HACID - Deliverable

Data management plan - mid term revision

This project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101070588. UK Research and Innovation (UKRI) funds the Nesta and Met Office contributions to the HACID project.

Deliverable number:	D1.4
Due date:	29.02.2024
Nature[1]:	DMP
Dissemination Level[2]:	PU
Work Package:	WP1
Lead Beneficiary:	MPG
Contributing Beneficiaries:	CNR

[1] The following codes are admitted:
- R: Document, report (excluding the periodic and final reports)
- DEM: Demonstrator, pilot, prototype, plan designs
- DEC: Websites, patents filing, press & media actions, videos, etc.
- DATA: Data sets, microdata, etc.
- DMP: Data management plan
- ETHICS: Deliverables related to ethics issues.
- SECURITY: Deliverables related to security issues
- OTHER: Software, technical diagram, algorithms, models, etc.

[2] The following codes are admitted:
- PU – Public, fully open, e.g. web (Deliverables flagged as public will be automatically published in CORDIS project's page)
- SEN – Sensitive, limited under the conditions of the Grant Agreement
- Classified R-UE/EU-R – EU RESTRICTED under the Commission Decision No2015/444
- Classified C-UE/EU-C – EU CONFIDENTIAL under the Commission Decision No2015/444
- Classified S-UE/EU-S – EU SECRET under the Commission Decision No2015/444

Document History

Version	Date	Description	Author	Partner
0.1	20.02.2024	Creation	Stefan Herzog	MPIB-MPG
0.2	21.02.2024	Initial draft	Stefan Herzog	MPIB-MPG
0.3	21.02.2024	Contribution to Amendm. 1	Alessandro Russo	ISTC-CNR
0.4	23.02.2024	Review	All	All
0.5	21.03.2024	Final review	Stefan Herzog	MPIB-MPG
0.6	21.03.2024	Final document	Stefan Herzog	MPIB-MPG

Table of content

1. Introduction

This is an amendment to the D1.3 Data Management Plan (v1 08.03.2023).

2. Amendment 1: SNOMED CT Affiliate License

In the medical case study, HACID relies on SNOMED Clinical Terms (SNOMED CT) for the standardisation and re-usability of medical terminology models. SNOMED CT is the international gold standard, providing a comprehensive, multilingual clinical healthcare terminology and is thus superior to other terminology models (e.g., ICD10, which is primarily used for coding and billing purposes). Furthermore, our consortium member Human Diagnosis Project (Human Dx, see https://www.humandx.org/) uses SNOMED CT for the crowdsourcing application used in the context of this grant.

More in detail, in the context of the medical diagnostics case study of HACID, SNOMED CT is used, together with other resources, to build the core of the so-called Domain Knowledge Graph (DKG). The DKG is thus derived from SNOMED for what concerns the representation of clinical concepts (such as disorders, findings, substances, organisms, etc.) and their relations, as well as the corresponding instances (i.e., all disorders, substances, organisms, etc.). The conceptual modelling of SNOMED was then used to enhance the ontology network with domain peculiar knowledge patterns. Data from Human DX was used for modelling the portion of the medical diagnostics ontology focused on the representation of clinical cases, collective diagnosis and procedural knowledge.

While the SNOMED CT Affiliate Licence[3] allows producing such derivative work (cf. point 2.1.2 in the licence) and use it as part of the HACID DKG, it requires that any system that has integrated SNOMED and that is made available to the general public must prevent users "to extract any substantial portion of SNOMED CT", as detailed in point 2.2.4 of the licence[4].

In the context of HACID, the constraints imposed by the SNOMED CT Affiliate Licence concretely mean the following:

- The DKG cannot be made publicly available nor redistributed (e.g., in the form of data dumps), and it must not be openly queryable by exposing and making available to the public an unconstrained SPARQL endpoint[5]. Direct access to the DKG via SPARQL must thus be constrained by introducing an authentication and authorisation layer, limiting the management and provision of credentials/accounts and permissions within the boundaries of the Consortium. Disposable and temporary accounts may be created for reviewers if and when needed.
- No constraints or limitations are needed when the access to the DKG is mediated by the HACID decision support system (DSS). Users of the HACID DSS will not be provided with the possibility to directly query the DKG and freely formulate queries. The kind and amount of data that the user will be able to access will be under the

[3] https://www.snomed.org/_files/ugd/900274_689013e9e0c74d23892abe9caee02612.pdf

[4] The Affiliate Licence states that (2.2.) "The Licensee may only use the International Release, and must ensure that its officers, employees, agents and contractors only use the International Release:" (2.2.4) "in the Licensee's systems (including browsers and data analysis systems) made available to the **general public for accessing and/or retrieving any part of the International Release and/or data encoded using the foregoing, provided that users of those systems are not able to extract any substantial portion of SNOMED CT** (...)

