HUMAN TECHNOPOLE NATIONAL FACILITIES ACCESS AGREEMENT

Access regulated by Convenzione

Template

Table of Contents

This Access Agreement (the "Agreement") is made effective as the date of last signature of the Agreement (the "Effective Date") by and between

(1) GIACOMO PIETRO COMI, FONDAZIONE IRCSS CA'GRANDA, via Francesco Sforza 35, hereinafter referred to as "the Principal Investigator"

(2) FONDAZIONE IRCSS CA'GRANDA-Policlinico Maggiore, hereinafter referred to as "the Institution"

(3) Fondazione Human Technopole, Viale Rita Levi-Montalcini 1, 20157 Milano, Italy, hereinafter referred to as "HT"

each a "Party" and collectively "the Parties".

Recitals

(A) WHEREAS, the "Principal Investigator" is the Researcher affiliated to an eligible Institution who is responsible for coordinating the research activities conducted within the framework of the project ID1998517, Decoding Disease Heterogeneity in Becker Muscular Dystrophy: a Multi-Spatial-Omics Analysis for Therapeutic Target Discovery and Patient Stratification submitted to the call for Access 24-G-Pilot to the National Facility for GENOMICS.

(B) WHEREAS, the submitted project [ID1998517, Decoding Disease Heterogeneity in Becker Muscular Dystrophy: a Multi-Spatial-Omics Analysis for Therapeutic Target Discovery and Patient Stratification] available in Annex I of this Agreement has been approved for Access on [17/04/2025].

(C) WHEREAS, HT is engaged in providing Services as specified in the Project Plan agreed upon by the Parties (Annex II);

(D) WHEREAS, the "Principal Investigator" wishes to receive the Services provided by HT in connection with the performance of apply this advanced technology to muscle biopsy of BMD patients and control subjects enabling high-resolution spatial mapping of gene expression changes

NOW, THEREFORE, the parties agree as follows:

1. DEFINITIONS

1.1 Access

"Access" refers to the authorized [REMOTE] use of the National Facility (NF) and of the services offered. Such Access can be granted for sample preparation, set-up, execution and dismantling of experiments, education and training, expert support and analytical services, among others. Access to the NFs includes all infrastructural, logistical, technical and scientific support (including training) that is necessary to perform the part(s) of the project approved for Access.

1.2 Confidential information

Confidential information means all Data, knowledge and information, including but not limited to any Background Intellectual Property disclosed by one Party to the others for use in the Project and identified as confidential before or at the time of disclosure and any Arising Intellectual Property owned by that Party.

1.3 Principal Investigator and Principal Investigator Institution

“Principal Investigator” (PI) is the Researcher affiliated to an eligible Institution with the role of independent Group Leader, who submitted a project as Applicant to the call for Access [24-G-Pilot] to the NF for [GENOMICS]

DATA HANDLING AND ANALYSIS] published by HT and whose project has been approved for Access (see Annex I). They are responsible for coordinating the research activities conducted within the framework of the approved project.

"PI Institution" means the Institution to which the PI is affiliated.

1.4 Input Material and Input Data

Input Material and Input Data mean respectively any and all materials and Data to be transferred by the PI to be analyzed and/ or processed on their behalf within the NF for [GENOMICS] as part of the Access. The complete list of Input Material and Input Data to be transferred is reported in Annex III of this agreement.

1.5 Intellectual property

Intellectual Property means trade-marks, service marks, certification marks, official marks, trade names, trade dress, distinguishing guises and other distinguishing features used in association with wares or services, whether or not registered or the subject of an application for registration and whether or not registrable, and associated goodwill; inventions, processes, articles of manufacture, compositions of matter, business methods, formulae, developments and improvements, whether or not patented or the subject of an application for patent and whether or not patentable, methods and processes for making any of them, and related documentation (whether in written or electronic form) and know-how; software in source code or object code form, documentation, literary works, artistic works, pictorial works, graphic works, musical works, dramatic works, audio visual works, performances, sound recordings and signals, including their content, and any compilations of any of them, whether or not registered or the subject of an application for registration and whether or not registrable; domain names, whether registered primary domain names or secondary or other higher level domain names; industrial designs and all variants of industrial designs, whether or not registered or the subject of an application for registration and whether or not registrable; and trade secrets, technical expertise, and Research Data and other confidential information. Background Intellectual Property means any and all Intellectual Property conceived, developed, reduced to practice or otherwise made or acquired by HT and/or the PI or the User before the Access and that was not developed or conceived during the Access. Foreground Intellectual Property means any and all Intellectual Property that is conceived, developed, reduced to practice or otherwise made by HT personnel during the Access as part of the service, including improvements and enhancements to Background Intellectual Property.

1.6 Output Material and Output Data

Output Material and Output Data mean respectively any material or Data generated by the NF for [GENOMICS] from the analysis of PI's Input Material or Input Data.

1.7 Service

Service includes activities as described in the PI's project approved for Access (see Annex I) and detailed in the Project Plan agreed upon by the Parties (Annex II, the "Project").

1.8 User

A "User" is intended as a Researcher affiliated with an eligible Institution who accesses the NFs to perform the approved activities or to support the NF staff while performing the approved service.

User can be the PI or a separate member of their research team.

