Protocol
On the management and use of the
Personal Exposure and Health Data Platform

Release date: 08/11/2023

Preliminary provisions

In the HBM4EU project a central data platform has been developed at VITO in order to give access and to share single measurement data from HBM studies in the highest possible resolution to the partners within the project.

It is the intention of the Supplying Data Controllers of the data included in this platform, to make the data on this central data platform further available to the partners of the HBM4EU project, as well as to the broader research community according to the terms and conditions of this protocol and the Regulation 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 ('GDPR', General Data Protection Regulation), and allow additional data to be added to it.

This Protocol describes the terms and conditions on the data exchange between Supplying and Receiving Data Controllers via this central data platform, further called the Personal Exposure and Health Data Platform ("PEH Data Platform"), the role of the PEH Data Platform Manager, as well as the processing activities performed by the Receiving Data Controller.

ARTICLE 1: DEFINITIONS

PEH Data Platform Manager: VITO who will host and manage the PEH data platform and will give access to subset(s) of the data to the Receiving Data Controllers after approval of the request by the DRAC.

Data Analysis Plan: a plan completed by the Receiving Data Controller in which the Receiving Data Controller describes on how the requested data would be processed and for what purpose. In this plan, the Receiving Data Controller should always bear in mind the principles of article 5 of the GDPR. The Data Analysis Plan is part of the Request For Access.

Data Controller: the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. Under these terms and conditions, there are the following two types of Data Controllers:

- **Supplying Data Controller ("SDC"):** a Data Controller who submits data into the Central Data Platform.
- **Receiving Data Controller ("RDC"):** a Data Controller who gets access to (subsets of) the data from the Central Data Platform.

It is possible that the same organisation is both Supplying and Receiving Data controller for different subsets of data within the scope of this Protocol.

PEH Data Platform: the central database system, developed in HBM4EU, containing Personal Exposure and Health data, used for exchanging data between the Data Controllers, and hosted and managed by PEH Data Platform Manager.

Data Request Approval Committee ("DRAC"): A committee formed by a limited group of Supplying Data Controllers appointed by the General Assembly. It evaluates the Request For Access of the Receiving Data Controller and grants or denies access to the Receiving Data Controller to PEH data through the Central Data Platform.

General Assembly: Assembly of representatives of all signatories to this Protocol.

Personal Exposure and Health data ("PEH data"): Single measurement data (records of a data collection obtained from single data subjects) obtained at personal level including data on human biomonitoring (HBM), effect markers, health effects, personal environmental exposure, exposure determinants, and other accompanying variables.

Objection Period: the period in which Supplying Data Controllers have the option to submit a motivated objection against the decision of the Data Request Approval Committee to give access to specific PEH data. This period starts the day the involved Supplying Data Controller has been notified of the decision of the DRAC and lasts thirty (30) calendar days.

Protocol: this document and its terms and conditions that must be explicitly accepted in order for Data Controllers to deposit PEH data and/or to get access to PEH data in the PEH Data Platform.

Pseudonymisation: 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 organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Request For Access: application form completed by the Receiving Data Controller (or a joint application by more than one RDC) wishing to receive and process PEH data according to the processing activities defined in it. The Request For Access will contain the research objectives, study design and Data Analysis Plan. This Request For Access will be submitted by the Receiving Data Controller to the Data Request Approval Committee and based on this document the Data Request Approval Committee will decide whether data will be exchanged or not. The template for the Request For Access is specified in **Appendix 2**.

Research Project: the specific research for which the data are requested, which directly relates to specific research questions that are addressed; the Research Project can be a work package, a task or an activity in a larger project, if specific enough, or can be an independent project.

ARTICLE 2: PURPOSE AND OBJECTIVES OF THE PEH DATA PLATFORM

The PEH Data Platform will be made available to HBM4EU partners as well as to new partners to deposit additional HBM data and/or to get access to HBM data contained in it, as long as these partners accept and adhere to the terms and conditions of this Protocol.

The PEH Data Platform is a tool to collect, store and grant access in a harmonised way to HBM data (in the highest possible resolution), in compliance with national and EU ethics and legal requirements for the following purpose:

> Science and research in the public interest on new or better insights in the presence of chemical substances and metabolites in a person’s body, and/or its relations with presence of chemical substances and metabolites in ambient, indoor and occupational environment, food and products, and/or its potential effects on a person’s health.

ARTICLE 3: DATA

The data stored on the PEH Data Platform will be Pseudonymised or Anonymised Single Measurement Data and include personal sensitive data (see **Appendix 1**).