[5] A SPARQL endpoint is the software service that allows humans and other software services to query and retrieve the data stored as RDF triples (basically, a knowledge graph) in a triplestore.

control of the application, which will internally rely on predefined and rate-limited queries. The fact that data consumption will primarily go through web-based dashboards, UI widgets and other data presentation and visualisation means that users will not be able *to extract any substantial portion of SNOMED CT*.

- Tools that we deploy to allow users browsing and exploring the DKG—such as the LodView[6] and LodLive[7] Linked Data browsers, as well as any knowledge graph exploration tool that is built in the project—can be used and made publicly available, provided that any feature for extracting or downloading data (e.g., access to the SPARQL endpoint or ability to produce data dumps) is properly constrained and rate-limited to meet the licence requirements.
- The ontology itself only relies on and encodes a limited number of concepts from SNOMED CT, as in our approach the bulk of SNOMED's terminological content is represented in the linked data layer that instantiates the ontology. The ontology thus qualifies as a standalone artefact that can be published and made available unconstrained from the terms of the SNOMED CT Affiliate Licence.
- As a consequence of the previous point, the tools that we deploy to allow users to browse and visualise the ontology, such as Lode[8] and WebVOWL[9], can be used as well, for the purpose of documenting the ontology and making it understandable to interested users.

Complementary to the previous points, SNOMED International offers access to SNOMED CT "through a variety of flexible membership, licensing and fee exemption options"[10] Thus, any individual or organisation with access to SNOMED CT can fully recreate the DKG using our scripts documented in a dedicated GitHub repository[11]. Furthermore, in line with points above, we will consider implementing a closed access demo and/or a small-scale public demo[12] of the DKG for interested individuals and organisations.

3. Amendment 2: Joint Controller Agreement and the handling of personal data

The Joint Controller Agreement (JCA) states its purpose in §2.1 as:

This Agreement regulates mutual relations between the Parties as regards the joint control of Personal Data, and in particular it determines in a transparent manner the Joint Controllers' responsibilities for compliance with the obligations under the GDPR; it also defines the representation of the Joint Controllers in contacts with the data subjects and their relations with those data subjects.

---

[6] https://github.com/LodLive/LodView
[7] https://github.com/LodLive/LodLive
[8] https://essepuntato.it/lode/
[9] https://github.com/VisualDataWeb/WebVOWL
[10] https://www.snomed.org/get-snomed
[11] https://github.com/hacid-project/knowledge-graph
[12] i.e., only covering a subset of SNOMED CT, thus fulfilling the requirements in the Affiliate License's section 2.2.4 by ensuring that public users "are not able to extract any substantial portion of SNOMED CT".

The JCA's sections most relevant for the data management plan are: controllers' rights and obligations (§3), data subjects' rights (§4), transfers of personal data to/from third countries (§5), and entrusting processors with processing of personal data (§6). Please refer to the Annex for the agreed text of the JCA.

4. Amendment 3: Handling of personal data in the medical diagnostics case study

Some surveys related to the activities in the medical diagnostics case study are carried out using the survey platform Qualtrics.[13] The data that we collect are already anonymized by Qualtrics, and, thus, we never handle any personal data of our respondents. More generally Qualtrics' operations are GDPR compliant[14] and Qualtrics confirmed in writing that the data from MPG-MPIB organisation and the corresponding account are stored solely in their European servers.

