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

Release date: 20/03/2026

Preliminary provisions

The Personal Exposure and Health Data Platform ("PEH Data Platform") has been developed at VITO in order to give access and to share single measurement Personal Exposure and Health data ("PEH data"), most commonly originating from population studies, in the highest possible resolution to researchers and other stakeholders.

It is the intention of the Supplying Data Controllers of the data included in this platform, to make the data on this data platform further available to stakeholders 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 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 Personal Exposure and Health (PEH) Data Platform is a secure infrastructure developed and managed by VITO to facilitate the collection, harmonized storage, and controlled access of pseudonymised or anonymised single measurement data from population studies. The platform enables Supplying Data Controllers (SDCs) to deposit data, and Receiving Data Controllers (RDCs) to access approved subsets of PEH data for re-use, in accordance with the terms and conditions of this Protocol and all applicable legal and ethical requirements. The PEH Data Platform supports transparent data governance, ensures data protection and traceability, and provides operational services for data harmonisation, data processing, quality control, and access management.

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. The DRAC operates in accordance with internal Rules of Procedure adopted by the General Assembly. These Rules of Procedure are binding for all DRAC members and may be amended by the General Assembly without the need for a formal amendment to this Protocol.

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 3**.

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 is accessible to stakeholders to deposit data from population studies and/or to get access to PEH 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 for the collection, storage, and harmonized access to single measurement PEH data from population studies (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.

In addition to the exchange of single measurement data as governed by this Protocol, the PEH Data Platform also offers additional functionalities, including (but may be not limited to) the collection and publication of metadata and the calculation and publication of summary statistics. The applicable rules and procedures for these functionalities, as well as for general platform use, are made transparent to users via terms and conditions boxes that must be acknowledged when accessing the platform and/or using these services. These functionalities and their associated rules fall outside the scope of this Protocol.

ARTICLE 3: DATA

The data stored on the PEH Data Platform will be Pseudonymised or Anonymised Single Measurement Data and include special categories of personal data, Article 9 of the GDPR (see **Appendix 1**).

Appendix 2 provides an overview of the PEH data available in the PEH Data Platform as of November 2025. As new studies and datasets may be added over time, the platform website includes a continuously updated ("living") overview of available data. This overview serves to inform users about data availability.

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 3)**.

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 3**), 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 (Art. 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. The RDC shall, within one (1) month after the end of the Research Project as indicated in the Request for Access, erase all personal data obtained related to this Research Project from all environments where the data are actively processed, and shall confirm this erasure to the SDC. Notwithstanding this erasure, the RDC may retain an archival copy of the data in a secure, restricted environment for up to two (2) years after the end of the Research Project, solely for the purpose of enabling reproducibility of the original research. This archival copy must not be used for any other purpose