The details concerning the data in the PEH Data Platform are specified in Appendix 2, which forms an integral part of this Protocol. Data Controllers will be regularly notified of any updates of Appendix 2. These updates to Appendix 2 do not need to be ratified by a signature from the Data Controllers.

Personal data shall only be processed by the Receiving Data Controller considering the specified purpose(s) defined in the Request For Access and Data Analysis Plan (Appendix 2).

ARTICLE 4: PROCEDURE FOR SUBMITTING AND EVALUATING A REQUEST FOR ACCESS

The procedure for submitting and evaluating a Request For Access is illustrated in Figure 1.

i. The RDC fills in a Request For Access (Appendix 2), describing the Research Project for which the data is necessary, an identification of Data Processors (if applicable) and a Data Analysis Plan with the requested variables.

ii. The Request For Access is sent to the DRAC by the RDC.

iii. The DRAC reviews the Research Project and performs a check for data minimization on the Data Analysis Plan of the RDC (5.3). Based on this review, the DRAC will:

   a. advise to grant access to the requested data in which case it informs – within two (2) calendar days - the involved SDC’s of its advice to grant access to the requested data.

   b. deny access to the requested data in which case it informs the involved SDCs and the RDC of the rejection of the Request For Access and the motivation for the rejection.

   c. ask for further clarification and adaptation from the RDC, after which it reviews the adapted Request For Access, and takes a decision to grant or deny access.

   The DRAC performs its review and take its decision to grant access within two (2) months of submission of the Request For Access. The RDC can request for an urgent treatment of its Request For Access. The DRAC is free to follow this request or not.

   Within a maximum of two (2) calendar days after its decision, the DRAC shall officially notify the involved SDCs in case of a positive advice, and both the involved SDCs and RDC in case of rejection of the Request For Access.

iv. Each involved SDC can submit a motivated objection to the advice to grant access during the Objection Period, starting the day the involved SDCs have been notified of the advice. The Objection Period starts from the notification of the official advice of the DRAC and lasts maximum thirty (30) calendar days. This Objection Period will be terminated as well when all involved SDCs have explicitly stated that they don't object to the Request for Access. The objection must be motivated, and will be communicated by the Supplying Data Controller to the DRAC.

In case there is no objection the request is automatically and definitively approved.

In case of motivated objection by one or more SDCs, the DRAC verifies if the objection is sufficiently motivated. It may ask for further clarification from the objecting SDC(s). Based on this verification:

a. The objecting SDC may decide to withdraw its objection;
b. the DRAC will reject the Request For Access;
c. the DRAC will partially approve the Requested Access For Data, i.e., deny access to the data of the objecting SDC only.

In the latter two cases it informs the involved SDCs and the RDC of the (partial) rejection of the Request For Access, and the motivation for the (partial) rejection. After a Request For Access has been (partially) rejected, the RDC is free to submit a new or adapted Request for Access to the DRAC, following the same procedure.

v. The DRAC submits the approved request to the PEH Data Platform Manager. The PEH Data Platform Manager provides the requested and approved data to the RDC.

vi. If requested by the SDC, the RDC will delete the data within one (1) month after the end of the Research Project as indicated in the application form, and confirms deletion of the data to the SDC. Notwithstanding the foregoing, the RDC can keep a copy of the data for 2 years to enable reproducibility.