2. TRANSFER OF MATERIAL/ DATA AND PRINCIPAL INVESTIGATOR'S OBLIGATIONS

The Input Material is temporarily transferred from the PI Institution to HT for the sole execution of the approved Access and remains property of the PI Institution . At the end of the Access, the Input Material not consumed by analysis will be [RETURNED to the PI Institution, as agreed upon during the Access]. When applicable, unused Input Material will be returned within 30 days after the delivery of the Output Material or Output Data.

[TO BE INCLUDED ONLY WHEN APPLICABLE ONLY FOR SB-IU2] When the service includes processing of input material, the processed material (output material) is property of the PI and will be returned to the PI in the timeframe and condition specified in the Project Plan. Notwithstanding the foregoing, any material added to the input material for the purpose of expressing proteins of interest within the services of the Infrastructural Unit Biomass Production ("added material") shall be processed solely for the purification phase and then destroyed and disposed of; any further use of said added material is forbidden.

The Input Data is temporarily made available by the PI to HT for the execution of the approved Access and remains property of the PI.

HT activities are among others guided by the Convention on Biological Diversity (CBD) (www.cbd.int) and the Nagoya Protocol on Access to Genetic Resources and the Fair and Equitable Sharing of Benefits Arising from their Utilization (ABS) (www.cbd.int/abs/), as applicable. Materials are transferred to HT on the condition that PI agrees to use material and Data in compliance with international laws and conventions.

2.1 Pseudonymization / anonymisation

Any Input Material and Input Data of human origin, including but not limited to DNA, RNA, blood, tissue, saliva, stool, must be provided by the PI Institution in pseudonymous form. This means that all identifiers other than the pseudonym must be removed and not available to HT personnel (this may include, but it is not limited to, name, surname, date of birth, fiscal code, *etc*.). Means of transmission include, but are not limited to mail, Sample list, shipped envelopes or direct labeling of tubes. HT shall process any personal Data contained within any Input Material and Input Data acting as Processor under applicable Data protection legislation (art. 28, Regulation (EU) 2016/679), as per the relevant Data Processing Agreement (DPA) entered into with PI Institution (Annex IV, in this agreement applicable/ NOT applicable). Data which might be used for the sole scope of the analysis (*e.g.,* age, weight, prognosis, sex, drug treatment, *etc.*) can be submitted through the Sample list without limitations.

2.2 Biosafety level

HT will not accept any Input Material containing pathogenic agent above [BSL-2].

If human Input Material is provided in the form of tissue or body fluid, the PI shall provide a signed declaration that "The Input Material does not contain any pathogenic agent (viral, bacterial, fungal, prionic)" OR "It is not known whether the Input Material may contain pathogenic agents" OR "It is known that the Input Material contains pathogenic agents (specify)"

2.3 Authorizations to use

The PI Institution warrants the absence of any third-party rights in the Input Material or Input Data that would preclude it from providing it to HT in accordance with this agreement.

The PI shall comply with the confidentiality requirements and should adhere to the code of conduct and standard ethical behaviour in scientific research when conducting research, and using and disseminating Research Data and findings, as detailed in the European Code of Conduct for Research Integrity of the European Science Foundation (link)

The PI shall confirm that all relevant authorizations, declarations and accreditation from the competent authorities have been obtained in order to process the submitted Input Material or Input Data and to perform the proposed activity, in full compliance with the applicable EU and National laws.

If applicable, PI shall confirm that legal requirements for exporting/importing materials to/from other countries have been met.

2.4 Research only restriction

The PI Institution warrants that the Access requested, and the use of the Input Material and Input Data is for research purposes only. The PI and the PI's Institution must not use the Output Material and Output Data as part of any clinical or diagnostic or other non-research related purposed.

HT shall not be responsible for the scientific results and publications that are further obtained by the PI based on the Output Material and/or Output Data resulting from the Access once said Output Material and Output Data have been delivered by HT to the PI or the User upon completion of the Access.

2.5 Input Material technical requirements

The PI shall provide the Input Material in the quantity and quality required for the Access as described in the call for Access [24-G-Pilot] and as reported in Annex II.

HT personnel will perform a quality check of the Input Material before starting the analysis. In case of any non-compliant Input Material, the NF will contact the PI who can decide how to proceed with the non-compliant Input Material.

Shall the PI fail to comply with any of the obligations included in the present agreement and in particular in Paragraph 2, HT may refuse to perform the Service.

3. COVERAGE OF ACCESS COSTS

Access to the NFs is supported by the Ministry of Health, Ministry of University and Research and Ministry of Economy and Finance. Law 160/2019, art. 1, comma 276, letter b foresees that Access of external PIs affiliated with Italian Universities, *Istituti di Ricovero e Cura a Carattere Scientifico* (IRCCS), and Public Research Entities is supported by open calls for Access, and is free of charge for the PI, for the project (or part of the project) approved for Access (Annex I) and described in the Project Plan (Annex II). If any further service is requested by the PI, a fee is applied.

The costs for the activities to be performed at the NFs will be fully covered, including shipment of relevant material from and to the PI's laboratory as well as travel and accommodation for the User while accessing the NF. Project-related costs (personnel, consumables, and other costs) at the PI laboratory are not covered by the funding of the project.