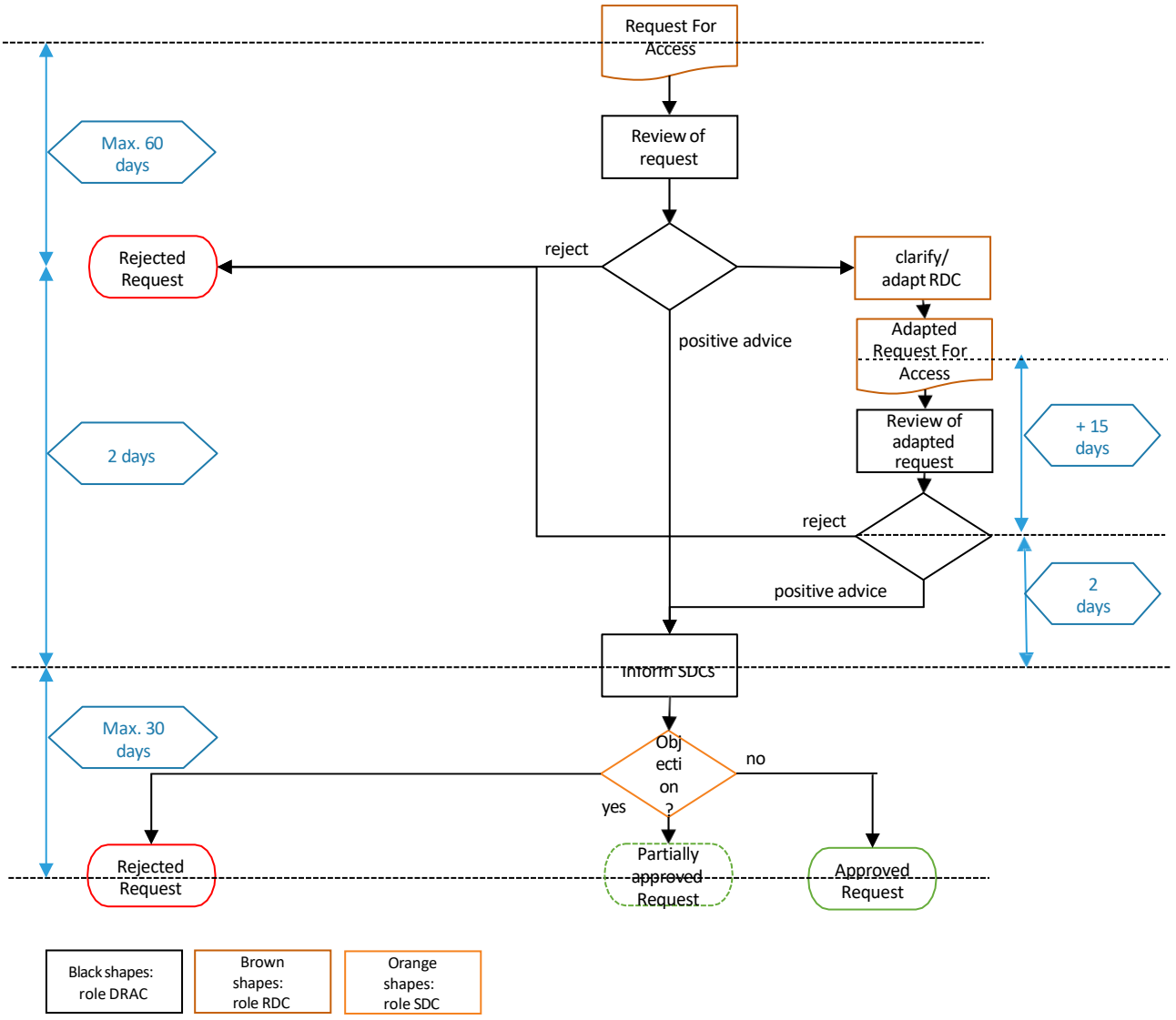

Figure 1: Procedure for submitting and evaluating a Request For Access.

The format and exact contents described in **Appendix 3** may be adapted over time to best fit the operational needs of the PEH data platform and its users; however, the general framework and procedures as agreed in this protocol remain binding..

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 PEH 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 PEH data.
- Is responsible for harmonization and Quality Control of the data. The PEH Data Platform managers support the SDC providing services via the PEH Data Platform.
- is responsible for clearly indicating to the PEH Data Platform Manager the end date or time period for which processing of the provided data is permitted from ethico legal perspective (e.g. ethical approval and/or data security approval). Any changes to this processing period must be communicated without undue delay. In case no end date applies to the provided data, this is made clear by the SDC.
- acknowledges that, for approved Requests for Access, the DRAC may, upon motivated request by the Receiving Data Controller, (i) approve an extension of the active processing period by up to one (1) additional year, and/or (ii) approve the addition of new nominated persons affiliated with the original institutions listed in the Request for Access, without further consultation of the Supplying Data Controllers. Supplying Data Controllers are expected to take these possibilities into account when approving the initial request. The SDC can request to the PEH Data Platform Manager an overview of data requests and involved RDCs (and the corresponding list of nominated users) concerning PEH data provided by the SDC.

5.2 Receiving Data Controller

The Receiving Data Controller shall, within one (1) month after the end of the Research Project as indicated in the Request for Access, erase all personal data obtained related to this Research Project from all environments where the data are actively processed, and shall confirm this erasure to the SDC. Notwithstanding this erasure, the RDC may retain an archival copy of the data in a secure, restricted environment for up to two (2) years after the end of the Research Project, solely for the purpose of enabling reproducibility of the original research. This archival copy must not be used for any other purpose

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 data.

The Receiving Data Controller may, for an approved Request for Access, submit a motivated request to the DRAC for (i) an extension of the active processing period by up to one (1) additional year, or (ii) the addition of new nominated persons to the list of individuals who require access to the data, provided these persons are affiliated with one of the institutions included in the original approved Request for Access. The DRAC may approve such requests without further consultation of the Supplying Data Controllers.

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")

Internal Rules of Procedure

The DRAC shall organise its, activities and meetings in accordance with internal Rules of Procedure, which are adopted, amended, and revoked by the General Assembly. These Rules of Procedure shall cover, among other things, the election of members, the frequency of meetings, convening procedures, decision-making, record-keeping, and other practical aspects of the DRAC's functioning.

The authorities of the DRAC, as described in this Protocol, remain unaffected. Amendments to the Rules of Procedure do not require a formal amendment of this Protocol but shall be adopted by the General Assembly and communicated to all parties.

Authority

The DRAC can ask the PEH Data Platform Manager to verify if requested data are available in the data platform.

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 10 of this Protocol).

In addition to the above, the DRAC has the authority to decide on the following matters related to approved Requests for Access:

- The DRAC may approve an extension of the active processing period for an approved Request for Access by up to one (1) additional year, upon motivated request by the Receiving Data Controller. Such an extension may be granted without further consultation of the Supplying Data Controllers. Supplying Data Controllers are expected to take this possibility into account when approving the initial processing period. The DRAC will inform the involved Supplying Data Controllers on approval of extension of the processing period.
- The DRAC may, upon motivated request by the Receiving Data Controller, approve the addition of new nominated persons to the list of individuals who require access to the data, provided that these persons are affiliated with one of the institutions included in the original approved Request for Access. Such additions may be granted without further consultation of the Supplying Data Controllers. The DRAC will inform the involved Supplying Data Controllers on approval of additional nominated users.

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;
- stop processing of single measurement data of a particular dataset when processing of the particular dataset is not further allowed from ethico legal perspective (on instruction of the SDC)

- 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, …)
- provide services through the PEH Data Platform to support the SDC in data harmonisation and Quality Control. This includes conformity checks with codebooks: consistency checks, missing data, ranges and categories for variables, …); 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
- on request of the SDC: provide an overview of data requests and involved RDCs (and the corresponding list of nominated users) concerning PEH data provided by the SDC.
- 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 5**).