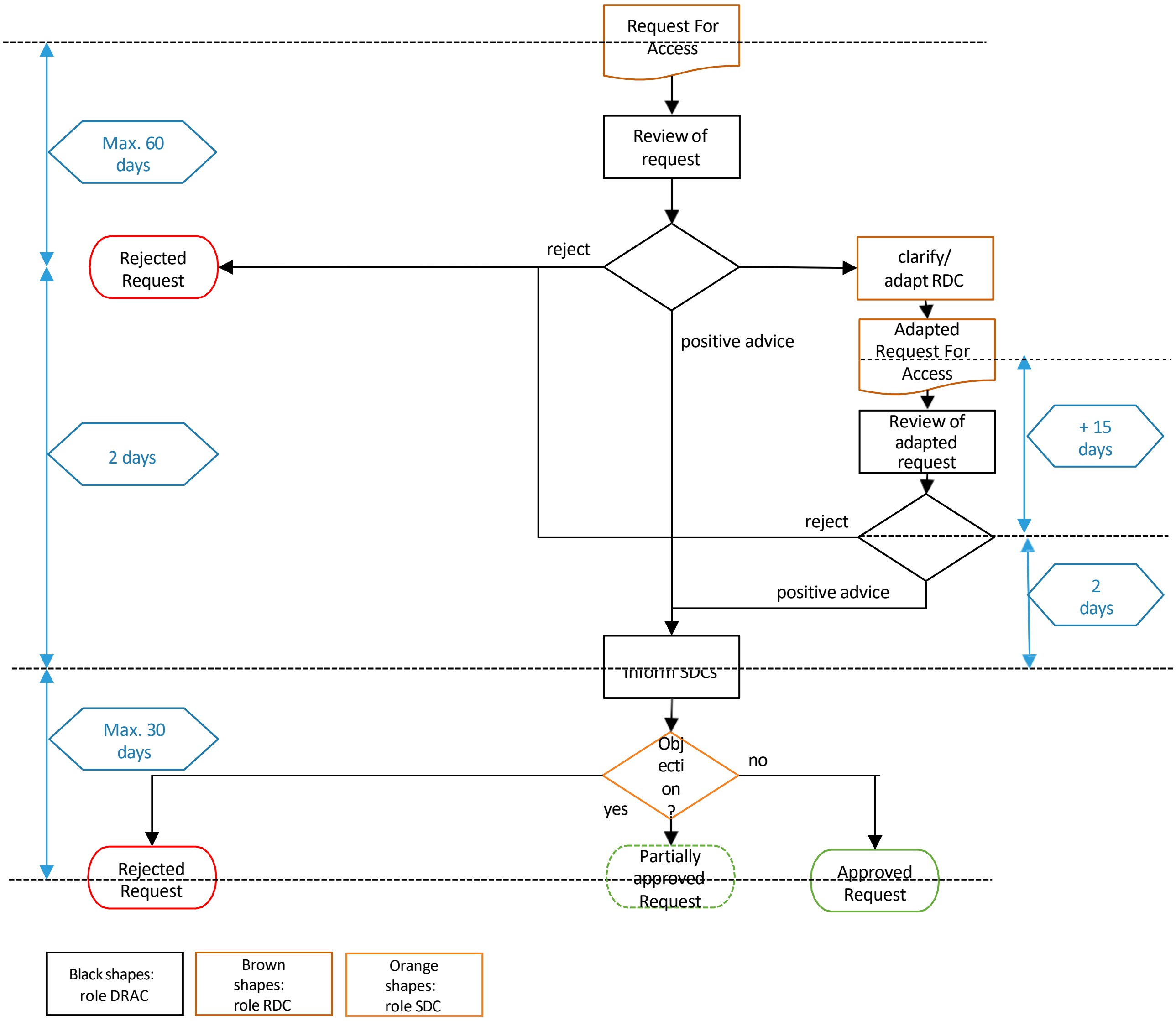

Figure 1: Procedure for submitting and evaluating a Request For Access.

ARTICLE 5: RIGHTS AND OBLIGATIONS

5.1 Supplying Data Controller

By signing this protocol the SDC declares that the collection of the data it submits to the PEH Data Platform complies with all national and EU ethics and legal requirements, i.e.,

- that all required ethical approval has been obtained for collecting the data it submits to the PEH Data Platform;
- that for the data it submits to the PEH Data Platform the consent of the data subject has been obtained for processing his or her personal data or that the processing of the data is based on another legal ground described in Article 9.1 of the GDPR.

The Supplying Data Controller:

- ensures that the data are pseudonymised before transfer to the Central Data Platform;
- informs the DRAC and the PEH Data Platform Manager of any requests or issues regarding the informed consent given by its data subjects which may affect the use or content of the data on the Central Data Platform;
- remains responsible towards the data subjects, shall inform the data subject of the further processing of his or her personal data in order to comply with the information obligation arising from article 5 of the GDPR, and shall inform the PEH Data Platform Manager and the DRAC of any change in the data or the informed consent of the data subjects from whom the HBM data is stored on the Central Data Platform.
- is responsible that PEH data are securely transferred to the PEH Data Platform.
- shall have appropriate technical and organizational measures in place for the fulfilment of their obligation to respond to requests for exercising the data subject's rights laid down in the GDPR.
- shall immediately inform the DRAC if, in its opinion, this Protocol infringes the GDPR or other Union or Member State data protection provisions to which the Supplying Data Controller is subject.
- has the option to submit a motivated objection against the decision of the Data Request Approval Committee to exchange specific HBM data.

5.2 Receiving Data Controller

The Receiving Data Controller destroys his copy of the data within one (1) month after the end of the Research Project indicated in the application form.

The Receiving Data Controller processes the personal data only in accordance to the approved Request For Access and Data Analysis Plan, and shall not further process the personal data subject to this Protocol in a manner which is incompatible with the provisions laid down in this Protocol and the documents and conditions on which the DRAC has given its consent to exchange HBM data.

