in good time to allow INCISIVE to revoke related access rights at the effective date of such change. These updates are made by email and other secure transmission channels to the Platform administrator.

2.3 INCISIVE Data User and any of his/her team members, shall ensure that the Data will be only used for the purposes for the implementation of the INCISIVE action. Any other use of Data requires a submission of candidate Data User form.

2.4 Once the INCISIVE Platform is fully operational few months before the project ends, it may become open to external Data Users. When the Platform becomes open to external Users, they must request to use the Data by submission of candidate Data User form.

2.5 Data Users are obligated to provide truthful and complete information in the candidate Data User form.

2.6 Data access request shall be reviewed by the DAC on behalf of Data Providers and validated by consensus of the Data Providers. If the use of Data for the purposes stated in Candidate Data User Form is granted, the Data Users may only use the Data for such purposes.

3 Use of Data

3.1 Data User represents and warrants that the Data shall be used in accordance with these terms, and all applicable local and international laws and regulations (including without limitation the GDPR) and the Consortium and Grant Agreement (if applicable). The Data User, on behalf of themselves and their User Organization (if acting in administrator role),

undertakes to implement and distribute any such guidelines, policies, procedures and instructions as necessary to ensure Data Users' compliance with the obligations contained in these terms and the Data Protection Law.

3.2 INCISIVE platform may be periodically unavailable, due to development work, maintenance or other unforeseen circumstances. INCISIVE will strive to inform the Users in advance of the scheduled maintenance work. If the Data is stored in the Federated Node by its Data Provider, the INCISIVE Beneficiaries cannot guarantee uninterrupted access to Data. INCISIVE Beneficiaries do not endorse or approve and are not responsible for any Data which is shared on the Platform by external Data Providers.

3.3 Data Users are aware that the Data Provider may modify the Data or withdraw their Data from the Platform, which may affect Data Users' research. While INCISIVE Project will endeavour to inform the Data Users in advance in case of planned interruption of such access or planned withdrawal of Data, Data User performs their Research Project at their own risk.

3.4 The Data User shall use the Data under the following conditions:

a) Data User will only use the Data for Federated Learning and AI research permitted on the Platform and cannot copy or corrupt the Data, modify it beyond pre-processing conducted in the scope of AI Model training (i.e. without intentionally downgrading the quality of the original Data), or use any AI Models which may conduct inference attacks, re-identification or copying the Data provided for in the Platform.

b) Data User shall not attempt to re-identify any Data Subject from the Data. In particular, Data User shall not analyse or make any use of the Data in such a way that has the potential to: (i) circumvent anonymization, pseudonymisation or similar measures taken to protect the confidentiality of Data Subjects' identity; or (ii) lead to the identification of any Data Subject; or (iii) otherwise compromise the confidentiality of any Data Subject's identity in any way, in particular Data User shall not attempt to link Data to/with other information or data, including one that is freely available without restriction, unless specifically authorised by the Data Provider.

c) In the event that any Data Subject, for whatever reason, becomes identifiable to the Data User, Data User agrees to immediately notify the Data Provider, to immediately and irretrievably remove the reference to that Data Subject and to preserve, at all times, the confidentiality of information pertaining to such Data Subject.

d) Data User may be requested to provide its AI Model for security check by the Data Access Committee (DAC), any INCISIVE Beneficiary or a vendor appointed by the DAC.

e) Data User will safeguard that any his/her employees or co-workers who have access to the Data are instructed by a binding agreement to process the personal data in accordance with the requirements stated in the GDPR.

3.5 Data User understands that their actions in the Platform may be tracked through block chain mechanism as explained in the Privacy Policy. This information may be made

available to Data Providers for review. Data User shall respond to any questions from the Data Providers, including the INCISIVE Beneficiaries, about the use of the Data.

3.6 The Data User shall report to Data Provider any incorrect or corrupted Data, as well as any use or disclosure of Data in violation of the terms.

4 Research use

4.1 The Platform is for research use only. In no event shall AI Models, data, images or other Results or generated through the use of the INCISIVE Platform be used or relied upon in the diagnosis or provision of patient care, unless applicable approvals have been sought by the Data Users.

5 GDPR and Data Protection

5.1 To the extent that the pseudonymized Data is provided by an external Data Provider (not a member of the INCISIVE project) and/or is not used for INCISIVE implementation, each Data User is considered independent controller of any use of such pseudonymized Data for their research purposes.

5.2 Data User may inquire with the Data Provider about a copy of the informed consent template (if applicable) and/or ethics approvals if this is relevant for the planned research use of the Data.

5.3 If any Data User becomes aware of a personal data breach related to Data on the Platform, the Data User shall promptly notify the relevant Data Provider, whose Data was affected. In such a case Parties will fully cooperate with each other to remedy the personal data breach, fulfil the statutory notification obligations in accordance with the GDPR and any other Data Protection Laws. In case the Data User receives a request from a Data Subject to exercise his/her rights according to the GDPR, the Data User will refer the Data Subject to the Data Provider.

5.4 If the Data User is located outside of European Economic Area, in a country which has not been declared as offering an adequate level of protection through a European Commission decision (‘adequacy decision’), or the Data would be accessed from such country, prior to any use or access to pseudonymized Data on the Platform, the Data User must enter into standard contractual clauses in accordance with the Commission Implementing Decision on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679.