[13] https://www.qualtrics.com/
[14] https://www.qualtrics.com/support/survey-platform/getting-started/qualtrics-gdpr-compliance/

Joint Controller Agreement

Hybrid Human Artificial Collective Intelligence for Decision Support in Open-Ended Domains

HACID

Joint Controller Agreement

THIS JOINT CONTROLLER AGREEMENT is made on March the 20th, 2024 hereinafter referred to as the 'Effective Date' between:

- CONSIGLIO NAZIONALE DELLE RICERCHE (**CNR**)**,** established in PIAZZALE ALDO MORO 7, ROMA 00185, Italy, hereafter also referred to as "Coordinator"

- MAX-PLANCK-GESELLSCHAFT ZUR FORDERUNG DER WISSENSCHAFTEN EV (**MPG**), established in HOFGARTENSTRASSE 8, MUNCHEN 80539, Germany,

- HUMAN DX EU, LTD (**Human Dx EU**), established in 3RD FLOOR KILMORE HOUSE PARK LANE SPENCER DOCK, DUBLIN D01 YE64, Ireland,

- **NESTA**, established in 58 Victoria Embankment, London EC4Y 0DS, United Kingdom

- MET OFFICE, for and on behalf of the SECRETARY OF STATE FOR SCIENCE, INNOVATION AND TECHNOLOGY OF THE UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND, whose principal place of business is at FitzRoy Road, Exeter, EX1 3PB, United Kingdom

hereinafter, jointly or individually, referred to as "Controllers" or "Joint Controllers" or "Parties" relating to the project entitled:

Hybrid Human Artificial Collective Intelligence in Open-Ended Domains (in short, **HACID**)

hereinafter referred to as "Project"

Whereas:

A. pursuant to the Consortium Agreement of January the 25th 2023, (hereinafter referred to as the "Consortium Agreement") and the Grant Agreement n. 101070588 of June the 3rd 2022, signed between the European Commission and the HACID consortium, the Joint Controllers have entered into cooperation, the subject of which is to perform additional activities within a consortium of executive agencies (hereinafter referred to as the "Cooperation");

B. the Cooperation requires that the Joint Controllers process personal data, whilst they jointly determine the purposes and means of processing of personal data;

C. the processing of personal data by the Joint Controllers requires that a transparent manner of determining their respective responsibilities be established as regards their compliance with the obligations under the 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 (hereinafter referred to as "General Data Protection Regulation" or "the GDPR"[1]) and other generally applicable laws including the UK GDPR and Data Protection Act 2018 as well as relations between the Joint Controllers and the data subjects;

D. on concluding this Agreement, the Parties, seek to regulate the terms of processing of personal data in such a way that they meet the provisions of the GDPR, and

[1] https://eur-lex.europa.eu/eli/reg/2016/679/oj

E. with regard to the data they process, the Joint Controllers act as controllers for the purposes of Article 24 et seq. of the GDPR,

the Parties decided to enter into the following Agreement:

§ 1.

Definitions

For the purposes of this Agreement, the Parties agree that the following terms shall have the following meaning:

1. **"Controller/Joint Controller"** means any 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 as defined within the GDPR;
2. **"Personal Data"** means any information relating to an identified or identifiable natural person (hereinafter referred to as "data subject") as defined within the GDPR;
3. **"Third Country"** means any country that is not a member of the European Union or the European Economic Area or any international organisation for which the European Commission has not confirmed a suitable level of data protection on the basis of an adequacy decision.;
4. **"Processor"** means any natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Controller as defined within the GDPR;
5. **"Data Protection Law"** means the GDPR and relevant EU GDPR adequacy decisions as well as other provisions of EU Member States' (or the UK's) national law applicable to a relevant Party, passed in relation to personal data protection, including including the UK GDPR and Data Protection Act 2018 and the provisions of the given Party's national law;
6. **"Processing**" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction as defined within the GDPR;
7. **"General Data Protection Regulation"**, **"GDPR"** means the 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 and includes reference to the UK GDPR, which has the meaning given to it in section 3(1) as supplemented by section 205(4) of the Data Protection Act 2018; wherever this Agreement refers to specific Articles of GDPR, it shall also apply to the corresponding provisions in national legislation guaranteeing a similar level of safety;
8. **"Information System"** means a group of cooperating devices, programs, information processing procedures and program tools used for the purpose of data processing;
9. **"Cooperation"** means the cooperation between Joint Controllers defined in Recital A;
10. **"Agreement"** means this Agreement relating to the Processing of Personal Data;
11. **"Consortium Agreement"** means the agreement referred to in Recital A

§ 2.