The Receiving Data Controller is not allowed to attempt to identify or contact any of the data subjects. In the event that the Receiving Data Controller inadvertently identifies any data subject, it must notify the Supplying Data Controller immediately and describe the circumstances by which it happened.

The Receiving Data Controller shall immediately inform the DRAC if, in its opinion, this Protocol infringes the GDPR or other Union or Member State data protection provisions to which the Receiving Data Controller is subject.

The Receiving Data Controller is responsible and liable for handling the personal data and its processing with utter confidentiality and in accordance with the GDPR.

The Receiving Data Controller ensures that only persons authorized to process the personal data and bound by confidentiality obligations at least as stringent as the ones set forth in this Protocol have access to these personal data.

The Receiving Data Controller may engage a Data Processor for carrying out specific processing activities under certain conditions (see Article 7).

5.3 Data Request Approval Committee ("DRAC"):

Members

The DRAC is elected by the General Assembly for a period of five (5) years, and can be dismissed by the General Assembly at any time. Every SDC can propose members. Each member shall be approved by the General Assembly. The platform manager will organize these elections and will provide timely all the SDC's with the necessary procedures and modalities. All members of the DRAC will carry out their responsibilities free of charge. The DRAC has between five (5) and ten (10) members ("DRAC members"), each from different Supplying Data Controller organisations, and preferably having complementary expertise and background needed to cover different aspects of the requests. The chairperson will be elected between the members themselves. The DRAC can ask the PEH Data Platform Manager to verify if requested data are available in the data platform.

Every five (5) years, the DRAC will be reconstituted, where each Supplying Data Controller who has signed the Protocol can participate in the election.

Members can be changed by (written) approval of the General Assembly.

Meetings

An ordinary meeting of the DRAC will take place whenever it is needed to fulfil its obligations in due time. An extraordinary meeting will take place at any time upon written request of the General Assembly or upon written request of a Receiving Data Controller if that RDC can demonstrate special urgency. Meetings can be online.

The chairperson shall prepare and send each DRAC member a written agenda no later than five (5) days preceding the meeting. The agenda will include the various requests from Receiving Data Controllers, including the associated Request for Access. During a meeting the DRAC members present can unanimously agree to add a new item to the original agenda.

The DRAC shall not deliberate and decide validly unless two-thirds (2/3) of the members are present or represented (quorum). If the quorum is not reached, the chairperson shall convene another ordinary meeting within fifteen (15) calendar days.

Each DRAC member present or represented in the meeting shall have one vote.

Decisions to grant access shall be taken by a majority of two-thirds (2/3) of the votes cast.

The chairperson shall produce written minutes of each meeting which shall be the formal record of all decisions taken. He/she shall send the draft minutes to all DRAC members within ten (10) calendar days of the meeting. The decision shall befinal after the minutes have been approved. Notification of the decision will be made within 2 days after approval.

Authority

The DRAC receives the Requests For Access from RDC's and shall verify the criteria for access:

- conformity of the Research Project and the research questions for which the PEH data is requested with the purpose of the PEH Data Platform specified in article 2 of this Protocol;
- conformity of the Data Analysis Plan with the Research Project and the research questions;
- whether the data request is restricted to only the data needed to carry out the Data Analysis Plan in adherence to the data minimisation principle laid down in the GDPR Article 5(1)(c);
- reasonable time frame of the Research Project;
- whether there is no embargo period on access to the requested data.

Based upon these verifications of the Request for Access, the DRAC shall approve or reject the Request For Access, possibly after adaptation, following the procedure described in Article 4.

The DRAC will perform its investigation and take its decision within two (2) months of submission of the Request For Access. In the case of a personal data breach related to the processing subject of this Protocol, the DRAC can instruct the Receiving Data Controller to stop further processing of the personal data with immediate effect. After this intervention the DRAC will report this to the General Assembly (procedure "Breaching Data Controller": see article 17 of this Protocol).

Internal rules of operation

After composition of the DRAC, internal rules of operation will be drawn up timely, in which the functionality of this organ will be addressed in detail.

5.4 PEH Data Platform Manager

The PEH Data Platform Manager shall:

- host the PEH Data Platform for ten (10) years starting from 1st July 2022;
- upon receipt of the approved request from the DRAC, supply the requested PEH data to the relevant RDC;
- ensure that only the approved subset of data is supplied to the RDC to perform the processing by the RDC;
- report yearly to the General Assembly on the use of the PEH Data Platform;
- organise the signing of the protocol, and adapt the protocol according to decisions of the General Assembly or its appendices.