6 Security of Data

6.1 When using the Data, the Data User shall maintain appropriate administrative, technical and organizational measures to meet the requirements of Art. 32 GDPR to protect the Data from misuse and unauthorized access or disclosure. The Data User is in particular liable for:

a) any access to and use of the Data by the Data User or any employee of the Data User Institution;

b) any access to the Data or the INCISIVE Platform through the Data User's access accounts or credentials;

c) implementing, testing, reviewing good practices in terms of information security (such as, clean desk policy, credentials management including non-sharing of credentials) and regularly training individuals from the Data User organization on those rules to ensure that those individuals comply at all times with these terms and Data Protection Law,

d) revoking immediately compromised (lost, stolen or shared) credentials with individuals from the Data User or Data User Institution by contacting the Platform administrator.

6.2 INCISIVE reserves the right (in its sole discretion) to suspend the access or account of Data Users whose credentials have been compromised or revoked, or who have acted in breach of these terms or General ToU of INCISIVE Platform.

7 IP Rights

8 License for use of Data

8.1 Data User understands that the Data Provider agrees to share the contributed Data with the Data Users registered on the INCISIVE Platform in accordance with the terms and conditions of the data sharing agreement.

8.2 Sharing of Data is free of charge and no payment is offered to the Data Provider for this sharing.

8.3 The Data and any other information provided by the Data Provider is made available as a service to the INCISIVE Beneficiaries and other Data Users admitted to the Platform. No ownership rights on the Data and any other information provided by the Data Provider shall be obtained by INCISIVE Beneficiaries or the Data Users.

8.4 When making Data available on the Platform, the Data Provider grants each Data User a limited, non-exclusive, royalty-free, revocable, worldwide, non-transferable, non-sublicensable right to use the Data for the purpose of the implementation of INCISIVE Project and/or for purposes stated by the admitted Data Users which may be approved in accordance with the agreed Data User acceptance process.

8.5 After expiration or termination of this Agreement or withdrawal of Data from the Platform by the Data Provider, INCISIVE Beneficiaries shall immediately cease using the Data and either return or demonstrably and irretrievably delete the Data (including copies, if any).

8.6 During the INCISIVE Project, unless otherwise agreed with the Data Provider, the Data shared by the Data Provider will be used by the INCISIVE Data Users for the purposes of fulfilment of the goals of the INCISIVE Project. Any other use of external Data Provider's Data by the INCISIVE Data Users require permission in accordance with the agreed Data User acceptance process.

8.7 The Data User acknowledges that the Data Provider retains ownership of as well as all right, title and interest to the Data.

8.8 All results, AI models and inventions generated by a Data User as a result of using the Data for their AI Models training (hereinafter: '**Results**') shall be the property of Data User or Data User Institution.

8.9 Notwithstanding the above and the provisions of the Consortium Agreement (if applicable), if Results are generated by active collaborative efforts of the Data Provider (meaning efforts beyond mere provision of the Data to the INCISIVE repository) and Data User, such Results shall be held in co-ownership by the Parties.

8.10 Data User Institution and Data Users will refrain from making IP claims relating to the Data and/or which may result in restrictions, conditions on the Data or otherwise create obstacles to the use of the Data by Data Provider or other Data Users.

8.11 On request, Data User shall disclose such Results to Data Provider in writing and specify Data Provider's role as the Data Provider of the Data used, as well as the role, if any, of any Data Provider's employee in creating such Results.

9 Publications

9.1 In all oral presentations or written publications (describing the Results, in particular AI Models, trained on this Data), the Data User agrees to provide acknowledgement of the Data Provider and INCISIVE Platform as the source of the Data. The acknowledgement shall be provided according to the guidelines indicated on the Platform.

9.2 Data User shall protect the confidentiality of Data in any publications by taking all possible care to limit the possibility of identification.

9.3 With a view to ensuring that INCISIVE policies and procedures applicable to the access to and use of Data are respected, at the end of their project, the User undertakes to provide to INCISIVE or its Data Access Committee, a report detailing how the Data have been used, including any Results generated as a result of the use of the Data and publications (with a copy thereof).

9.4 INCISIVE may publish the title and a short summary of successful Data user stories and publications on the INCISIVE Platform of INCISIVE website.

8.4 Template Data Sharing Agreement with the Data Providers

[Explanation: These are template terms to be proposed to external Data Providers which wish to share the data on the Platform.]

This agreement, further referred to as 'Agreement', effective as of [DATE] is executed (the 'Effective Date'), by and between:

(1) [FULL NAME OF THE DATA PROVIDER] - whose administrative offices are at [ADDRESS], validly represented by [NAME], in the capacity of [CAPACITY] (the 'Data Provider' or 'external Data Provider')

And

(2) MAGGIOLI S.P.A., established in VIA DEL CARPINO 8, 47822 SANTARCANGELO DI ROMAGNA, Italy, validly represented by [NAME], in the capacity of INCISIVE Beneficiaries (the 'Coordinator'),

individually, a 'Party' and, collectively, the 'Parties'.