Subject-matter of the Agreement

1. This Agreement regulates mutual relations between the Parties as regards the joint control of Personal Data, and in particular it determines in a transparent manner the Joint Controllers' responsibilities for compliance with the obligations under the GDPR; it also defines the representation of the Joint Controllers.
2. For the purpose of proper implementation of this Agreement, the Joint Controllers shall:
   a) cooperate on performing the obligations of the Joint Controllers of Personal Data;
   b) process the Personal Data with which they have been entrusted with regard to the Cooperation pursuant to this Agreement, GDPR, Consortium Agreement and
   c) refrain from any actions which might in any way undermine the security of Personal Data or threaten the other Joint Controllers with civil, administrative or criminal liability.
3. Categories of data subjects and Personal Data, the purposes and means of Processing, including the participation of Joint Controllers in those processes, is be defined in Appendix 1 to this Agreement.

§ 3.

Joint Controllers' rights and obligations

1. The Joint Controllers declare that they have the means enabling them to process and protect Personal Data they are processing, including information systems meeting the requirements of the appropriate level of security, as stipulated by the GDPR. They will each fully adhere to the applicable Data Protection Law(s) with respect their obligations and responsibilities.
2. In particular, the Joint Controllers shall:
   a) exercise due diligence in processing Personal Data and process Personal Data pursuant to the Agreement, the GDPR and other provisions of Data Protection Law(s), including the appropriate provisions of each Party's national law;
   b) restrict access to Personal Data only to persons who need the access to Personal Data for the purposes of the Agreement and Cooperation, provide those persons with relevant authorisations, offer relevant training on processing Personal Data and ensure confidentiality of Personal Data processed thereby, both during and after their employment or other cooperation with a Joint Controller;
   c) assist the other Joint Controllers, where possible, in meeting its (i) obligation to respond to requests from data subjects and (ii) obligations laid down in Articles 32 through 36 of the GDPR;
3. The Joint Controllers shall provide each other with the necessary assistance in carrying out the obligations referred to in section 2 point 3) above, in particular in the notification of a personal data breach, by:

a) ensuring that any necessary notification to the supervisory authority is conducted without delay. The party in whose responsibility the personal data breach occurred shall be responsible for any necessary notification to the supervisory authority.

b) providing, at the request of the other Joint Controller(s), information concerning the Processing of Personal Data immediately upon receipt of such request as soon as reasonably possible;

c) notifying the other Joint Controller(s) of any breach as soon as possible but in any event no later than 48 hours of its discovery. The notification should include all the information referred to in Article 33 (3) of the GDPR. If - and to the extent that - the information cannot be provided at that time, it will be provided without undue delay;

d) providing to the other Joint Controllers all information necessary for the communication of a personal data breach to the data subject;

e) informing the other Joint Controllers of inquiries, requests or demands from data subjects and other individuals, national or European Union public administrations, including relevant supervisory authorities and courts, as well as any controls or inspections by such authorities in connection with the Processing of Personal Data in respect of this Agreement; information shall be provided promptly and in such a way as to enable the other Joint Controllers to comply with their obligations set out in sections 2 and 3, without undue delay but not later than 7 calendar days after receipt of an inquiry, request or demand or after the start of a control or inspection.

§ 4.

Data subjects' rights

1. The Joint Controllers shall inform, in any way they deem appropriate, the data subjects of the essences of this Agreement and shall provide them the information referred to in Appendices 1 and 2 in accordance with Article 26 and Article 12 of the GDPR.
2. The information referred to in section 1 shall be primarily provided to the data subjects by the Party who collects the personal data.
3. Data subjects may contact any of the Joint Controllers about the rights granted to them by Articles 15 - 22 of the GDPR. The contacted Controller shall identify the responsible Controller and forward the request internally to this Controller. The originally contacted Controller shall carry out all necessary communication with the data subject.
4. The responsible Controller shall be determined as follows: If the data of the data subject is part of a set of data which can be attributed to an individual Controller, this Controller shall be responsible for actioning the request. In all other cases the Controller contacted by the data subject shall be the responsible Controller.
5. The Joint Controllers agree to comply with the data subjects' rights and shall assist one another with the execution of data subjects' requests.

§ 5.

Transfers of Personal Data to/from third countries

Data Controllers will not transfer any personal data collected within the scope of the project to/from third countries in the scope of the Agreement, exception made for data transfers to/from the UK among the Data Controllers involved in this Agreement.

Personal data will remain in the exclusive possession of the Data Controller that collected them. All data transferred among Data Controllers (including data transfers to/from UK-based Data Controllers) will be anonymised (or at least pseudonymised) and encrypted.