The PEH Data Platform will be managed by the following Data Processor:

> VITO, a limited liability company, with its registered office situated at Boeretang 200, 2400 Mol,
> Belgium, CBE 0244.195.916 (RPR Turnhout)

contact details DPO: charlotte.vanhoof@vito.be

VITO has the following specific responsibilities as PEH Data Platform Manager:

- assist the SDC in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR relating to data breach procedure;
- notify, in the case of a data breach, the SDC, when becoming aware of a personal data breach. Furthermore the PEH Data Platform Manager shall assist the SDC in the assessment of the consequences of the personal data breach and the measures taken or proposed to be taken to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
- enable secure transfer of the PEH data to and from the PEH Data Platform
- make templates available (such as: Request For Access, code books and data templates for data delivery, codebooks for data users, …)
- run scripts for quality control of the provided data (conformity with codebooks, consistency checks, missing data, ranges and categories for variables, …), and for calculating derived variables (i.e., creatinine adjusted variables, imputed variables for biomarker data below LOD/LOQ, …)
- keep a registry of all Requests For Access and the decisions taken
- keep a registry of data exchanges and data use
- manage the user accounts for Supplying Data Controllers and Receiving Data Controllers (= data users).
- manage the access and download rights for each user.
- carry out the initial DPIA for the PEH data platform. The Data Controllers shall assist each other as they carry out a data protection impact assessment (DPIA) in accordance with Article 35 of the GDPR.
- change – and capacity management of hardware and software components
- in general terms comply with the GDPR. VITO commits to handle the personal data and its processing with utter confidentiality. VITO ensures that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- VITO is not responsible for the interruptions of the data platform services that are due to force majeure.

VITO has technical and organizational measures in place to comply with the GDPR and to enable secure processing and transfer of the PEH data (**Appendix 4**).

VITO has the right at any time to adapt the PEH Data Platform's hardware and software if it deems this advantageous for a more efficient operation of the Data Platform and performance of its obligations.

In the coming years VITO will not charge any costs for hosting and maintaining the platform (as they are borne by PARC, the Partnership for the Assessment of Risks of Chemicals, in which they are included in the VITO budget). Adaptations to this cost arrangement, such as reimbursement of costs made for projects outside PARC, and for guaranteeing long-term sustainability (including funding) will be made in agreement with the General Assembly.

5.5 General Assembly

Members

The General Assembly consists of one representative of each of the parties to the Protocol, including the PEH Data Platform Manager, ("GA members"). The chairperson will be elected between the members themselves.

Meetings

At least once a year an ordinary meeting of the General Assembly will take place. An extraordinary meeting will take place at any time upon written request of one third (1/3) of the GA members. Meetings can be online.

The chairperson shall prepare and send each GA member a written agenda no later than five (5) days preceding the meeting. During a meeting the GA members present or represented can unanimously agree to add a new item to the original agenda.

Each GA member shall not deliberate and decide validly unless two-thirds (2/3) of the members acting as SDC or PEH Data Platform Manager are present or represented (quorum). If the quorum is not reached, the chairperson shall convene another ordinary meeting within fifteen (15) calendar days.

Each GA member, except members that solely act as RDC, present or represented in the meeting shall have one vote. Decisions shall be taken by a majority of two-thirds (2/3) of the votes cast.

The chairperson shall produce written minutes of each meeting which shall be the formal record of all decisions taken. He/she shall send the draft minutes to all GA members within ten (10) calendar days of the meeting.

Authority

The General Assembly is responsible for:

- Updates or changes to this Protocol
- Appointment and dismissal of members of the DRAC
- Analysing the yearly report of the PEH Data Platform Manager on the use of the PEH Data Platform
- Deciding, in case of violations of the terms and conditions under this Protocol or the GDPR and applicable national legislation by a Data Controller, to declare a Data Controller to be a "Breaching Data Controller" and deciding on the consequences thereof which may include termination of its participation to this Protocol and further use of the PEH Data Platform (see article 17 of this Protocol).

The PEH Data Platform Manager can object to updates or changes to this protocol that have important repercussions on its ability to carry out its obligations and/or on its workload.

ARTICLE 6: DATA TRANSFER CONDITIONS

The data are collected in the PEH Data Platform by the PEH Data Platform Manager. The Supplying Data Controllers submit these data in a single environment (data pool) where data from all the Supplying Data Controllers are stored together.

The Receiving Data Controllers will get access to the subset of data, subject to the conditions and approval of the DRAC.