Whereas:

- INCISIVE Beneficiaries manage the 'INCISIVE Repository', an Interoperable pan-European hybrid repository of health images and related data that allows sharing data in compliance with legal, ethical, privacy and security requirements, for AI-related training and experimentation.
- INCISIVE's mission is to develop this Repository in a sustainable and inclusive way, by connecting the community of healthcare professionals, researchers, AI developers, patients and industry parties.
- Subject to the Consortium Agreement and intra-project data sharing arrangements, INCISIVE Data Providers participate in the provision of Data to the Repository. INCISIVE Data Users use the Data through AI training techniques to develop AI Models for the purpose of INCISIVE. To further develop the Repository, INCISIVE project wishes to engage with external stakeholders, who will act as additional Data Providers.
- The INCISIVE (or – in the future - possibly an entity/project to which INCISIVE has delegated this role) has assessed the information provided in application submitted by the Data Provider and recognizes the interest of the data identified by Data Provider for INCISIVE, and the alignment of its vision and profile with INCISIVE.
- INCISIVE acknowledges the launch of EUCAIM Project EUropean Federation for CAncer IMages (EUCAIM) funded as a flagship project by the Digital Europe Programme. Among other objectives, EUCAIM aims at enabling the interoperability at technical and semantic level between several existing data infrastructures, including the AI4HI repositories. Given that EUCAIM can significantly help in the sustainability of the INCISIVE data repository, INCISIVE aims at facilitating the sharing of its Data through the EUCAIM pan-European digital federated infrastructure of FAIR pan-cancer images. It also aims at facilitating technical interoperability of the INCISIVE data repository with other cancer

imaging repositories, such as the AI4HI repositories. The proposed legal terms already anticipate such cooperation.

- Now, therefore, and in consideration of the abovementioned premises and the covenants and agreements set forth below the Parties agree as follows:

1 Representations

1.1 Each Party represents and warrants that (i) it has the full right and authority to enter into and perform its obligations as set forth in this Agreement; (ii) it will not grant any rights in conflict with this Agreement; (iii) to its best knowledge, the rights granted pursuant to this Agreement do not and will not infringe any Data Subject's or third party rights and, notwithstanding the foregoing, each Party will notify the other immediately after becoming aware of any Data Subject or third party right infringement.

1.2 The Data Provider appoints [NAME, LAST NAME], [POSITION], with email address [EMAIL] as contact person for the provided Data to address potential questions from INCISIVE Beneficiaries in relation to the information on the contributed Data. The Data Provider shall immediately notify of any changes in relation with this contact person to the Coordinator.

2 Definitions & relationship with General ToU

2.1 All definitions of the General Terms of Use of the Platform ('General ToU') will apply, in case of conflict, the terms of this Agreement and its definitions will prevail.

2.2 The following capitalized terms used in this Agreement shall have the following meanings (any other capitalized terms shall have the meaning assigned to it in the General ToU):

a) 'Confidential Information' - All information, know-how, grant applications, method of work, techniques, expertise of disclosing Party, including information regarding the Data, Platform, security measures, tools, their characteristics as well as research, whether of a scientific, technical, engineering, operational, or economic nature, supplied to or obtained by the receiving Party.

b) 'Central Node Provider' - The INCISIVE Beneficiary providing for the hosting of the Central node i.e. Maggioli S.P.A.

c) 'Federated Node Provider' – Data Provider which choses to host the Data that they are sharing thorough INCISIVE Platform in their own infrastructure (or infrastructure provided by their own provider) which will be connected to the Central infrastructure.

2.3 This Agreement applies in addition to General ToU of the Platform (Attachment b) and regulates the terms of sharing of Data by the users acting as Data Providers.

2.4 Where a Data Provider contributes anonymised Data to the INCISIVE Platform, it is understood that neither the GDPR nor related provisions in this Agreement apply to such anonymised Data when used and processed in the INCISIVE Platform.

3 Representations about the Data

3.1 Data Provider is responsible for all Data, information, or other content they share in the INCISIVE Platform.

3.2 Data Provider is responsible for the preparation of the Data according to prescribed steps and technical requirements determined by the INCISIVE Project. In particular, the Data must be de-identified (i.e. anonymized or pseudonymized, using tools provided by INCISIVE or other appropriate tools), annotated (unless it is agreed that no annotations will be provided) and must pass the data integration quality check. The details of the Data preparation steps and requirements are available on the public information pages of the Platform.

3.3 Data Provider must provide accurate and complete description of the Data (metadata), in accordance with the requirements of the INCISIVE Project.

3.4 The Data Provider represents and warrants that:

a) The description of its Data and other information given in the Candidate Data Provider Form is accurate, complete and correct (Attachment a);

b) To Data Provider's best knowledge it's sharing of Data complies with all applicable privacy and personal data laws and regulations (including the Data Protection Laws), notably that all consents, waivers, authorisations from Data Subjects and/or ethics approvals or other approvals required from competent authorities or bodies necessary for the valid legal ground of processing, including for sharing of Data as described below, have been obtained by the Data Provider;

c) Data Provider has a right to make that Data accessible for AI training in the INCISIVE Platform (i) by the INCISIVE Beneficiaries (during the Project) and (ii) other Data Users (after the Project) and that sharing the Data by Data Provider does not infringe, violate or misappropriate any privacy rights of the Data Subjects or intellectual property rights of third parties;

d) Data Provider remains responsible for managing the consents of the Data Subjects, if applicable, and that such consent covers: (i) allowing use of Data that is stored in Federated Node or Central Node by INCISIVE Beneficiaries for the purpose of cancer research and for AI training as part of implementation of the INCISIVE Project, (ii) sharing of Data with researchers within and outside of the European Union/EEA (where applicable); (iii) use of Data for the research and learning purposes of AI training and validating technologies related to cancer research and healthcare improvement in general, by INCISIVE Beneficiaries and by other researchers outside the INCISIVE Project, as described in this Agreement and also in the framework of the EUropean Federation for CAncer IMages (EUCAIM). Data Provider will be responsible for informing INCISIVE Project about any withdrawal of Data Subjects' consent without undue delay;

e) Data shared on INCISIVE Platform corresponds to the requirements and guidelines on Data provided on the Platform, notably that it relates to imaging data (MRI, US, CT, PET-CT, Mammography, radiography and histopathological images) for any of the four types of cancer e.g., breast, colorectal, prostate or lung cancer as DICOM or NIfTi files and de-

identified clinical metadata related to the imaging data as excel files (.xls) following a specific template.