§ 6.

Entrusting Processors with processing of Personal Data

1. The Joint Controllers consent to each of them entrusting Processors with processing of Personal Data subject to this Agreement on terms and to the degree defined by this Agreement and Article 28 of the GDPR.
2. Each Controller may entrust Processors with Processing of Personal Data under this Agreement only for the purposes of this Agreement, Consortium Agreement and the Cooperation.
3. Processors may only carry out specific Personal Data processing activities on behalf of a Controller once the Controller has entered into a contract with such a Processor detailing the obligations of the latter related to the Processing of Personal Data in a manner ensuring sufficient guarantees of technical and organisational measures for the Processing to meet the requirements of the GDPR.
4. A Processor may carry out specific Personal Data processing activities on behalf of a Controller without entering into the contract referred to in section 3 as long as it is possible pursuant to another legal instrument under EU law or national law, which binds the Processor and the Controller.
5. This Paragraph shall apply in the case of any intended modifications regarding adding processors or replacing processors with other processors.
6. Categories of processors are listed in Appendix 1. The Joint Controller shall provide detailed information on its Processors on request to the data subject

§ 7.

Controllers' liability

The liability of the Parties is governed by Article 82 of the GDPR with regard to the processing activities as defined in Appendix 1.

Each Party's liability to the other Parties collectively is detailed within clause 5 of the Consortium Agreement dated 25 January 2023.

§ 8.

Collaboration of the Parties

1. The Parties shall cooperate in supervising the implementation of this Agreement.
2. The Parties agree that at the time of the implementation of this Agreement they shall cooperate closely, informing other Parties of any circumstances that have or may affect the Processing of Personal Data. Each Party designates a contact point to coordinate the collaboration of the Parties in connection with the implementation of the Agreement, disclosing their personal data in the privacy notice.
3. Amendments to Appendix 1 shall not require an amendment of the Agreement, however all Parties shall have to be notified thereof either in writing or electronically by the Coordinator.

§ 9.

Term and termination of the Agreement

The Agreement will take effect as of the Effective Date.

The Agreement shall be concluded for the period of implementation of the Cooperation and as long as and until, after the termination of the Cooperation, obligations still have to be fulfilled.

§ 10.

Final provisions

1. The Parties hereby agree that the Joint Controllers shall process Personal Data pursuant to this Agreement free of charge, and neither the conclusion of this Agreement nor the Processing of Personal Data pursuant thereto shall entitle any Party to seek, on whatever legal basis,
   a) remuneration,
   b) reimbursement of any costs or expenses incurred for the purpose of due performance of the Agreement,
   c) exemption from any obligations contracted to that end or advances on such costs or expenses,

   even if at the time of entering into Cooperation or concluding this Agreement, despite exercising due care, the party was unable to foresee the circumstances justifying such rises, costs, expenses or obligations.
2. Should any provision hereof become invalid or ineffective, the Parties shall adopt all measures possible to replace it with a valid and effective provision reflecting the goal and meaning of the invalid or ineffective provision to the extent of applicable law. Should any provision hereof be or become invalid or ineffective at any time, it shall not restrict the validity or effectiveness of the remaining provisions of the Agreement.
3. In the event of any discrepancies between the provisions of the Agreement and the terms of Cooperation, the provisions of this Agreement shall prevail.

4. Any amendments hereto must be in writing on sanction of invalidity, subject to § 8 (3).
5. In the event of any inconsistency between the General Data Protection Regulation and the UK GDPR, the requirements of the General Data Protection Regulation shall prevail.
6. Any disputes arising under the Agreement shall be resolved by amicably or by a common court with jurisdiction over the registered office of the Controller sued and pursuant to the laws applicable in its country, in accordance to the terms of the Cooperation.

This Agreement has been drawn up in 5 counterparts, one counterpart for each Party.