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.

VITO will not charge any costs for hosting and maintaining the platform for the duration of PARC, the Partnership for the Assessment of Risks of Chemicals, as they are included in the VITO PARC budget. Adaptations to this cost arrangement 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
- Adoption, amendment, and revocation of the Rules of Procedure 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 10 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 Supplying Data Controller performs the steps for data harmonisation and Quality Control, based on guidelines and services in the PEH Data Platform. The resulting 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 PEH data is allowed by the DRAC. At the choice of the Supplying Data Controller, the Receiving Data Controller shall delete or return all the PEH 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 3**), 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, relating to the obligations of the Data Processor within the scope of the instructions of the Receiving Data Controller, the Receiving Data Controller shall remain fully liable for the performance of that Data Processor's obligations. In case the Data Processor fails to fulfill its data protection obligations which goes beyond the scope of instructions by the Receiving Data Controller, the Processor shall be liable.

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 PEH 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 PEH 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 for Receiving Data Controllers is included in **Appendix 4** to this Protocol.

Technical and organizational measures related to the PEH Data Platform Manager are included in **Appendix 5.**

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 immediately, without undue delay, 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.

The parties will reasonably assist each other, at first request, in the investigation, mitigation and remediation of a (suspected) personal data breach and in notifying a personal data breach to the supervisory authority and the data subjects concerned and will prioritize responding to any question or request from the parties concerned regarding a personal data breach.

In case a party notifies a supervisory authority, said party is then obliged to include in its notification that other supervisory authorities may have been notified by the parties concerned.

Each party concerned is entitled to receive copies of another party's communication with any supervisory authority.

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 PEH 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 PEH 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: SPECIAL CATEGORIES OF PERSONAL DATA IN THE PEH DATA PLATFORM

Data requests pertain to special categories of 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
- **Data revealing racial or ethnic origin**
- **Political opinions**
- **Religious or philosophical beliefs**
- **Trade union membership**
- **Data concerning a natural person's sex life or sexual orientation**

Furthermore, data from data subjects younger than 13 years of age and Data from data subjects younger than 16 years of age may be included

APPENDIX 2: DATA IN THE PEH DATA PLATFORM

As new studies and datasets may be added over time, the platform itself also includes a continuously updated ("living") overview of available data. This overview is an integral part of the PEH Data Platform and serves to inform users about the current status of data availability.

HBM4EU Aligned studies in CHILDREN (6-11 years)			
Study Acronym	**Country**	**Supplying data controller**	**Link to IPCHEM metadata page**
☐ OCC	DK	SDU	https://ipchem.jrc.ec.europa.eu/index.html#showmetadata/OCC
☐ NEB II	NO	NIPH	https://ipchem.jrc.ec.europa.eu/#showmetadata/NEBII
☐ Indoor Air Quality	HU	NPHI	https://ipchem.jrc.ec.europa.eu/index.html#showmetadata/INAIRQ
☐ PCB cohort	SK	SZU	https://ipchem.jrc.ec.europa.eu/index.html#showmetadata/PCBCOHORT
☐ POLAES	PL	NIOM	https://ipchem.jrc.ec.europa.eu/#showmetadata/POLAES
☐ SLO CRP	SL	JSI	https://ipchem.jrc.ec.europa.eu/index.html#showmetadata/SLOCRP
☐ CROME	EL	AUTH	https://ipchem.jrc.ec.europa.eu/#showmetadata/CROME
☐ NAC II	IT	EPIUD	https://ipchem.jrc.ec.europa.eu/index.html#showmetadata/NACII
☐ ESTEBAN	FR	SPF	https://ipchem.jrc.ec.europa.eu/#showmetadata/ESTEBAN
☐ GerES V	DE	UBA	https://ipchem.jrc.ec.europa.eu/index.html#showmetadata/GERESV
☐ 3xG	BE	VITO	https://ipchem.jrc.ec.europa.eu/index.html#showmetadata/3XG
☐ SPECIMEn-NL	NL	IRAS	https://ipchem.jrc.ec.europa.eu/#showmetadata/SPECIMENNL
☐ RAV MABAT	IL	MOH-IL	https://ipchem.jrc.ec.europa.eu/#showmetadata/RAVMABAT
☐ ORGANIKO	CY	MOH-CY	https://ipchem.jrc.ec.europa.eu/#showmetadata/ORGANIKO

HBM4EU Aligned studies in TEENAGERS (12-19 years)			
Study Acronym	**Country**	**Supplying data controller**	**Link to IPCHEM metadata page**
☐ Riksmaten Ungdom	SE	SFA	https://ipchem.jrc.ec.europa.eu/#showmetadata/RIKSMATENADOLESCENTS201617
☐ NEB II	NO	NIPH	https://ipchem.jrc.ec.europa.eu/#showmetadata/NEBII
☐ (C)ELSPAC: TE	CZ	MU	https://ipchem.jrc.ec.europa.eu/#showmetadata/CELSPACTE
☐ PCB cohort follow-up	SK	SZU	https://ipchem.jrc.ec.europa.eu/index.html#showmetadata/PCBCOHORT
☐ POLAES	PL	NIOM	https://ipchem.jrc.ec.europa.eu/#showmetadata/POLAES
☐ SLO CRP	SL	JSI	https://ipchem.jrc.ec.europa.eu/index.html#showmetadata/SLOCRP
☐ CROME	EL	AUTH	https://ipchem.jrc.ec.europa.eu/#showmetadata/CROME
☐ BEA	ES	ISCIII	https://ipchem.jrc.ec.europa.eu/#showmetadata/BEA
☐ ESTEBAN	FR	SPF	https://ipchem.jrc.ec.europa.eu/#showmetadata/ESTEBAN
☐ GerES V	DE	UBA	https://ipchem.jrc.ec.europa.eu/index.html#showmetadata/GERESV
☐ FLEHS IV	BE	FLEHS consortium	https://ipchem.jrc.ec.europa.eu/#showmetadata/FLEHS4REFADO