3.5 INCISIVE retains a right to refuse to include any Data in the Repository, or to discontinue with immediate effect the making the Data available via connection to the Federated Node or storage of Data in the Central Node (in the latter case the Data Provider accepts that INCISIVE may decide, in its discretion, to proceed immediately and without further notice to the destruction of all copies of Data held by INCISIVE hereunder), if:

a) the Data Provider fails to provide the required metadata;

b) the Data Provider does not respect the General ToU;

c) the Data Provider is found in breach of its representations and warranties;

d) INCISIVE is notified by Users or third parties about the illegal or infringing nature of Data;

e) based on reasonable grounds, INCISIVE considers that Data is infringing third parties' rights or may otherwise be illegal or its processing for purposes stated in this Agreement be contrary to Data Protection Law;

f) Data is not useful to the purposes of the INCISIVE repository; or

g) the Data Provider unreasonably delays Data Access Committee decisions or denies access to Users.

4 License for use of Data

4.1 The Data Provider hereby agrees to share the contributed Data with the Data Users registered on the INCISIVE Platform in accordance with the terms and conditions of this Agreement, General ToU and Data User Terms.

4.2 Sharing of Data is free of charge and no payment is offered to the Data Provider for this sharing.

4.3 The Data and any other information provided by the Data Provider is made available as a service to the INCISIVE Beneficiaries and other Data Users admitted to the Platform. No ownership rights on the Data and any other information provided by the Data Provider shall be obtained by INCISIVE Beneficiaries or the Data Users.

4.4 When making Data available on the Platform, the Data Provider grants each Data User a limited, non-exclusive, royalty-free, revocable, worldwide, non-transferable, non-sublicensable right to use the Data for the purpose of the implementation of INCISIVE Project and/or for purposes stated by the admitted Data Users which may be approved in accordance with the agreed Data User acceptance process.

4.5 After expiration or termination of this Agreement or withdrawal of Data from the Platform by the Data Provider, INCISIVE Beneficiaries shall immediately cease using the Data and either return or demonstrably and irretrievably delete the Data (including copies, if any).

4.6 During the INCISIVE Project, unless otherwise agreed with the Data Provider, the Data shared by the Data Provider will be used by the INCISIVE Data Users for the purposes of

fulfilment of the goals of the INCISIVE Project. Any other use of external Data Provider's Data by the INCISIVE Data Users require permission in accordance with the agreed Data User acceptance process.

5 Storage of Data and Data Provider's control of the use of Data

5.1 The Data will be stored, at the choice of the Data Provider, in the Federated Node or in the Central Node or both. Unless otherwise agreed, the Data will not be copied from the Federated Node or the Central Node by the INCISIVE Project or the Data Users. If the Data Provider enables viewing of the Data by installation settings, the Data may also be viewable to the Data Users in the Repository.

5.2 Data Provider shall indicate its choice referred to in 5.1 above to INCISIVE Beneficiaries and shall follow the below requirements:

a) When sharing the Data with the use of Federated Node, the Data will remain in the Data Provider's infrastructure (including any external or cloud storage selected by the Data Provider and being under their control) and the Data Provider shall act as Federated Node Provider. For storage of Data in Federated Node, the Federated Node Provider must follow the INCISIVE guidelines. Federated Node Provider remains responsible for security measures deployed in the Federated Node.

b) When sharing the Data with the use of Central Node, the Data Provider must additionally sign a data processing agreement in writing. The template of the data processing agreement is provided in Attachment c: Terms of Storage of Data in the Central Node: Data Processing Agreement. Additionally, Data Providers located outside of European Economic Area who wish to store pseudonymized Data in the Central Node will need to enter into standard contractual clauses agreement in accordance with the Commission Implementing Decision on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679.

5.3 When the Data will be stored:

a) In the Federated Node, it will be used only for Federated Learning;

b) In the Central Node, it may be used both for Federated Learning and also for other AI training, which takes place in the Central Node (if agreed by the Data Provider).

5.4 The use of Data will be tracked using blockchain technology recording the INCISIVE Data transactions, thus ensuring transparency and traceability. On request, the INCISIVE Project undertakes to provide to the Data Provider a list detailing how their Data have been used.

5.5 The Data Provider may withdraw the shared Data from the Platform. For the INCISIVE Data Providers any withdrawal must comply with the obligations of the DoA. The Data Provider may inform the Coordinator of their intent to withdraw the Data in advance of 1 month. In urgent cases (such as, for example, data breach or other privacy violation), the Data Provider may immediately disconnect its Federated Node or demand that their Data is immediately deleted from the Central Node. Once the withdrawal of Data is in effect, the Data Users shall immediately cease using the Data.

6 GDPR and Data Protection

6.1 This Agreement regulates any sharing of Data by the external Data Providers with INCISIVE Data Users and/or by external Data Users (once they are approved). For those purposes, the Data Provider does not (co-)initiate the research, nor participate in the performance of the research conducted by the Data User.

6.2 For any Data which is personal data, the Data Provider is considered controller in relation to the collection, pseudonymization or anonymization and transfer/sharing of Data to the Platform.