4. DATA MANAGEMENT, DELIVERY AND STORAGE

When applicable (for this agreement applicable) PI and NF staff agree on a Data Management Plan (DMP) included in the Project Plan, regulating how Research Data of the project are handled. Data Management shall refer to HT Research Data Management Guidelines (link) and shall be in line with the FAIR principles that aim at making Research Data findable, accessible, interoperable and re-usable. The DMP includes information on:

- the handling of Input and Output Data during and after the end of the project,
- what Input Data are collected, processed and/or what Output Data are generated,
- which methodology & standards are applied,
- whether Output Data are shared/made Open Access and
- how Output Data are curated & preserved (including after the end of the project).

During the course of the project, the NF may make available intermediate datasets of the Output Data to the PI by uploading them to the HT Fast Data Exchange (FDE). During the project, the NF may make available intermediate datasets of the Output Data to the PI by uploading them to the HT FDE. The PI shall download the dataset within 30 calendar days from receipt of the notification of availability, using one of the download methods offered by the system. At the end of the 30-day period, the intermediate datasets may be removed from the HT FDE at the discretion of the NF.

When all activities specified in the Project Plan are completed (End of Access – EOA), all Output Data related to the project (raw data, processed data, analysis reports) will be made available to the PI on the HT FDE, and the PI will receive a notification of availability of the data. The PI must download the full dataset within 30 calendar days from EOA. After this date, the Output data will be available for download upon payment of a fee for late download. After this period, Output Data will be deleted without notification.

Should extra time be required for downloading because of technical issues on the PI's side, the PI may request extended retention of the Output Data. This request must be placed in writing within 30 calendar days of EOA. The Output Data will be stored on HT storage for the requested length of time (not greater than 180 calendar days). When the PI is ready to receive the Output Data, it will be made available on the HT FDE for download for a period of 30 calendar days. After this period, Output Data will be deleted without notification.

HT reserves the right to archive data when there are legal justifications.

The NF-DATA staff is available to assist the PI with downloading the data throughout the duration of the Access.

5. CONFIDENTIALITY AND PRIVACY POLICY

All PI and User information is held with strict confidentiality. All materials and information sent to HT and the Data produced by HT for the PI's project are exclusive property of the PI and will be returned to the PI or discarded in confidential manner. For HT's privacy policy, please retrieve the latest document available at the following link.

6. INTELLECTUAL PROPERTY RIGHTS

Unless a dedicated collaboration agreement provides otherwise, all Intellectual Property Rights (IPR) deriving from the activities within the scope of the Project, including those consisting in the execution of the Service, shall belong to the PI's Institution,

All IPR that are developed by HT while carrying out the Service but beyond the scope of the Project shall solely belong to HT. Shall the PI and/ or the User contribute to the latter, the related IPR shall be shared between HT and the PI Institution on the basis of PI/ User's actual contribution.

7. ACKNOWLEDGEMENT AND CO-AUTHORSHIP

By signing this agreement, the PI and the PI Institution agree to acknowledge HT as the Access provider in any publications or presentations of the Data and results provided by the NF, using the following statement "*We acknowledge the Access and services provided by the National Facility for GENOMICS, Fondazione Human Technopole, Milan, Italy"; Call for Access (*24-G-Pilot*), Project ID1998517".*

Moreover, in scientific publications the statement "[Whole-transcriptome spatial gene expression analysis] was performed at the National Facility for [GENOMICS], Fondazione Human Technopole, Milan, Italy" shall be indicated in the materials and methods section of the publication.

When NF staff critically contributes to the PI's project while performing the service requested, providing intellectual and technical contribution beyond the application of established protocols and methods, co-authorship shall be discussed. Activities for which authorship is recommended are: design of project that includes critical input and/or original ideas (e.g., providing guidance for experimental design, solving technical problems, developing technology/ methods that make the project feasible); Data acquisition, analysis and/or interpretation beyond routine practices; critical drafting and/or revision of manuscript for intellectual content purposes.

8. ACCESS REPORT, FEEDBACK FORM AND SCIENTIFIC OUTPUT

At the end of the activities carried out at the NF, and not later than 3 months thereafter unless agreed otherwise with the NF User Access Office, the PI must submit (via email to national.facilities@fht.org) a short report on the results obtained and the impact of the service on their research, to be published on the NF website as required by the *Convenzione Art 6, comma 5.*

Moreover, the PI will be required to fill in a brief survey regarding their experience, providing feedback and suggestions for further service improvement.

The PI must communicate to the NF User Access Office (via email to national.facilities@fht.org) any publication acknowledging the NFs.

Research Data obtained during the Access shall be made available to the scientific community following the FAIR principles. PI must inform the NF Users Access Office (via email to national.facilities@fht.org) when and how the Data are made public.

9. LIMITATION OF LIABILITY

HT does not guarantee:

- the suitability, with respect to the research purposes of the PI, of its premises, equipment and personnel;

- the accuracy of the services provided by the NFs, nor that such services are free from errors or omissions.

HT shall be liable to the PI and to the PI Institution for any losses, liabilities, damages, costs or expenses arising out of inadequacy or malfunctioning of its laboratories or arising out of delays or negligence in the provision of the services.