HBM4EU Aligned studies in ADULTS (20-39 years)			
Study Acronym	**Country**	**Supplying data controller**	**Link to IPCHEM metadata page**
☐ CPHMINIPUB parents/DYMS	DK	RegionH	https://ipchem.jrc.ec.europa.eu/index.html#showmetadata/DYMS
☐ DIET_HBM	IS	UI	https://ipchem.jrc.ec.europa.eu/#showmetadata/DIETHBM
☐ (C)ELSPAC: YA	CZ	MU	https://ipchem.jrc.ec.europa.eu/#showmetadata/CELSPACYA
☐ POLAES	PL	NIOM	https://ipchem.jrc.ec.europa.eu/#showmetadata/POLAES
☐ HBM in Croatia	HR	CIPH	https://ipchem.jrc.ec.europa.eu/index.html#showmetadata/HBMSURVEYINADULTSINCROATIA
☐ INSEF-ExpoQuim	PT	INSA	https://ipchem.jrc.ec.europa.eu/#showmetadata/INSEFEXPOQUIM
☐ HBM4EU-study Switzerland	CH	SWISS TPH	https://ipchem.jrc.ec.europa.eu/#showmetadata/HBM4EUSTUDYINSWITZERLAND
☐ ESTEBAN	FR	SPF	https://ipchem.jrc.ec.europa.eu/#showmetadata/ESTEBAN
☐ ESB	DE	UBA	https://ipchem.jrc.ec.europa.eu/index.html#showmetadata/ESB
☐ Oriscav-Lux2	LU	LNS	https://ipchem.jrc.ec.europa.eu/#showmetadata/ORISCAVLUX2
☐ RAV MABAT	IL	MOH-IL	https://ipchem.jrc.ec.europa.eu/#showmetadata/RAVMABAT

FinHealth data (https://ipchem.jrc.ec.europa.eu/#showmetadata/FINHEALTH) are not available via the PEH data platform.

Further specify the sub-datasets of the MoM-study that are needed for this study protocol in the table below:

HBM4EU MoM study (MethylmercurY-contrOl in expectant Mothers through suitable dietary advice for pregnancy)			
	Country	**Supplying data controller**	**Link to IPCHEM metadata page**
☐ HBM4EU mom-ES	ES	ISCIII	(not yet available)
☐ HBM4EU mom-CY	CY	MOH-CY	
☐ HBM4EU mom-EL	EL	AUTH	
☐ HBM4EU mom-IS	IS	UI	
☐ HBM4EU mom-PT	PT	INSA	

APPENDIX 3: TEMPLATE REQUEST FOR ACCESS

Appendix 3 serves as an example template for submitting a Request For Access under this protocol. The format and exact contents described in Appendix 3 may be adapted over time to best fit the operational needs of the platform and its users; however, the general framework and procedures as agreed in this protocol remain binding.

Personal Exposure and Health Data Platform

("PEH Data Platform")

Data Access Request Form

Version 0.2

Preliminary note

This template serves to request access to data stored in the PEH data platform at VITO. Access to extracts of the data will be provided through this data platform after approval of the request by the DRAC and signing the Protocol by the Receiving Data Controller.

This template reflects the actual availability of datasets in the Platform. It will be updated regularly to reflect the availability of new datasets. Parts of this template, i.e., available datasets, available data and selection of data requested for the Research Project, may be provided in the future through web-based catalogues.

1 Request identification

In some cases, more than one Receiving Data Controller (RDC) may be involved in the same Research Project. In that case each RDC submits a separate Request for Access, specifying the specific research questions that will be addressed by the RDC and the specific data requested.

Date of submission:	
Main project name:	*(e.g., main project under which the specific Research Project may resort, e.g., acronym and full name of Horizon Europe or member state funded project, …*
Research Project for which data access is requested:	*(The title of the specific research for which the data are requested, which directly relates to the specific research questions that are addressed; this can be a work package, a task or an activity in a larger project, if specific enough, or a dedicated title; in some cases, the main project name will be specific enough)*
Request number	*(Not to be filled in by the requesting party)*

2 Background

Provide the scientific background regarding the research hypothesis including key references (appr. 1000 characters, excluding references).

….

3 Objective

Explain the objective of the Research Project and state the specific research question(s).

….

4 Methods

4.1 Study design

Describe the overall study design and target group e.g., age (children/teenagers/adults), sex,… inclusion, exclusion criteria

…..