6.3 Data Provider is responsible for ensuring and documenting legal basis for the sharing of Data through the INCISIVE Platform, obtaining ethical approvals as well as compliance to any other applicable European or national regulations and ethical requirements. At the request of INCISIVE Beneficiaries or Data Users, Data Provider may be required to provide a copy of the informed consent template (if applicable) and/or ethics approvals for review. If applicable, Data Provider shall perform their own Data Protection Impact Assessment. In particular, it is the responsibility of the Data Provider to consider the risk of re-identification of any shared Data. Data Provider should also check whether Data Subjects need to be informed about the (re)use of the Data.

6.4 Data Provider is solely responsible for de-identification of the Data prior to its sharing to the Platform. The Data Provider may make use of the de-identification tools provided on the Platform or may use external tools. In both cases, the Data Provider must carefully read the terms and conditions (including any limitations) of the used de-identification tools and verify that the Data have been properly de-identified. INCISIVE shall make available to the Data Provider supporting documentation regarding the de-identification protocols and tools available on INCISIVE data sharing Platform.

6.5 The use of the INCISIVE de-identification tools may not be treated as a substitute for Data Provider's review and assessment of the shared Data. Those tools are provided 'as is' and do not guarantee that the Data will be irrevocably anonymized and unable to be linked to the Data Subjects. In particular, INCISIVE is not responsible for storage of original (raw) data by the Data Providers. Data Provider should evaluate that the patient would not be directly identifiable from the submitted health information or the image itself before submitting the Data, i.e., validate whether the anonymization/pseudonymization was done correctly. When in doubt Data Provider shall consult its Data Protection Officer or its privacy advisors. INCISIVE will follow Data Provider's final assessment of this aspect.

6.6 If the Data that is shared is pseudonymized:

a) Any information which can re-identify the Data, such as the codes/ID mapping key shall be kept by the Data Provider separately, outside of the Platform and be protected by protected by technical and organisational measures; this information will not be shared with the Platform or its Users.

b) When using the Data for medical research, the Data User is considered independent controller in the context of processing of pseudonymized Data for the purpose of

conducting its research. The Data Provider and Data User will both act in accordance with the applicable Data Protection Laws (including but not limited to the GDPR).

c) the Data Provider shall manage requests from Data Subjects for access, rectification, restriction of processing, data portability, objection to the processing or erasure of their Data. In case the Data User receives a request from a Data Subject to exercise his/her rights according to the GDPR, the Data User will refer the Data Subject to the Data Provider.

d) If Data Subjects from whom the Data has been derived decide to withdraw consent for use of their Personal Data, the Data Provider will be responsible for withdrawing their data from the Repository. If the Data is kept at the Central Node, then it will instruct the Central Node Provider accordingly.

e) The Data Provider shall conclude a standard contractual clauses agreement in accordance with the Commission Implementing Decision on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 with Data Users from countries which have not been declared as offering an adequate level of protection through a European Commission decision ('adequacy decision').

6.7 If the Data that is shared is anonymized:

a) The Data Provider shall apply appropriate anonymization process to ensure anonymization of the Data, so as to avoid that any Data qualifies as personal data within the meaning of Data Protection Law; in such case, the Data Provider undertakes to review the Data's anonymisation process periodically.

7 Security of Data

7.1 On request, subject to confidentiality requirements outlined below, INCISIVE will disclose to Data Provider the description of the technical and organizational means to protect the security and integrity of Data in INCISIVE Platform.

7.2 When storing the Data in the Federated Node, the Data Provider as Federated Node Provider shall maintain appropriate administrative, technical and organizational measures to meet the requirements of Art. 32 GDPR to protect the Data from misuse and unauthorized access or disclosure.

7.3 When storing the Data in the Central Node, the responsibilities of the Data Provider and the Central Node Provider regarding the security of Data will be outlined in the Terms of storage in the Central node (Data Processing Agreement in Attachment c).

8 Data Access Committee

8.1 INCISIVE Project may establish a Data Access Committee to streamline the management and governance of the Data in the Platform. In particular, the Data Access Committee may verify the user requests and provide recommendations to the Data Providers on the user requests approval.

8.2 Data Access Committee will act in accordance with the instructions of the Data Providers.

8.3 INCISIVE is planning to connect to pan-European infrastructure developed by EUropean Federation for CAncer IMages (EUCAIM) and may cooperate or delegate certain administrative functions (such as maintaining of DAC) to this infrastructure. Further details of this cooperation will be developed and shared with the Data Providers and Users.

9 IP rights to the Data

9.1 Data Provider confirms that it has the right to share the Data to the INCISIVE Platform. INCISIVE Beneficiaries are not responsible for checking the Data contributed by the external Data Provider and shall rely on the representations of the external Data Provider regarding third party rights to the Data, including intellectual property rights, security or trade secrets.

9.2 Data Provider retains ownership of as well as all right, title and interest to the Data.

9.3 Data Provider acknowledges and agrees that all results, AI Models and inventions generated by Data User as a result of using the Data for the Project (hereinafter: '**Results**') shall be the property of Data User. Data Provider may request a list of Results from the Data User.

9.4 Notwithstanding the above and the provisions of the Consortium Agreement (if applicable), if Results are generated by active collaborative efforts of the Data Provider (meaning efforts beyond mere provision of the Data to the INCISIVE repository) and Data User, such Results shall be held in co-ownership by the Parties.

10 Publications

10.1 The Data Provider will be entitled to be listed as the source of Data in any publications or articles describing the Results, in particular about AI Models, trained on this Data. With a view to ensuring that Data Users acknowledge the Data Provider's role and contribution to their research project in all Publications resulting from any use of the Data for Federated Learning or AI training, the Data Provider will provide acknowledgement for publication when submitting the Data.