10. REPRESENTATIONS AND WARRANTIES

The PI and the PI Institution represent and declare that the relevant research project has received full ethical clearance and that all biological samples and personal Data involved have been collected in accordance with applicable laws and regulations. In this regard, the PI and the PI Institution expressly undertake to indemnify and hold harmless HT, its regents, officers, agents and employees from any liability, loss or damage HT may suffer as a result of claims, demands, costs or judgments arising due to the breach of ethical protocols, privacy laws or biosafety regulations.

The PI and the PI Institution also expressly undertake to indemnify and hold harmless HT in connection with any loss or damage, direct or indirect, HT may suffer as a consequence of the PI or the User or the PI Institution's own negligence or failure to comply with the instructions given, time by time, by HT's HSE Area or by NF staff.

11. GOVERNING LAW AND COURT OF EXCLUSIVE JURISDICTION

This Agreement is governed by and shall be construed in accordance with the law of Italy.

The Court of Milan shall have exclusive jurisdiction to deal with any disputes which may arise out of or in connection with the present Agreement.

12. REGISTRATION

This Agreement shall be registered only in the event of use. All expenses relating to its potential registration will be exclusively borne by the Party requesting registration. The costs eventually incurred for the payment of the stamp duty shall by borne by HT by telematic stamps:

- num. XXXXX
- num. XXXXX'
- num. XXXXX'

13. NATIONAL FACILITY ACCESS RULES

For any aspect not covered by this agreement, the Parties shall refer to the NF Access rules (link).

IN WITNESS WHEREOF this Agreement is executed as follows:

for and on behalf of [FONDAZIONE IRCSS CA'GRANDA-Policlinico Maggiore]	for and on behalf of Fondazione Human Technopole
Signed: _____	Signed: _____
Name: Flavio Blandini	Name: Marino Zerial
Title: Scientific Director	Title: Director
Dated: _____	Dated: _____

For acceptance of the terms [GIACOMO PIETRO COMI]

Signed: _____

Name: Giacomo Pietro Comi

Title: Full professor

Dated: _____

Annex I Proposal approved for Access (ID1998517)

Annex II Project Plan (ID1998517)

Annex III List of Material/ Data to be transferred

Annex IV Data Processing Agreement Template

DATA PROCESSING AGREEMENT

pursuant to art. 28, GDPR

[FONDAZIONE IRCSS CA'GRANDA-Policlinico Maggiore**]**, tax code [04724150968], with its registered office in [via Francesco Sforza 28, 20122, Milan], hereby represented as indicated in the signature page below (hereinafter referred to also as "**PI'S Institution**" or the "**Controller**")

and

Fondazione Human Technopole, tax code 97821360159, with its registered office in Palazzo Italia, Viale Rita Levi-Montalcini n. 1, Milan, hereby represented as indicated in the signature page below (hereinafter referred to also as "**HT**" or the "**Processor**")

hereinafter referred to individually as "Party" and jointly as "Parties".

RECITALS

a) On [the same date as this agreement] ("Data Processing Agreement" or "DPA"), the PI'S Institution and HT entered into an agreement ("National Facilities Access Agreement" or "Access Agreement") regarding access to certain HT's facilities and/or services to enable PI's Institution to carry out a scientific research project, as described in more details in the Access Agreement itself. This DPA is deemed attached by reference to the Access Agreement. The execution of the Access Agreement involves the processing of personal Data by HT, acting as processor, on behalf of and on the basis of the information and instructions provided by PI's Institution, acting as controller.

b) The Processor has represented to the Controller that it fulfils the necessary requisites of professionalism, experience, ability and reliability and has adopted technical and organizational measures such as to guarantee adequate protection for the personal Data to be processed and protection of the rights of the Data subjects, in execution of the Access Agreement.

c) With the present Data Processing Agreement, the Parties intend to regulate the processing operations to be carried out under the Access Agreement, including but not limited to setting out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal Data and categories of Data subjects concerned ("Data Subjects") and the corresponding obligations and rights of both Parties.

d) This DPA complements the Access Agreement in relation to the purpose referred to in letter c) above, otherwise the content of the Access Agreement remains unchanged.

Whereas all the above, the Parties agree as follows.

1. Recital and Appendixes

1.1. The Recitals and Appendixes form an integral and substantial part of the DPA.

2. Object

2.1. Through this DPA, the Controller hereby designates HT as processor with regards to the processing of personal Data to be carried out on behalf of and under the instructions of the Controller (the "Instructions") and to perform the relevant activities foreseen in the Access Agreement.

2.2. The Parties undertake to comply with the provisions prescribed by the Applicable Data Protection Legislation (as defined at Article 3.1(c) below) that apply, respectively, to PI's Institution in its capacity as controller and HT in its capacity as processor.

3. Definitions

3.1. For the purposes of this DPA, the terminology and definitions used in Applicable Data Protection Legislation, as well as all terms defined below and within the DPA, shall apply.

a) "**Personal Data**" or **"Data"**: means any personal Data (as defined in the Applicable Data Protection Legislation), in any form, format or support, that may be associated with, incorporated in or derived from the Input Material and Input Data (as described in the Access Agreement) transferred by the Controller to the Processor, which processes it on behalf of the Controller in order to carry out the activities described in the Access Agreement and under the instructions provided by the Controller itself.

b) "**Data Subjects**": means the natural persons whose personal Data are processed under this DPA.

c) "**Applicable Data Protection Legislation**": means any applicable law relating to the processing, privacy, and the use of personal Data, as applicable to the performance of the activities described in the Access Agreement. The above may include any law, regulation or measure of a competent Authority that regulates the protection of personal Data. In respect of both Parties' processing, Applicable Law includes Regulation (EU) 2016/679 ("GDPR") and the applicable Italian national Data protection law.

d) "**Breach of Security**": means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Data.

e) "**Sub-processor":** means any other processor, established within or outside EU/EEA, appointed by the Processor to carry out some specific processing activities on behalf of the Controller.