Specify the dataset available in the PEH to which you request access:

☐ HBM4EU Aligned studies

☐ HBM4EU MoM study

Further specify the sub-datasets of the HBM4EU Aligned studies that are needed for this study protocol in the table below[1]:

HBM4EU Aligned studies in CHILDREN (6-11 years)			
Study Acronym	**Country**	**Supplying data controller**	**Link to IPCHEM metadata page**
☐ OCC	DK	SDU	https://ipchem.jrc.ec.europa.eu/index.html#showmetadata/OCC
☐ NEB II	NO	NIPH	https://ipchem.jrc.ec.europa.eu/#showmetadata/NEBII
☐ Indoor Air Quality	HU	NPHI	https://ipchem.jrc.ec.europa.eu/index.html#showmetadata/INAIRQ
☐ PCB cohort	SK	SZU	https://ipchem.jrc.ec.europa.eu/index.html#showmetadata/PCBCOHORT
☐ POLAES	PL	NIOM	https://ipchem.jrc.ec.europa.eu/#showmetadata/POLAES
☐ SLO CRP	SL	JSI	https://ipchem.jrc.ec.europa.eu/index.html#showmetadata/SLOCRP
☐ CROME	EL	AUTH	https://ipchem.jrc.ec.europa.eu/#showmetadata/CROME
☐ NAC II	IT	EPIUD	https://ipchem.jrc.ec.europa.eu/index.html#showmetadata/NACII
☐ ESTEBAN	FR	SPF	https://ipchem.jrc.ec.europa.eu/#showmetadata/ESTEBAN
☐ GerES V	DE	UBA	https://ipchem.jrc.ec.europa.eu/index.html#showmetadata/GERESV
☐ 3xG	BE	VITO	https://ipchem.jrc.ec.europa.eu/index.html#showmetadata/3XG
☐ SPECIMEn-NL	NL	IRAS	https://ipchem.jrc.ec.europa.eu/#showmetadata/SPECIMENNL
☐ RAV MABAT	IL	MOH-IL	https://ipchem.jrc.ec.europa.eu/#showmetadata/RAVMABAT
☐ ORGANIKO	CY	MOH-CY	https://ipchem.jrc.ec.europa.eu/#showmetadata/ORGANIKO

[1] *Remark: More information about available exposure data for each of the sub-datasets is available (https://hbm.vito.be/peh-data-platform).*

HBM4EU Aligned studies in TEENAGERS (12-19 years)			
Study Acronym	**Country**	**Supplying data controller**	**Link to IPCHEM metadata page**
☐ Riksmaten Ungdom	SE	SFA	https://ipchem.jrc.ec.europa.eu/#showmetadata/RIKSMATENADOLESCENTS201617
☐ NEB II	NO	NIPH	https://ipchem.jrc.ec.europa.eu/#showmetadata/NEBII
☐ (C)ELSPAC: TE	CZ	MU	https://ipchem.jrc.ec.europa.eu/#showmetadata/CELSPACTE
☐ PCB cohort follow-up	SK	SZU	https://ipchem.jrc.ec.europa.eu/index.html#showmetadata/PCBCOHORT
☐ POLAES	PL	NIOM	https://ipchem.jrc.ec.europa.eu/#showmetadata/POLAES
☐ SLO CRP	SL	JSI	https://ipchem.jrc.ec.europa.eu/index.html#showmetadata/SLOCRP
☐ CROME	EL	AUTH	https://ipchem.jrc.ec.europa.eu/#showmetadata/CROME
☐ BEA	ES	ISCIII	https://ipchem.jrc.ec.europa.eu/#showmetadata/BEA
☐ ESTEBAN	FR	SPF	https://ipchem.jrc.ec.europa.eu/#showmetadata/ESTEBAN
☐ GerES V	DE	UBA	https://ipchem.jrc.ec.europa.eu/index.html#showmetadata/GERESV
☐ FLEHS IV	BE	FLEHS consortium	https://ipchem.jrc.ec.europa.eu/#showmetadata/FLEHS4REFADO

HBM4EU Aligned studies in ADULTS (20-39 years)			
Study Acronym	**Country**	**Supplying data controller**	**Link to IPCHEM metadata page**
☐ CPHMINIPUB parents/DYMS	DK	RegionH	https://ipchem.jrc.ec.europa.eu/index.html#showmetadata/DYMS
☐ DIET_HBM	IS	UI	https://ipchem.jrc.ec.europa.eu/#showmetadata/DIETHBM
☐ (C)ELSPAC: YA	CZ	MU	https://ipchem.jrc.ec.europa.eu/#showmetadata/CELSPACYA
☐ POLAES	PL	NIOM	https://ipchem.jrc.ec.europa.eu/#showmetadata/POLAES
☐ HBM in Croatia	HR	CIPH	https://ipchem.jrc.ec.europa.eu/index.html#showmetadata/HBMSURVEYINADULTSINCROATIA
☐ INSEF-ExpoQuim	PT	INSA	https://ipchem.jrc.ec.europa.eu/#showmetadata/INSEFEXPOQUIM
☐ HBM4EU-study Switzerland	CH	SWISS TPH	https://ipchem.jrc.ec.europa.eu/#showmetadata/HBM4EUSTUDYINSWITZERLAND
☐ ESTEBAN	FR	SPF	https://ipchem.jrc.ec.europa.eu/#showmetadata/ESTEBAN
☐ ESB	DE	UBA	https://ipchem.jrc.ec.europa.eu/index.html#showmetadata/ESB
☐ Oriscav-Lux2	LU	LNS	https://ipchem.jrc.ec.europa.eu/#showmetadata/ORISCAVLUX2
☐ RAV MABAT	IL	MOH-IL	https://ipchem.jrc.ec.europa.eu/#showmetadata/RAVMABAT

FinHealth data (https://ipchem.jrc.ec.europa.eu/#showmetadata/FINHEALTH) are not available via the PEH data platform.