10.2 The provision of the Data to INCISIVE in no way prevents or restricts the Data Provider right to publish any document relating to the Data.

10.3 Data Provider shall be able to request the list of Data Users which used the Data for training to verify the fulfilment of the above provision.

10.4 The Data Provider gives consent for INCISIVE Project to use Data Provider's institutional (corporate) name, contact details and/or logo when communicating about the inclusion of Data from Data Provider in the INCISIVE Platform.

11 Confidentiality

11.1 The Parties acknowledge that they may share Confidential Information during the course of cooperation. Unless otherwise agreed between the Parties, they may use Confidential Information only to implement the activities within the limits of this Agreement. In particular, INCISIVE Beneficiaries undertake to hold in strict confidence any information

about the Data, which is not disclosed or shared in the Platform according to the terms of this Agreement. The Data Provider undertakes to hold in strict confidence any information relating to the business, products or research of any INCISIVE Beneficiary which becomes known to the Data Provider during the course of negotiations of this Agreement or collaboration with INCISIVE Project. Parties will use Confidential Information only for the purposes of this Agreement; and not to disclose such information to any third party without a prior written consent of the disclosing Party. Any documentation provided must be returned to the disclosing Party at their request during the term of this Agreement and shall be returned to the disclosing Party, without being asked, upon the termination of this Agreement. A Party may keep a copy if obliged to under mandatory law.

11.2 The Parties shall limit disclosure of Confidential Information to their personnel and other individuals under their supervision and control only if they: (i) need to know the Confidential Information to implement this Agreement, and (ii) are bound by obligations of confidentiality at least equivalent to those set forth herein; and shall not disclose confidential information to any third party (whether an individual, corporation, or other entity) without the prior written consent of disclosing Party. The receiving Party shall be responsible to the disclosing Party for any disclosure by any such personnel which violates the terms of this Agreement.

11.3 The confidentiality restrictions on use and disclosure will not apply to any such information which: (a) at the time of disclosure is in the public domain; (b) after disclosure becomes part of the public domain, except through breach of this Agreement by the receiving Party; (c) the receiving Party can demonstrate by reasonable proof was in receiving Party's possession prior to the time of disclosure, and was not acquired directly or indirectly from the disclosing Party; (d) the receiving Party can demonstrate by reasonable proof was developed by or on behalf of the receiving Party independent of and without reference to the Confidential Information; or (e) becomes available to the receiving Party from a third party who did not acquire such information directly or indirectly from a disclosing Party and who is not otherwise prohibited from disclosing such information.

11.4 Disclosure of Confidential Information shall be permitted if the receiving Party is required to do so by or in connection with any laws, regulations or legal processing, or court of competent jurisdiction, subject to applicable EU and national laws in the country which the disclosing Party operates, provided that such disclosure is subject to all applicable governmental, regulatory or judicial protection available and in so far as legally possible immediate written notice of such requirement is given to the disclosing Party with a view to agreeing the timing and the content of such disclosure.

11.5 This confidentiality and non-use obligation shall remain in effect: during the implementation of the Action and for seven (7) years after the completion of the Action, but for no more than ten (10) years after receiving the Confidential Information.

12 Liability

12.1 The Data User, Data Provider and INCISIVE Beneficiaries are liable for their respective obligations under the GDPR and/or other Data Protection Laws applicable to them.

12.2 Data Provider is responsible for making a back-up copy of the Data which they share in the Federated Node or Central Node.

12.3 The Data Provider:

a) will hold the INCISIVE Beneficiaries and Data Users harmless in relation to any claim that arises from use of the Data in breach of the warranties, representations and obligations made under this Agreement. Notwithstanding the above, they are not liable for any use by the Data User of the Data and/or Results, or any loss, claim, damage or liability of whatsoever kind of nature, which may arise from or in connection with the use, handling, storage or deletion of the Data and/or Results, unless damage was caused by a wilful act or gross negligence.

b) do not warrant or guarantee that the Data will be accurate, be merchantable or useful for any particular purpose, including for Data User's research purpose.

12.4 Should any liability arise, each INCISIVE Beneficiary shall be solely liable for any loss, damage or injury to third parties (including external Data Providers, Data Users or other users of services provided on the Platform) resulting from the performance of that Partner's obligations by them or on their behalf under the Consortium Agreement or from its use of Results or Background.

13 Miscellaneous

13.1 This Agreement will be valid for [to be determined by the Parties] years and shall be automatically renewed for subsequent [to be determined by the Parties] year term, unless terminated by either Party.

13.2 The Agreement may be terminated by Coordinator on behalf of INCISIVE before this term if:

a) the Data Provider does not ensure effective access to the Data as provided in this Agreement or in any other way commits a material breach of the Agreement or General ToU;

b) the financing from the European Union is discontinued, substantially reduced or the INCISIVE Project is terminated;

c) the Data shared with the Platform does not meet the required format and quality check, or otherwise is of such low quality that it is hard to use it or access for the Users.

In such a case, INCISIVE will notify the Data Provider of the termination.

13.3 The Data Provider agrees for the INCISIVE Beneficiaries to transfer the rights and obligations arising from this Agreement to pan-European infrastructure developed by EUropean Federation for CAncer IMages (EUCAIM) or a joint-venture/entity created by INCISIVE beneficiaries for sustainability purposes. In such a case the Data Provider shall be

informed about the transfer, change of these terms (if any) and given the opportunity to object within a reasonable period.