The Receiving Data Controller shall not store the personal data any longer than needed to carry out the research for which the HBM data is allowed by the DRAC. At the choice of the Supplying Data Controller, the Receiving Data Controller shall delete or return all the HBM data to the Supplying Data Controller after the end of the provision of services in relation to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data. If the data is deleted, the Receiving Data Controller must provide the Supplying Data Controller with a declaration including sufficient supporting documentation that the data had been destroyed. The personal data shall be returned to the Supplying Data Controller without charge.

ARTICLE 7: USE OF PROCESSORS

The Receiving Data Controller may engage a Data Processor for carrying out specific processing activities. The RDC has to identify these processors in the Request For Access (Appendix 2), if the Data Processor(s) are already known at the time of the request. If the SDC wants to object to the engagement of the Data Processor(s), he can do so within the objection period described under article 6 of the Protocol.

In case the RDC wants to engage a Data Processor when the requested data has already been obtained, the RDC will notify the DRAC by writing, prior to the processing activities of the Data Processor. The DRAC will inform the Supplying Data Controller of the engagement of the Data Processor(s) by the RDC. The SDC can object to the engagement of the Data Processor(s), by a motivated objection within thirty (30) calendar days, starting from the moment the SDC has been notified.

In case the Receiving Data Controller engages a Data Processor, the same data protection obligations as set out in these terms and conditions shall be imposed on that Data Processor by way of a processing agreement, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of the GDPR. In case that Data Processor fails to fulfil its data protection obligations, the Receiving Data Controller shall remain fully liable for the performance of that Data Processor's obligations.

ARTICLE 8: MEMBERSHIP

A new party can join this Protocol as a Receiving/Supplying Data Controller without prior written approval of all the Parties, provided that the new party complies with and accepts in writing the terms and conditions of this Protocol. The PEH Data Platform Manager will notify all supplying Data controllers in case a new party joins the Protocol.

A participating Data Controller can decide to terminate its participation in this Protocol with a prior notice of three (3) months. After these three (3) months its data will be removed from the PEH Data Platform. However, it is still bound to the approved Requests For Data for which data have been provided to the Receiving Data Controller.

ARTICLE 9: SECURITY MEASURES

The Supplying Data Controller and the PEH Data Platform Manager are responsible for secure transfer of the data to the PEH Data Platform. The PEH Data Platform Manager will enable secure transfer of the HBM data to and from the PEH Data Platform.

The PEH Data Platform Manager is responsible for ensuring secure storage of the PEH data.

The PEH Data Platform Manager is responsible to enable secure access to subset(s) of the data to the Receiving Data Controller according to the approved Request For Access.

The Receiving Data Controller shall implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject.

The Receiving Data Controller shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, according to Article 32 of the GDPR.

In assessing the appropriate level of security, the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed, should be taken into account by the Receiving Data Controller.

A general description of the technical and organization security measures is included in **Appendix 3** to this Protocol.

ARTICLE 10: DATA BREACH

The Supplying Data Controller and the Receiving Data Controller shall assist each other in ensuring compliance with their obligations pursuant to the GDPR.

In the case of a personal data breach related to the processing subject of this Protocol, the Supplying Data Controller and the Receiving Data Controller shall notify each other, the PEH Data Platform Manager and the DRAC within twenty-four (24) hours after becoming aware of that personal data breach. To this purpose a list of contact persons of each signatory to be contacted in case of data breach will be accessible for all signatories to this protocol. All signatories are responsible that the information in this list is up to date.

This notification shall at least include following information:

- the nature of the personal data breach;
- the categories of personal data;
- the categories and approximate number of data subjects concerned;
- the categories and approximate number of personal data records concerned.
- the name and contact details of the data protection officer or other contact point where more information can be obtained;
- description of the likely consequences of the personal data breach;
- description of the measures taken or proposed to be taken to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

The DRAC is also responsible for determining further steps in the event of a data breach and shall involve the General Assembly.

In the event of breach of this Protocol or the GDPR and applicable national legislation, the DRAC can instruct a Receiving Data Controller to stop further processing of the personal data with immediate effect, after which it will report this to the General Assembly. If, after notification from the DRAC, the Receiving Data Controller does not stop further use, the General Assembly will decide which further steps should be taken, and the participation to this Protocol (and thus further exchange and use of HBM data) can be terminated. In such situation, the Supplying Data Controller shall not be liable for any claims or damages which may result from the unauthorized use by the Receiving Data Controller.

In case of breach of this Protocol by a Data Controller ("Breaching Data Controller"), and the Breaching Data Controller cannot rectify the breach within a period of thirty (30) calendar days from notification by the General Assembly to the Breaching Data Controller of the breach in question, then the General Assembly can decide that the Breaching Data Controller has to withdraw from the Protocol as a Receiving Data Controller and the use of the HBM data.