4. Processing activities

4.1. The Processor shall process, on behalf of the Controller, the Personal Data that may be incorporated into the Input Material and Input Data (as described in the Access Agreement) transferred by PI's Institution under the Access Agreement and listed in Appendix A of this DPA, referring to the categories of Data Subjects also identified therein.

5. Purposes of the processing

5.1. The processing activities set forth by this DPA are aimed at what is necessary to enable HT to carry out the activities described within the Access Agreement on behalf of the Controller.

6. Instructions on the processing activities

6.1. The Processor declares and guarantees that it will process the Personal Data exclusively on behalf of the Controller, according to the instructions given by this one and contained in the DPA or otherwise provided in writing by the Controller ("Instructions"). The Controller may propose to modify, replace or add processing instructions in writing during the term of the DPA.

6.2. Notwithstanding the full responsibility of the Controller for the Instructions given and the relating processing activities performed, in the event that the Processor considers that one or more Instructions issued by the Controller violate the Applicable Data Protection Legislation ("Contested Instructions"), the Processor shall send the Controller a written communication as soon as possible, indicating both the Contested Instructions and the reasons for the contestation. Following the communication, the Processor may suspend the processing connected to the mentioned Contested Instructions.

6.3. Following the information provided by the Processor, the Controller may confirm the Contested Instructions. In any case, the Controller will remain fully responsible towards the Processor, keeping the latter fully indemnified and unharmed from any and all prejudicial consequences deriving from them. The Processor will in any case be required to comply with the Contested Instructions, provided that the Controller contacts the competent Supervisory Authority to obtain confirmation of the legitimacy of the Contested Instructions. The Controller shall inform the Processor of the opinion provided by the authority without delay.

6.4. Without prejudice to the foregoing, if for the Processor the confirmation of the Contested Instruction leads to a breach of the Applicable Data Protection Legislation, the Processor may terminate the DPA by a written communication to be sent to the Controller by registered letter with return receipt or certified e-mail (PEC) providing the reasons for that choice. The DPA will be considered terminated 15 (fifteen) natural and consecutive days after the delivery of the communication to the Controller.

7. Obligations of the Controller

7.1. The Controller declares and guarantees that:

a) the instructions relating to the processing of the Data provided to the Processor during the execution of this DPA are consistent with the information provided – by the Controller

or a third party - to the Data Subjects and the consent expressed by the latter and/or to any other valid legal basis under which the Controller processes the Personal Data (the validity of which is acknowledged and granted by the Controller itself), and compliant with Applicable Data Protection Legislation;

b) where the Controller processes Data on the basis of the Data Subject's consent, the abovementioned information and consent were, respectively, given to and expressed by the Data Subjects in compliance with all Applicable Data Protection Legislation;

c) all personal Data processing activities governed by this DPA are carried out on the basis of at least one of the conditions referred to in Applicable Data Protection Legislation;

d) the Data provided by the Controller are accurate and up-to-date.

7.2. If, in the course of the execution of this DPA, the purposes for which the Personal Data are collected should change, the Controller guarantees, under its own responsibility, to negotiate with the Processor on the possible amendment of this DPA.

8. Obligations of the Processor

8.1. The Processor will process the Personal Data only for the agreed purposes and to carry out the activities described in the Access Agreement. The categories of personal Data processed as well as the relevant Data Subjects, the means and purposes of processing are listed in Appendix A of this DPA. This DPA is without prejudice to any processing operation that may be prescribed to the Processor by any applicable law; however, the Processor shall promptly inform the Controller in such circumstance.

8.2. Without prejudice to the provision of art. 19 below, the processing of the Personal Data will be carried out for a period no longer than that necessary to carry out the activities described in the Access Agreement.

8.3. The Processor does not produce copies of the Personal Data and does not perform any other type of processing that is not related to the activities described in the Access Agreement.

8.4. Without prejudice to the possible designation of Sub-processors pursuant to this DPA, the Processor shall not communicate nor transmit to third parties nor disclose the Personal Data, wholly or partially, without the authorization of the Controller, unless such communication, transmission or disclosure is necessary to carry out the activities described in the Access Agreement or in order to comply with a legal obligation to which the Processor is subject or with an order issued by a competent Authority.

8.5. Without prejudice to provision of art. 8.4 above, if the Processor is required to communicate personal Data in order to comply with legal obligations or to comply with an order from a competent authority, the Processor will promptly notify the Controller in writing before complying with any request for communication, unless the applicable legislation expressly forbids the Processor to do so; furthermore, the Processor shall communicate only the minimum possible amount of personal Data necessary to comply with the relevant law or order of a competent Authority.