13.4 Other than provided above, these terms may only be altered or amended by an instrument in writing signed by all of the Parties. INCISIVE Coordinator will sign the amendment on behalf of the INCISIVE Beneficiaries, within the scope of authorization and subject to prior approval of the INCISIVE Beneficiaries.

13.5 The Parties agree that the transmission of an electronic copy (e.g. scanned pdf) of the Agreement signed in wet ink or an electronic signature pursuant to the EU-elDAS-Regulation shall in any case be sufficient to comply with the agreed written form requirement.

13.6 If any portion of this terms is in violation of any applicable law or regulation, or is unenforceable or void for any reason whatsoever, such portion will be inoperative and the remainder of this Agreement will be binding upon the Parties.

13.7 Parties acknowledge that the signatories to this Agreement are authorized representatives of each of the Parties and legally authorized to sign this Agreement.

13.8 If the lawful performance of any part of this Agreement by a Party is rendered impossible by or as a result of any cause beyond such Party's reasonable control, such Party will not be considered in breach hereof as a result of failing so to perform.

13.9 Attachments:

a) Description of Data and other information given in the Candidate Data Provider Form

b) General Terms of Use the Platform and Data User Terms

c) Terms of Storage of Data in the Central Node: Data Processing Agreement

For INCISIVE Beneficiaries:	For Data Provider:
Name: _____	Name: _____
Position: _____	Position: _____
Signature: _____	Signature: _____

8.5 Terms of storage in the Central node (including Data Processing Agreement)

[Explanation: This would be attached to Data Sharing Agreement as Attachment c and would only be applicable for those Data Providers which store the Data in the Central Node.]

This agreement, further referred to as 'Central Node ToS', effective as of [DATE] is executed (the 'Effective Date'), by and between:

(1) [FULL NAME OF THE DATA PROVIDER] - whose administrative offices are at [ADDRESS], validly represented by [NAME], in the capacity of [CAPACITY] (the 'Data Provider')

And

(2) Maggioli S.P.A., established in VIA DEL CARPINO 8, 47822 SANTARCANGELO DI ROMAGNA, Italy, validly represented by [NAME], in the capacity of INCISIVE Beneficiaries (the 'Central Node Provider'),

individually, a 'Party' and, collectively, the 'Parties';

Whereas,

- The Data Provider and Central Node Provider have concluded Data Sharing Agreement for the sharing of Data in the INCISIVE Platform;
- The Data Provider will be sharing the Data with the use of the Central Node, which is provided as a service to the Data Provider by the Central Node Provider;
- These terms of storage regulate the obligations of the Parties related to hosting the Data in the Central Node.

1 Definitions

1.1 These Terms of storage in the Central node ('Central Node ToS') are concluded between the Data Provider and Central Node Provider only.

1.2 Capitalized terms shall have the same meaning as in the Data Sharing Agreement and General ToU.

2 Description of processing. Instructions of the Data Provider.

2.1 The subject-matter of the processing under these Central Node ToS is the storage of Data by Central Node Provider on behalf of the Data Provider which selected storing of the Data in the Central node.

2.2 Data is pseudonymized or anonymized health data related to patients (Data Subjects). The exact scope of Data (data categories) have been defined in the Data Sharing Agreement. For pseudonymized Data, the Central Node ToS contain Data Processing Agreement terms in accordance with Art. 28 GDPR. For anonymized Data, the Data Processing Agreement terms will apply *mutatis mutandis* to ensure that the Data is stored securely and is not re-identified.

2.3 The processing operations performed by Central Node Provider will consist in (nature of the processing) providing infrastructure for storing Data for the purpose of making it

available in the Repository for Federated Learning and/or AI training in the Central Node by authorized Data Users.

2.4 Central Node Provider will process the Data only on documented instructions from Data Provider, including with regard to transfers of Data to a third country or an international organisation, unless required to do so by EU or Member State law to which Central Node Provider is subject; in such case, Central Node Provider will inform Data Provider of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest. Central Node Provider will immediately inform Data Provider if, in its opinion, an instruction could entail a breach or infringes the GDPR or other EU or Member State data protection provisions, and ask Data Provider to withdraw, amend or confirm the instruction in question. Central Node Provider, as processor, may suspend application of the instruction in question while awaiting the Data Provider' decision regarding the withdrawal, amendment or confirmation of the relevant instruction.

3 Security of Data

3.1 The Data will be uploaded to the Central Node and accessed by Data Provider via VPN and in accordance with agreed protocols.

3.2 The Central Node Provider will take measures required pursuant to Article 32 GDPR in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject. These measures will at least be: (i) the pseudonymization of personal data, which will be performed by the Data Provider and encryption during upload of Data to the Central Node, as applicable; (ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (iii) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and (iv) the process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

3.3 The Data kept in the Central Node shall be protected as described in the document 'Description of the Hybrid Repository and Technical and Organisational Measures to Ensure the Security of the Data'.

3.4 Data Provider shall be informed of any changes to the storage and security measures. The security measures applied to safeguard Data will provide a level of security no lesser than described in point 3.2 above.

4 Sub-processors

4.1 By means of this Central Node ToS, Data Provider authorizes Central Node Provider to engage other processors ('sub-processors') when it is necessary to carry out the provision of the services.