ARTICLE 11: TRANSFER TO THIRD PARTIES

The transfer to third parties, in any manner possible is prohibited, unless it's legally required or in case the Receiving Data Controller has obtained the explicit consent by the DRAC to do so. In case a legal obligation applies to transfer to third parties of personal data subject to this Protocol, the Receiving Data Controller shall - prior to the transfer - notify the Supplying Data Controller and the DRAC.

ARTICLE 12: TRANSFER TO THIRD COUNTRIES OR AN INTERNATIONAL ORGANIZATION

The parties expressly agree that the personal data shall not be transferred outside the European Economic Area without a prior written consent given by the DRAC. Transfer of personal data to a third country or an international organization may take place in case there is an adequacy decision. In the absence of such adequacy decision the transfer to a third country may only take place in case the Receiving Data Controller has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

ARTICLE 13: LIABILITY

The Supplying Data Controller is responsible for obtaining the consent of the data subject for processing his or her personal data according to the provisions of the GDPR.

All Data Controllers declare that the processing activities subject to this Protocol are allowed from ethico-legal perspective.

The Receiving Data Controller is liable for the damage caused by processing only: where the Receiving Data Controller, or its Data Processor(s), has not complied with obligations of the GDPR specifically directed to Receiving Data Controllers, where the Receiving Data Controller has acted outside or contrary to lawful instructions of the Supplying Data Controller.

The Receiving Data Controller is liable to pay administrative fines which derive from their breach of the provisions of the GDPR.

The Receiving Data Controller shall be exempted from its liability, if it proves that it is not responsible for the event giving rise to the damage.

ARTICLE 14: INTELLECTUAL PROPERTY RIGHTS

All intellectual property rights as regards to the databases which contain the personal data (except for the PEH Data Platform) are reserved to the Supplying Data Controller, unless otherwise contractually agreed upon. VITO owns the PEH Data Platform and its intellectual property rights.

ARTICLE 15: DISSEMINATION OF RESULTS

The Receiving Data Controller has the right to disseminate the results obtained from the approved processing of the PEH data in any form (such as scientific papers, abstracts and presentations for conferences or workshops, other publications). It shall contact the Supplying Data Controller and provide title, abstract, and author list at latest thirty (30) calendar days prior to submission of material for presentation or publication. The Supplying Data Controller will be requested to explicitly acknowledge receipt of this communication. For scientific papers and abstracts for scientific conferences the Supplying Data Controller is entitled to request to include two (2) co-authors. The use of the PEH Data Platform will be acknowledged. The Supplying Data Controller has a period of twenty (20) days to object the dissemination. In case of objection, the Receiving Data Controller and the Supplying Data Controller shall cooperate to correct the material. In case the Supplying Data Controller did not object the dissemination within aforementioned period, the material shall be deemed approved for dissemination. The original data owners' requirements or project-specific requirements for acknowledgment have to be followed.

The RDC will provide the SDCs with a summary in laymen's terms of the results of the research carried out with the data, for possible communication with the data subjects.

ARTICLE 16: TERMINATION

A participating Data Controller can decide to terminate its participation in this Protocol with a prior notice of three (3) months (article 8 Membership). A Breaching Data Controller can be excluded from the Protocol (article 10 Data Breach). Neither of these do affect this Protocol between the other participating Data Controllers, so this Protocol continues to exist and apply, until all parties decide to terminate it. the Supplying Data Controller will inform the PEH Data Platform Manager of what should be done with the supplied data. If the Supplying Data Controller fails to do so within a term of thirty (30) days after termination of the platform, the data will be deleted by the PEH Data Platform Manager.

ARTICLE 17: APPLICABLE LAW – DISPUTE SETTLEMENT

This Protocol and all action related hereto shall be governed, controlled, interpreted, and enforced by and under the laws of Belgium, without regard to the conflict of law provisions thereof.

Any dispute arising from this Protocol unless resolved by amicable negotiations will be finally settled by the competent courts located in Antwerp (Belgium).

ARTICLE 18: EXHAUSTIVENESS OF THE PROTOCOL

In the event that either one of these contractual clauses is destroyed or elucidated non-valid in any other way, the rest of the Protocol still applies and the concerning contractual clause shall be replaced by a valid contractual clause which correctly represents the initial intentions of the parties.

Every Data Controller who wishes to use the PEH Data Platform will first have to sign this Protocol. The Protocol shall be effective only when signed by the authorized representatives of the Data Controllers and the PEH Data Platform Manager.