8.6. The Processor undertakes to identify the persons authorized to process the Data ("Authorized Persons") and to provide them with proper instructions regarding the operations to be carried out and to implement adequate security measures to minimize the risks of accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data.

8.7. The Processor manages and documents its activities in a manner compatible and functional to the requirements of the Applicable Data Protection Law and the DPA.

8.8. The Processor shall adequately assist and cooperate with the Controller in order to enable the latter to comply with its obligations under the Applicable Data Protection Legislation, responding promptly and adequately to the Controller's reasonable requests relating to the processing of personal Data carried out by the Processor on behalf of the Controller.

8.9. Upon request of the Controller, the Processor will assist as far as reasonably possible in carrying out the Data protection impact assessment, taking into account and within the limits of the nature of the processing and the information available to the Processor.

8.10. Upon request of the Controller, the Processor shall inform of any replacement of the Data Protection Officer (DPO) happening during the execution of this DPA, providing the Controller with the contact details of the new DPO.

8.11. The Processor shall inform the Controller in advance and in writing of any circumstance that may generate uncertainties regarding the maintenance of the requirements according to which it has been appointed as Processor by the Controller in pursuance of the Applicable Data Protection Legislation, or of any total or partial incapacity to process the Data or ensure their security in accordance with the instructions of the Controller, the DPA, the Access Agreement and the Applicable Data Protection Legislation.

9. Possible interactions of the Processor with the Data Subjects

9.1. According to the Access Agreement, the Processor shall only receive Data in pseudonymized or anonymized form, without information that can identify Data Subjects and, therefore, HT will not know the identity of these ones. Similarly, the Processor shall not attempt in any way to re-identify Data Subjects and shall not have any interaction with these ones.

10. Confidentiality of the Personal Data

10.1. The Processor guarantees that the Authorized Persons, as well as any Sub-processors and their employees, are committed to confidentiality or have an adequate legal obligation of confidentiality and that such Authorized Persons will process Personal Data according to the instructions of the Controller.

11. Security Measures

11.1. For the processing operations provided for by this DPA, the Processor undertakes to adopt technical, logical and organisational measures according to Applicable Data Protection Legislation, in order to ensure a level of security appropriate against risks for the rights and freedoms of the Data Subjects, deriving, inter alia, from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Data, as well as processing non-authorised, incorrect or not in accordance with the means and purposes agreed upon the Parties, and/or loss of integrity, accuracy and confidentiality of the Data.

11.2. At any time, the Controller may require in writing the Processor to adopt specific and additional technical and organisational security measures, when those already adopted by the Processor (listed in the Appendix B) are proved to be no longer suitable for the protection of the

Data taking into account the objectives and proven technical progress and the state of the art as well as the costs of implementation, to be assessed according to objective criteria based on the technical standards approved and applied in the referenced sector, and, in any case, whenever technical/organisational measures are prescribed by the competent authority or by the Applicable Data Protection Legislation.

12. Conservation of documents

12.1. The Processor shall manage with effective procedures the documentation related to the obligations provided for by the DPA, the regulations or prescribed by the Supervisory Authority, ensuring its custody, integrity and prompt recovery.

13. Sub-processors

13.1. The Controller provides the Processor with its general authorization to engage one or more Sub-processors in order to fulfil, wholly or partially, the obligations provided for by this DPA and in the Access Agreement. The Processor, before engaging any new Sub-processor and without prejudice to those already in use at the date of signing of this DPA which are included in Appendix C (if any), shall notify the Controller so that the latter may exercise its right to oppose such new appointments pursuant to article 13.2 below.

13.2. In order to exercise its right to oppose to the engagement by Processor of new Sub-processors, the Controller shall inform the Processor in writing of its opposition to one or more of the new Sub-processors within and no later than seven (7) working days from the notification of the Processor, providing the reasons for its opposition. In this case, the Processor shall do everything in its reasonable power to make available a different method to fulfil its obligations for which the new appointment as Sub-processor has been notified, without this being excessively burdensome for the Processor. If the Processor is not able to make available such different modality within a reasonable term agreed between the Parties, the Processor may, by written communication, withdraw from this DPA only with regard to those obligations that cannot be fulfilled by the Processor without engaging the new Sub-processor to which the Controller has opposed. The consequent total or partial termination will not entitle the Controller to claim compensation or indemnification of any kind.

13.3. Without prejudice for the above, the Processor entering into an agreement with a Sub-processor shall respect the following conditions.

a) The Processor shall diligently choose the Sub-processor, paying particular attention to the reputation and experience as well as the adequacy of the technical and organizational measures adopted by the latter. The Processor shall enter into a written agreement with any Sub-processor which must: (i) provide for the Sub-processor the same obligations as those set forth in the DPA for the Processor itself; (ii) describe the processing operations covered by the agreement; (iii) describe the technical and organizational measures that the Sub-processor shall implement pursuant to this DPA and applicable legislation. The Processor is required to promptly transmit to the Controller, upon request of the latter, a copy of the aforementioned agreement entered into with any Sub-processor.

b) The Processor shall promptly notify the Controller with any failure of a Sub-processor to comply with the obligations arising from the Applicable Data Protection Legislation and/or from the agreement entered into with the Sub-processor. Furthermore, the Processor shall request in writing to any Sub-processor to remedy any non-compliance. In the event that the Sub-processor is not able to remedy any non-compliance within a reasonable period of time from the request of remedy, the Controller may revoke the authorization granted for the appointment of the Sub-processor. In the event that the Sub-processor fails to comply with its Data protection obligations, the Processor remains fully liable to the Controller for the failure of the Sub-processor to comply with its Data protection obligations.

c) Where the appointment of a Sub-processor may cause the transfer of the Data to a third country, the Processor shall preemptively ensure that at least one of the safeguard mechanisms provided for in Articles 44 and following of the GDPR is in force or is adopted.