Signatures of the Parties (in the case of a multilateral agreement, each Party on a separate page):

HACID

CONSIGLIO NAZIONALE DELLE RICERCHE

Signature(s)

Rosario Falcone

Director of the Institute of Cognitive Sciences and Technologies

Date

HACID

Appendix 1: Essential elements of the means

Categories of data subjects	Categories of personal data	Purpose of processing	Means of processing	Who is responsible for data collection and processing?	Recipients / Categories of recipients	Categories of processors
Climate Science Experts and other relevant Specialists	● Name ● Age ● Gender ● Institution ● Professional role ● Seniority ● E-mail	The main goal of the HACID project is to provide decision support to professionals relying on a hybrid collective intelligence. Users of an online platform can submit cases to be solved, and provide solutions to cases. These data are aggregated by an automated system to produce a collective solution.	● Data collection: ○ Users register to an online platform hosted by CNR providing personal data subject to informed consent, under the responsibility of CNR. ○ Upon registration, a unique user identifier is generated that is later used for pseudonymisation ○ Transcription is performed automatically through the platform, assigning unique identifiers to users and institutions. ● Data storage: ○ Data will be stored in a secure system accessible only by authorised persons, that is, CNRBox hosted by CNR. Data will be encrypted before storage ○ Data will be stored for the whole duration of the HACID project (plus 5 years from data collection).	Responsible for data collection and pseudonymization, storage and transfer: ● CNR Responsible of pseudonymized data analysis: ● CNR ● MPG ● Nesta ● Met Office	No data recipients outside the Joint controllers	No data processors

			After this period, personal data will be erased. ● Data transfer: ○ Data subject to transfer will only consists in a user identification number, institution identification number and professional role level ○ Data will be encrypted before being transferred to any other partner ○ Data will be transferred via secure means by CNR through the GARR Filesender ● Data analysis: ○ Data will be analysed in anonymized, pseudonymised and/or aggregate form ○ Data in anonymized, pseudonymised and/or aggregated form will be used for scientific publications and/or presentations at scientific conferences.			
Climate Science Experts and other relevant specialists	● Audio-visual recordings of interviews and transcripts ● Name ● Age ● Gender ● Institution ● Professional role	The HACID system will be developed and evaluated using participatory methods. This will necessitate collecting personally identifiable data about stakeholders during design research and evaluation activities.	● Data collection ○ All participants will review the conditions of data collection and sign a consent form for collection and storage of personal data prior to participation in relevant activities, under the responsibility of Nesta. ● Data storage:	Responsible for data collection, analysis and storage: Nesta	No data recipients	Google Drive for data storage

	• Seniority		○ Data will be encrypted and stored in a secure system accessible only by the Nesta research team: An encrypted Google Drive with restricted access. All data is stored in Google's European data centres. ○ Data will be stored for the whole duration of the HACID project (plus 5 years from data collection). After this period, personal data will be erased. • Data transfer: no personal data will be transferred • Data analysis: data in anonymized and/or aggregated form will be used for publications and/or presentations at events/workshops/conferences.			
Medical experts enrolled on the Human Dx platform	• Medical specialty • Seniority • Date in which they joined the Human Dx platform • Affiliated institution • Country of affiliated institution • Timestamp of interactions	The main goal of the HACID project is to provide decision support to professionals relying on a hybrid collective intelligence. Users of an online platform hosted by Human Dx can submit cases to be solved, and provide solutions to cases.	• Data collection ○ Data is collected through the Human Dx platform, under the responsibility of Human Dx EU. Only data strictly related to the requested cases is sent. The fields "Affiliated institution" and "Country of affiliated institution", as well as the unique ID of the users, are pseudonymized before being shared. ○ Personal data from users is collected by Human Dx when the users create an account on the	Responsible for data collection and pseudonymization: Human Dx EU Responsible for storage and transfer: CNR Responsible of pseudonymized data analysis: • CNR • MPG	No data recipients outside the Joint controllers	No data processors

	with the system	The purpose of the data processing is to provide real-world data for experiments on how to best aggregate users' suggestions into collective solutions. Medical cases are either fictitious or completely anonymised, and are provided to the Human Dx platform mainly for training and research purposes.	platform or edit their information. Informed consent is requested under the responsibility of Human Dx. ● Data Storage: ○ Data will be stored for the whole duration of the HACID project (plus 5 years from data collection) by CNR with CNRBox, after encryption. ● Data Transfer: The pseudonymised data will be transferred in encrypted form via secure means by CNR through the GARR Filesender. ● Analysis: ○ Data will be analysed in anonymized, pseudonymised and/or aggregate form ○ Data in anonymized, pseudonymised and/or aggregated form will be used for scientific publications and/or presentations at scientific conferences.	● Nesta ● Human Dx Eu		