Further specify the sub-datasets of the MoM-study that are needed for this study protocol in the table below:

HBM4EU MoM study (MethylmercurY-contrOl in expectant Mothers through suitable dietary advice for pregnancy)			
	Country	**Supplying data controller**	**Link to IPCHEM metadata page**
☐ HBM4EU mom-ES	ES	ISCIII	(not yet available)
☐ HBM4EU mom-CY	CY	MOH-CY	
☐ HBM4EU mom-EL	EL	AUTH	
☐ HBM4EU mom-IS	IS	UI	
☐ HBM4EU mom-PT	PT	INSA	

4.2 Exposure variables and accompanying variables

Describe the exposure variables (specific metabolites), accompanying variables (age, sex, SES, NUTS,…), effect biomarker/health outcome data needed to investigate the specific research questions. More information about available exposure data, effect biomarker data and health outcome information for each of the sub-datasets is available in the overview tables *(https://hbm.vito.be/peh-data-platform)*. The full list of variables can be consulted in annex 1 of this template ("Annex_1_PEH_DataAccessRequestForm_PEHstudies_variable_list"), more detailed information on variable coding is available in the codebooks.
All variables needed for this research project should be described and the need for these variables justified in this section. Also, data in this section should be in agreement with the data requested in the excel file in "Annex 1: PEH Research protocol variable list" of this research protocol.

Exposure data:
Exposure data use should be evident from the objectives of the study (section 2). If not, please add additional justification.
Effect/health outcome data:
Effect/health outcome data use should be evident from the objectives of the study (section 2). If not, please add additional justification.
Accompanying data:
Please briefly justify why each accompanying variable is needed, e.g. as potential effect-modifying factor, as confounder, as potential exposure source, etc.

4.3 Data Analysis Plan

Explain the statistical methods that will be used.

Describe the analytical models you will use, the sensitivity analysis you will perform,…

Specify if you will do meta- and/or pooled analysis and set out the minimal requirements of data comparability to enable these analyses.

…..

The requesting party explicitly declares that only data are requested that are strictly necessary to carry out the Data Analysis Plan to answer the specific research questions.

5 Organization, publication and time schedule

5.1 Organization

Specify the responsible person who will coordinate the Research Project

Responsible person:	
Name of institution:	
E-mail:	
Phone:	

State who will do the data analyses. Only these nominated persons will be granted access to the data:

Name:	**Institute:**	**Email:**

Note: If, during the course of the project, additional nominated persons require access to the data and are affiliated with one of the institutions listed in the original approved Request for Access, the Receiving Data Controller may submit a motivated request to the DRAC to add these persons. The DRAC may approve such additions without further consultation of the Supplying Data Controllers. The DRAC will inform the involved Supplying Data Controllers on approval of additional nominated users.

5.2 External Data Processors

Indicate in the table below if an external Data Processor[2] will be engaged and which specific processing activities this Data Processor will carry out.

☐ yes, (data processor will be engaged)

☐ no, (no data processor will be engaged)

Data Processor	**Data processing activities**

[2] According to GDPR, 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

5.3 Publication

The procedures described in the Protocol on the management and use of the Personal Exposure and Health Data Platform shall be followed considering dissemination of results as outlined in ARTICLE 15: DISSEMINATION OF RESULTS.

Specify which publication(s) will result from this study protocol:

….

List of potential co-authors and their contribution to the manuscript:

….

5.4 Time schedule

Clarify the working plan in a time schedule, e.g., describe the different steps that will be taken and put a timing on it, including a timing for writing a paper of the results.

Proposed study start date: …

Propose study completion date (including publishing of the data): …

Note: The RDC shall, within one (1) month after the end of the Research Project as indicated in the Request for Access, erase all personal data obtained related to this Research Project from all environments where the data are actively processed, and shall confirm this erasure to the SDC.

If, during the course of the project, an extension of the active processing period (up to one additional year) is required, the Receiving Data Controller may submit a motivated request to the DRAC. The DRAC may approve such an extension without further consultation of the Supplying Data Controllers. Supplying Data Controllers are expected to take this possibility into account when approving the initial request. The DRAC will inform the involved Supplying Data Controllers on approval of extension of the processing period.

Notwithstanding this erasure, the RDC may retain an archival copy of the data in a secure, restricted environment for up to two (2) years after the end of the Research Project, solely for the purpose of enabling reproducibility of the original research. This archival copy must not be used for any other purpose

Annex 1

Excel file ("Annex_1_PEH_DataAccessRequestForm_PEHstudies_variable_list") must be submitted together with this request form as it is an integral part of this Data Access Request Form.