14. Places of Data processing

14.1. The Parties expressly agree that the Processor may transfer the Data outside the EEA without prior request and corresponding written authorization by the Controller. However, if requested by the Controller, the Processor shall provide the Controller with a complete list of all processing operations carried out outside the EEA. For the purposes of this clause, "transfer of Data" means any procedure carried out in the context of the processing operations referred to in this DPA where there is a flow of Data to a third country.

14.2. Without prejudice for Article 14.1, in case of transfer of the Data to a third country in relation to which the European Commission has not issued an adequacy decision, the Processor is in any case obliged to use one of the mechanisms indicated in Articles 46 and following of GDPR.

14.3. The provisions referred to in this Article 14 shall be also applied to Sub-processors.

15. Obligation of notification and exercise of rights by Data Subjects

15.1. Without undue delay, the Processor shall notify the Controller of any legally binding request for disclosure of personal Data, submitted by judicial or police authorities and relating to the Data, unless such notification is prohibited by specific rules (e.g. criminal law rules aimed at protecting the confidentiality of investigations), or by any court order or order of any competent authority/regulator.

15.2. Without prejudice to the above, if the Processor receives even through Authorized Persons or Sub-processors eventually appointed pursuant to this DPA requests for information or other requests from possible Data Subjects (such as exercise of the rights of access to Data, rectification, erasure, opposition, withdraw of consent), the Processor shall immediately:

- notify the Controller in writing by attaching a copy of the request;
- follow any operating instructions of the Controller;
- give to the Controller any information necessary to verify the identity of the applicant in order to verify the legitimacy of the request;

- contribute in general to the completeness of the information to be provided by the Controller to the Data Subject.

15.3. In any case, and also considering the pseudonymisation of the Data, the Processor will not give any feedback to the Data Subjects.

16. Breach of Security (*Data Breach*)

16.1. In the event of a Breach of Security pertaining the Data, after becoming aware of it, the Processor shall promptly notify the Controller. As soon as possible after becoming aware of the Breach of Security, and in any case no later than 48 hours after becoming aware of it, the Processor shall provide the Controller, even in subsequent stages, for detailed information regarding the Breach of Security and in particular the following:

a) the type of breach[1]

b) the nature, sensitivity and volume of the personal Data concerned

c) possibility of identification of persons (pseudonyms)

d) the seriousness of the consequences for Data Subjects (e.g. physical harm, psychological distress, humiliation or damage to reputation)

e) the list of persons concerned (pseudonyms) by the security breach (if available)

f) the categories and approximate number of Data subjects and the categories and approximate number of personal Data records concerned

g) probable consequences of the Breach of Security for the Controller and those suffered by the Processor and/or Sub-processors

h) the measures taken or to be taken to address the personal Data breach, to mitigate the effects and minimize the damage resulting from the breach of security, insofar as the remedies are within the reasonable control of the Processor.

16.2. In accordance with the Applicable Data Protection Legislation, in the event of a Breach of Security the Processor shall provide reasonable assistance to the Controller in fulfilling the latter's obligation to inform the competent Supervisory Authority and the Data Subjects (where necessary pursuant to Applicable Data Protection Legislation) by providing the information at its disposal referred to in Article 16.1 above and taking into account the nature of the processing.

17. Controls and Audits

17.1. The Processor shall make available to the Controller the information necessary to demonstrate compliance with the obligations arising from this DPA and from the Access

[1] Types of data breaches:
- "breach of confidentiality" – in case of unauthorized or accidental disclosure or access to personal data.
- "breach of availability" – in case of unauthorized or accidental loss of access or destruction of personal data.
- "breach of integrity" - in case of unauthorized or accidental alteration of personal data.
  Examples of loss of availability are when the data has been accidentally or by an unauthorized person deleted or, in the case of encrypted data, when the decryption key is lost. If the Controller cannot restore access to the data, for example through a backup, this is considered a permanent loss of availability.

Agreement. In addition, the Processor allows and contributes to audit activities - including inspections carried out by the Controller.

17.2. In particular, the Controller is entitled to carry out, at its own and sole expenses and with a prior notice of thirty (30) days, audits and inspections in the places where the processing operations pursuant to this DPA are carried out and the Data or the documentation relating to this DPA are stored. In any case, the audits and inspections shall be carried out by the Controller exclusively on "working days" (i.e. days different from Saturday, Sunday and public holidays). Audits and inspections shall be conducted without prejudice to the confidentiality and the performance of the activities of the Processor not related to the ones encompassed within the present DPA.

17.3. The Processor shall promptly notify the Controller of requests from possible Data Subjects, disputes, inspections or requests by the Supervisory Authority and the judicial authorities, and any other relevant information in relation to the processing operations carried out pursuant to this DPA.