4.2 As of effective date, Central Node Provider authorized IPHOST I. K. E., located in Agia Varvara, Attica, Terpsithea 18, P.O. Box 12351 ('Service provider') to act a sub-processor providing data hosting services for the Data stored in the Central Node. Central Node

Provider shall inform Data Provider about any intended changes concerning the addition or replacement of sub-processors by sending an advance notice to Data Provider by email. These changes or replacements may be carried out by Central Node Provider as long as the Data Provider does not express their objections within a period of two weeks of receiving the email.

4.3 If Central Node Provider engages a sub-processor, it will enter into a written agreement with this sub-processor including the same or equivalent obligations as those of Central Node Provider's set forth in this Central Node ToS and meeting the requirements of Article 28 GDPR. For the avoidance of doubt, this requirement does not apply to Central Node Provider's own staff and personnel.

4.4 Central Node Provider will ensure that each of its sub-processors (if any) will comply with all their obligations under the GDPR and other applicable data protection rules, such as respecting the conditions referred to in Articles 28.2 and 28.4 GDPR for engaging a sub-processor.

5 Confidentiality

5.1 Central Node Provider will treat the Data as strictly confidential and will not directly or indirectly disclose or make these available to any third parties without Data Provider' prior, written and explicit consent, unless authorised or obliged to do so in the Data Sharing Agreement, Central Node ToS or by a legal or judicial obligation. Instructions regarding making the Data available for Users on the INCISIVE Platform are provided in the Data Sharing Agreement.

5.2 Central Node Provider shall only disclose or make available any Data to those of its employees, contractors, directors, agents and representatives who are directly involved in the performance of the Data Sharing Agreement and on a strict 'need-to-know' basis.

5.3 Central Node Provider ensures that persons authorised to process the Data have committed themselves in writing to confidentiality or are under an appropriate statutory obligation of confidentiality, and have been made aware of Central Node Provider's obligations under the GDPR, other Data Protection Laws and this Central Node ToS.

6 Information and assistance. Audits.

6.1 Taking into account the nature of the processing, Central Node Provider will assist Data Provider by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of Data Provider' obligation to respond to requests for exercising the Data Subject's rights laid down in Chapter III GDPR.

6.2 Central Node Provider will assist Data Provider in ensuring compliance with the obligations pursuant to Articles 32 to 36 GDPR taking into account the nature of processing and the information available to Central Node Provider.

6.3 Central Node Provider will make available to Data Provider all information necessary to demonstrate compliance with the obligations laid down in the GDPR, including Article 28

GDPR, and will allow for and contribute to audits, including inspections, conducted by Data Provider, another auditor mandated by Data Provider, or a supervisory authority.

7 Security Breach

7.1 In case the Central Node Provider becomes aware of or has documented reason to believe that a security breach or personal data breach has occurred that may affect the Data, Central Node Provider shall notify Data Provider without any delay, and ultimately within 24 hours by phone and e-mail upon becoming aware of the breach, providing all information needed to allow Data Provider to meet their obligations under Articles 33 and 34 GDPR or Data Protection Laws applicable to them.

7.2 Central Node Provider will immediately take all measures needed to mitigate and remedy the breach and will at Data Provider' first request assist Data Provider and supervisory authorities in investigating the breach as well as with fulfilment of obligation under applicable data protection law to inform the Data Subjects and the supervisory authorities, as applicable, by providing information according to Art. 33.3 GDPR or other Data Protection Laws applicable to each Data Provider. Central Node Provider shall implement agreed remediation measures and corrective measures in order to prevent further breaches from occurring again.

7.3 Notwithstanding any provision in the Central Node ToS, if a third party or supervisory authority brings a claim against Data Provider in connection with an alleged infringement of any of its rights or any obligations of Data Provider, Central Node Provider or any of its sub-processors caused by Central Node Provider or any of its sub-processors, then Central Node Provider will at Data Provider' first request provide all information and assistance to Data Provider, to enable Data Provider to organise its defence.

7.4 The Data Provider shall inform Central Node Provider immediately if they notice errors or infringements regarding protection and security of Data during the performance of the processing activities.

8 Liability

8.1 The Data Provider and Central Node Provider are liable for their respective obligations under the GDPR and/or other Data Protection Laws applicable to them.

9 Deletion or return of Data

9.1 After the end of the provision of all services relating to processing, Central Node Provider shall, and must make sure that its sub-processors shall return or delete all the Data stored in the Central Node or otherwise directly and indirectly held by Central Node Provider. If Data needs to be returned, Data Provider will instruct Central Node Provider about the protocol of return of the Data. Central Node Provider will delete existing copies unless and only to the extent and for as long as EU or Member State law requires storage of the personal data.

10 Attachments, inconsistencies and severability

10.1 The defined terms are the same as in the main Data Sharing Agreement. In case the terms of this Central Node ToS are in conflict with the terms of the Data Sharing Agreement, the latter shall prevail.

10.2 Should any provision of this Central Node ToS become invalid, illegal or unenforceable, it shall not affect the validity of the remaining provisions of this Central Node ToS. In such a case, the Parties concerned shall be entitled to request that a valid and practicable provision be negotiated which fulfils the purpose of the original provision. If the Parties fail to enforce any portion of this Central Node ToS, it will not be considered a waiver. Any amendment to or waiver of obligation arising from this Central Node ToS must be made in writing and signed by all Parties.

11 Termination

11.1 This Central Node ToS will apply for as long as the Data Providers agree for the Data to be maintained and stored in the Central Node.

11.2 This Central Node ToS will be terminated upon termination of the Data Sharing Agreement and/or withdrawal of Data from the Repository.

For Central Node Provider:	For Data Provider:
Name: _____	Name: _____
Position: _____	Position: _____
Signature: _____	Signature: _____