APPENDIX 4: 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 of personal data
- Encryption of personal data when relevant
- 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 5: OVERVIEW OF TECHNICAL AND ORGANIZATIONAL MEASURES PEH DATA PLATFORM MANAGER

INFORMATION SECURITY- AND PRIVACY POLICY

OVERVIEW OF TECHNICAL & ORGANIZATIONAL MEASURES:

October 2025

vito

Vision on technology
for a better world

vito.be

TABLE OF CONTENTS

INFORMATION SECURITY- AND PRIVACY POLICY 2
Table of contents 2
Purpose 3
Summary of Technical & Organizational Measures (TOM) 4
1.1 Information Security Policy 5
1.2 Organization of Information Security 5
1.3 Human Resource Security 5
1.4 Asset Management 6
1.5 Access control 6
1.6 Physical and Environmental Security 7
1.7 Operations Security 7
1.8 Security of the Communication 8
1.9 System Acquisition, Development, Maintenance & Third party risk 8
1.10 Incident Management 9

INFORMATION SECURITY- AND PRIVACY POLICY

VITO
Boeretang 200
2400 MOL
Belgium
BTW No: BE0244.195.916
vito@vito.be – www.vito.be
IBAN BE34 3751 1173 5490 BBRUBEBB

Vision on technology
for a better world

vito.be

Purpose

The purpose of this document is to provide a consolidated overview of the technical and organizational measures that VITO is progressively implementing to ensure information security and privacy. These measures are designed to achieve the strategic objective of optimally safeguarding data, enhancing our cyber resilience, and supporting that of our partners.

In practice, each processing activity may require specific organizational and technical measures depending on its nature, context, and associated risks. Depending on the processing activity, VITO can act as a processor or as a (joint) data controller when processing personal data. In case VITO acts as a processor of personal data, such measures are defined in consultation with the data controller and formally documented in the data processing agreement or its annexes.

VITO always operates in compliance with applicable legislation, including NIS2 and the General Data Protection Regulation (GDPR).

If a processing activity involves the use of (sub-)processors, the technical and organizational measures in place at the (sub-)processor must also be taken into account.
VITO strives to ensure that these measures are at least equivalent to our own standards and that the sub-processor is contractually bound to appropriate security and privacy obligations.

The processor provides services on behalf of the data controller in accordance with the scope defined in the annex of each data processing agreement or SLA.

The following points describe the general measures applied to ensure optimal protection regarding confidentiality, integrity, and availability of (personal) data.

These measures are periodically reviewed and updated where necessary, in response to technological developments, changing risks, or new legal requirements.

Summary of Technical & Organizational Measures (TOM)

1.1 Information Security Policy

VITO has an Information Security Policy to enable the principles and organisation of information security at VITO. This contributes to the strategic objective of optimally safeguarding information security and strengthening our cyber resilience.

The VITO Information Security Policy:

- Is approved by VITO management, published and communicated to all employees and relevant stakeholders.
  - Is systematically reviewed, or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.
- Contains a set of domain specific policies addressing information & cyber-security.

1.2 Organization of Information Security

In accordance with the **VITO Information Security Policy**, all information security responsibilities are defined and allocated (ISO, DPO, decision-making structures, etc.)

In addition to the overall governance related to privacy and cybersecurity, VITO:

- Has domain specific policies and operational procedures for addressing information security risks in a structured manner.
- Has a process for conducting Data Protection Impact Assessments (DPIAs) where required.
- Has requirements on implementing privacy and security by design.
- Has a Incident-response-procedure stipulating the appropriate contacts with relevant authorities and external parties, concerning information security incidents (NIS2), and data breaches (GDPR). See 1.10 below.
- Is formally registered as an 'Essential Entity' under the Centre for Cybersecurity Belgium by adhering to the CyberFundamentals framework, in alignment with the NIS2 directive requirements in Belgium.
- Maintains appropriate contacts with special interest groups or other specialists, 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

In respect to Human Resource security, the focus lies on ensuring that all personnel understand and fulfill their information security responsibilities.

Therefore VITO :

- Has contractual agreements with employees and contractors that state the responsibilities for information security for both parties. The employee contract stipulates how to handle confidential information. 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).

- Makes all employees of VITO and relevant contractors aware of the risks and the importance of information security. On a regular basis, employees receive appropriate awareness education regarding information security, including phishing-simulations, to improve awareness and correct actions.
- Has a formal and communicated disciplinary process in place to take action against employees who have, willingly or unwillingly, committed an information security breach.
- Has information security responsibilities and duties in place that remain valid after termination or a change of employment. NDA's are defined, made enforceable, and communicated to the employee or contractor.

1.4 Asset Management

In regard to asset management, the focus is on identifying, classifying, and protecting information assets to ensure their appropriate handling throughout their lifecycle.

In response, VITO:

- Maintains an inventory of assets associated with information processing in a CMDB (Configuration management database).
  - Assigns to each asset in the CMDB a designated owner, responsible for governance and operational integrity.
- Requires that asset owners adhere to an 'Acceptable Use Policy', which is being established to outline the rules for asset usage throughout its lifecycle. This includes clear instructions on data storage, secure transfer, proper disposal, and other handling procedures.
- Classifies an asset based on the sensitivity level of the data it processes, in accordance with the organization's Data Classification Policy. This classification influences the required security controls and compliance obligations.
- Reviews the asset management practices periodically to ensure they remain aligned with applicable regulatory requirements and are consistent with the principles outlined in the VITO Information Security Policy.

1.5 Access control

Through access control mechanisms, VITO ensures that access to information and systems is restricted to authorized individuals based on defined roles, responsibilities, and the principle of least privilege and need to know.