18. Execution, duration and termination

18.1. This DPA shall have effect from the date of signature and its duration is the same as that provided for in the Access Agreement. Without prejudice for the provision of this DPA, the conditions and rights of withdrawal are the same as those set out in the Access Agreement of which this DPA is an integral part.

-

19. Termination of processing operations

19.1. At the termination of the Access Agreement, for whatever reason, the Processor shall:

- cease or cause to cease the processing operations related to this DPA and the execution of Access Agreement;
- at the Controller's discretion, return to the Controller the Data – in accordance to the modalities prescribed by the Controller – or provide for their complete erasure. In this case the Controller shall notify its will to the Processor with prior notice of sixty (60) days before the end of the Access Agreement;
- in the absence of communications within the established terms, the Processor will proceed to return the Data and, at the same time, will delete the Data from its systems.

The above does not affect any communication or transmission of the Data made within the Access Agreement and under the instruction of/in accordance with the Controller.

19.2. The retention of personal Data to the extent and for the time as prescribed to the Processor by applicable law remains unaffected.

20. Prevalence between agreements

20.1. If there are contradictions or incompatibilities between the provisions of the DPA and the Access Agreement and/or other existing agreements between the Parties, the provisions of the DPA governing the obligations of the Parties in matters of Data protection will prevail. The DPA also prevails in case of doubts on whether the contractual clauses contained in those other

agreements regulate the obligations of the Parties in matters of Data protection.

21. Miscellaneous

21.1. Each Party undertakes to defend, indemnify and hold harmless the other Party, its collaborators, administrators, employees, successors and agents (collectively the "Indemnified Parties") from any action, damage, liability, loss, cost, administrative fine and other expense (including reasonable fees and legal fees) arising from any legal action, claim, request, order or other proceeding by third parties (including control authorities) arising from or related to the breach of the obligations of the other Parties provided for by this DPA. Both Parties agree that upon receipt of a notice of claim, demand or judgement foreseen above, the Party receiving such notice will promptly notify the other Party to allow the latter to exercise its related right of defense.

21.2. The applicable law and exclusive competent Court for any dispute arising from the DPA are the same established by the Access Agreement and subsequent amendments thereof.

21.3. The unenforceability or invalidity of one or more provisions of the DPA does not affect the remaining parts of this DPA. The invalid or unenforceable provision may be: (i) amended if it is necessary to ensure its validity and enforceability, respecting as closely as possible the will of the Parties and the balance of the respective interests or – if this is not possible – (ii) considered as if it were not ever included in the DPA. The foregoing also applies in the case where the DPA has gaps.

21.4. Each amendment, even partial, of this DPA shall be done through a written agreement between the Parties.

21.5. The Parties may request to amend any content of the DPA in such a manner as to satisfy any interpretation, guideline or ordinance issued by competent authorities, national implementing provisions, or further regulatory developments relating to the general requirements provided for by the Applicable Data Protection Legislation for the appointment of processors or additional requirements for such appointment. The Parties shall agree on any amendment in good faith as well as perform their contractual obligations thereof in compliance with Applicable Data Protection Legislation.

The Controller	**The Processor**
Name: …	Name:
Title: …	Title:
Place: …	Place: Milano
Date: __/__/__	Date: …
Signature	Signature

APPENDIX A

The Data Protection Officer of the Controller

- The Controller has not appointed any Data Protection Officer as the requirements indicated by the Applicable Data Protection Legislation for the relevant mandatory appointment do not occur.
- The Controller has appointed a Data Protection Officer whose contact details are the following: ...

The Processor will be immediately informed about any variation to these contact details.

The Data Protection Officer of the Processor

The Processor has appointed a Data Protection Officer whose E-mail address is: dpo@fht.org

Data Subjects:

The Personal Data will be referred to the following categories of Data subjects:

- [e.g The donors from whose biological samples the materials to be transferred were generated.]

Categories of personal Data processed.

HT will process the Personal Data transferred by the Controller in pseudonymised/anonymised form and associated with, incorporated in or derived from the Input Material and Input Data (as described in the Access Agreement).

APPENDIX B

TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

The Processor shall comply with the following technical and organizational security measures.

- Ensure adequate environmental prevention measures
- Provide appropriate instructions to those in charge to process personal Data
- Allow access to IT systems through the use of unique identifiers for each user, avoiding identifiers shared between multiple users, and allow the attribution to each user profile only to the permission necessary for the performance of their respective operational tasks;
- Ensure the adoption of a correct application architecture through: Least privilege (each process must be performed with the minimum set of necessary permissions);
- Use highly robust administrative credentials and periodically check the confidentiality of said credentials;
- Prevent the reuse of previously used passwords (password history);
- Use updated antivirus software on end-user computers;
- Adopt firewalls and backup and Data recovery systems;
- Carry out periodic vulnerability assessments;
- Tracking and logging for the duration of the collaboration;
- Provide appropriate instructions to those in charge;
- Stay up to date on rules, regulations or security vulnerabilities;
- Develop and keep safety standards constantly updated;
- Share personal Data of Data subjects exclusively in encrypted form to an identifiable destination.
- Transfer Data using secure communication protocols such as sftp
- Ensure correct Data Management

APPENDIX C