The signature of a representative of a Party received by electronic image transmission (such as portable document format) will constitute an original signature. Each Party receives a fully executed copy of the Collaboration protocol. Delivery of the fully executed copy by electronic image transmission shall have the same force and effect as delivery of the original Collaboration protocol.

The General Assembly may, in whole or in part, alter, amend, update or review the Protocol. A Data Controller's use of the PEH Data Platform will be subject to the most current version of the Protocol generally announced by the General Assembly at the time of such use.

APPENDIX 1: SENSITIVE PERSONAL DATA IN THE PEH DATA PLATFORM

Data requests pertain to **sensitive personal data**. More specifically they potentially include:

- **Data concerning health**: all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject. This includes information about the natural person collected in the course of the registration for, or the provision of, health care services as referred to in Directive 2011/24/EU of the European Parliament and of the Council to that natural person; a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes; information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test
  - **Genetic data*:** personal data relating to the inherited or acquired genetic characteristics of a natural person which result from the analysis of a biological sample from the natural person in question, in particular chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis, or from the analysis of another element enabling equivalent information to be obtained

    *Only applicable for data collections that participate in the analysis of effect biomarkers.
- **Data revealing racial or ethnic origin**
- **Data from data subjects younger than 13 years of age**
- **Data from data subjects younger than 16 years of age**

APPENDIX 3: SECURITY OF PROCESSING

The receiving Data Controllers should provide sufficient guarantees, in particular in terms of expert knowledge, reliability and resources, to implement technical and organizational measures as mentioned in article 32 GDPR which will meet the requirements of the GDPR, including for the security of processing.2

In order to ensure a level of security appropriate to the risk, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Data Controllers shall implement appropriate technical and organizational measures.

Minimal technical measures must be all of the following:

- Pseudonymization and encryption of personal data
- Firewall
- Anti-malware software
- Back-ups
- Extra servers in case needed
- Network infrastructure Logging (Read and write)
- Physical protection of devices

Minimal organizational measures must be all of the following:

- Records of processing activities3
- Information security policy
- Access management: 2-factor authentication for example (something you have + password + login)
- Directory of those processing personal data
- Contractual protocols with employees and contractors stating confidentiality
- Process for regularly testing, assessing and evaluating
- Privileged identity management: minimalize access to personal data
- Disaster recovery

To conclude it may be very interesting to get certified by an ISO 27001 certificate in order to cover for IT security:

- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

Note: when assessing the appropriate level of security, the risks that are presented by processing should be taken into account, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.

[2] Recital 81 GDPR

[3] Article 30 GDPR

APPENDIX 4 OVERVIEW OF TECHNICAL AND ORGANIZATIONAL MEASURES PEH DATABASE MANAGER

INFORMATION SECURITY- AND PRIVACY POLICY

OVERVIEW OF TECHNICAL& ORGANIZATIONAL MEASURES

Version Q4 2019

Summary of technical and organizational measures

1.1 Information Security Policies

- VITO has a set of formal and up-to-date policies for information security defined by the senior management, published and communicated on a regular basis to all employees and relevant external parties. *(Measure subject to continuous improvement)*
- The policies for information security are reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

1.2 Organization of Information Security

- All information security responsibilities are defined and allocated in line with the information security policies (DPO, decision-making structures, etc.)
- VITO has a procedure stipulating the appropriate contacts with relevant authorities and external parties, concerning information security (e.g.. a GDPR-compliant incident procedure or a procedure regarding consulting of the DPA concerning a DPIA.)
- VITO maintains appropriate contacts with special interest groups or other specialist, security forums and professional associations. The goals of such contacts are among others staying up-to-date, developing best practices, getting informed quickly when new threats arrive, getting access to specialized services and exchanging information and experiences.

1.3 Human Resource Security

- The contractual agreements with employees and contractors state the responsibilities for information security for both parties. The employee contract stipulates how to handle confidential information and makes mention of 3 levels of confidentiality. Furthermore, standard clauses are used (e.g. for Ph.D. students) as well as data processing agreements and NDA's (in case of external employees related to sub-processors).
- All employees of the Organisation and relevant contractors are aware of the risks and the importance of information security. On a regular basis, they receive appropriate awareness education among others via Lunch talks, newsletters (Channel V), intranet and a SharePoint site where information security aspects are discussed.
- VITO has a formal and communicated disciplinary process in place to take action against employees who have, willingly or unwillingly, committed an information security breach.
- Information security responsibilities and duties that remain valid after termination or a change of employment are defined, made enforceable, and communicated to the employee or contractor.