Accordingly, VITO:

- Has defined and implemented a comprehensive **password policy**. It governs requirements for password settings, including strength (complexity), change (rotation) and attack prevention, across various account types, including administrative, service, and user accounts.
  - Has defined and implemented an **access control policy**, aligned with both functional business needs and information security requirements. It applies conditional access policies based on strong authentication mechanisms, including two-factor authentication (e.g. Authenticator apps, Biometrics, client certificates on managed laptops,…) for remote network access, and privileged accounts. These measures are actively maintained and further expanded to external facing assets.

- Enforces network authentication across all VITO networks—wired and wireless—ensuring that all activities are both authenticated and authorized. VLAN access is managed via a NAC tool.
- Has formal procedures in place for user onboarding and offboarding, enabling the appropriate assignment and deactivation of access rights. These processes are initiated via HR workflows and are largely executed through automated workflows.

1.6 Physical and Environmental Security

On behalf of physical security, VITO focusses on protecting facilities, equipment, and information from unauthorized physical access, damage, or disruption.

To mitigate these threats, VITO:

- Has defined a **physical security policy** and implemented a comprehensive set of physical security controls.
- Uses a physical security perimeter to protect areas that contain either sensitive or critical information and information processing facilities.
- Protects secure zones with access controls to restrict entry to authorized personnel only and strictly supervises access to the datacenters. (e.g. camera surveillance, badge control to track access)
- Has protective measures in place against natural disasters, malicious threats, and accidental damage.
- Has shielded critical equipment from power outages and utility disruptions.
- Has established and enforced procedures for operating within secure areas.
- Physically protects data-carrying power and telecom cables against interception, interference, and manages VLAN access via a NAC tool.
- Has procedures in place to ensure sensitive data is securely erased or overwritten before disposal or reuse of VITO devices with storage media.
- Configures critical infrastructure components redundantly to ensure continuity in case of equipment failure.

1.7 Operations Security

Through operational security practices, VITO aims to ensure the secure and resilient management of information processing facilities, systems, and supporting infrastructure.

Therefore VITO :

- Monitors and optimizes system resource usage continuously, supported by capacity forecasting to maintain performance.
- Configures critical components in high-availability mode to ensure resilience in the event of asset failure.
- Applies a layered security approach to reduce the risk of malware and cyberattacks, including:
    - (Web Application) Firewalls
    - Intrusion Detection and Prevention Systems (IDPS)
    - Endpoint protection and encryption
    - Ransomware protection for data storage
    - Network access control
    - Automated isolation of compromised endpoints or users

    - Security event monitoring and alerting

- Has implemented Backup and restore procedures, ensuring regular creation and testing of backups for data, software, and system images, in line with the backup policy.
- Maintains a patch management process to deploy critical security updates in a timely manner, and applies compensating controls such as network isolation, system hardening, or virtual patching when patching is not feasible.
- Supports vulnerability management through automated scanning tools.
- Secures email communication using multiple protective measures, including authentication protocols (SPF, DKIM, DMARC), phishing filters, safe link protection, and automated scanning of attachments and URLs.
- Applies hardened standard images to system configurations, aligning with industry-recognized security standards.

1.8 Security of the Communication

To safeguard the confidentiality, integrity, and availability of information exchanged across internal and external networks, VITO enforces strong communication security measures.

In response, VITO:

- Secures all networks to prevent unauthorized access and ensure safe data transmission.
- Implements network segregation through VLANs, ensuring that critical systems requiring elevated protection are isolated from less sensitive segments.
- Includes confidentiality clauses in contracts involving third-party data exchange, such as NDAs and data processing agreements, in alignment with GDPR requirements.

1.9 System Acquisition, Development, Maintenance & Third party risk

To ensure that information security and privacy requirements are embedded throughout the system lifecycle and services — from planning to development, implementation and ongoing support — VITO applies structured practices that also address third-party risk.

To embed this, VITO:

- Incorporates information security requirements into specifications for new systems and enhancements to existing ones.
- Protects application services that transmit data over public networks against fraud, unauthorized access, and data modification by using encrypted protocols such as HTTPS and SFTP where possible.
- Reviews and tests business-critical applications when operating platforms are changed, ensuring continuity and security are not compromised.
- Applies a controlled SCRUM process to implement software modifications based on business requests.
- Defines and documents information security requirements for suppliers who access organizational assets. This is done systematically for data processors under GDPR, and as needed for other suppliers.
- Conducts regular service review meetings with key suppliers to monitor performance and address security expectations.

- Ensures that third-party engagements are governed by appropriate contractual safeguards, including confidentiality clauses, NDAs, and data processing agreements where applicable.

1.10 Incident Management

To minimize the impact of security events and foster continuous improvement, VITO ensures that incidents are promptly identified, reported, assessed, and resolved through a structured incident management process.

Therefore, VITO:

- Maintains an Incident Response Plan that is regularly reviewed and updated to remain effective and aligned with evolving threats.
- Applies formal criteria to classify incidents as data breaches or significant security incidents, in accordance with the GDPR and/or NIS2 regulation.
- Follows a documented procedure for responding to and reporting incidents or data breaches, ensuring that responsibilities and actions are clearly defined to enable a swift, structured, and effective response. This includes timely communication with management, affected data subjects, the Data Protection Authority (DPA), the National CERT, in line with applicable legal and regulatory requirements.